AUSTRALIAN BANKERS' ASSOCIATION INC.
Strong banks – strong Australia

Level 3, 56 Pitt Street
Sydney NSW 2000
Australia
+61 2 8298 0417
@austbankers
bankers.asn.au

4 March 2016

Mr Andrew Walter
Assistant Secretary
Commercial and Administrative Law Branch
Attorney-General's Department
3-5 National Circuit
Barton ACT 2600

By email to: privacy.consultation@ag.gov.au

Dear Mr Walter,

Discussion Paper Mandatory Data Breach Notification and Materials

With the active participation of its 25 members, the Australian Bankers' Association (ABA) provides analysis, advice and advocacy for the banking industry and contributes to the development of public policy on banking and other financial services.

The ABA works with government, regulators and other stakeholders to improve public awareness and understanding of the industry's contribution to the economy and to ensure Australia's banking customers continue to benefit from a stable, competitive and accessible banking industry.

The ABA appreciates the detailed consultation process initiated by the Government on the proposed regulatory scheme for mandatory data breach notification under the Privacy Act. The proposed Privacy Amendment (Notification of Serious Data Breaches) Bill 2015 (Bill) is modelled on and would replace the existing *Data breach notification — A guide to handling personal information security breaches* (Data Breach Notification Guide) overseen by the Office of the Australian Information Commissioner (OAIC).

1. Preliminary comments

There are three preliminary comments which the ABA wishes to make to ensure that the Government's approach will avoid undue resourcing, implementation and ongoing costs for businesses to comply with this law.

1.1 Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Data Retention Bill)

Your Department's Discussion Paper, refers to the Government's agreement to introduce a mandatory data breach notification scheme and to consult on the scheme in response to Recommendation 38 of the Parliamentary Joint Committee on Intelligence and Security (Joint Committee) in its Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Data Retention Bill).

The Joint Committee considered that a mandatory data breach notification scheme would be one effective mitigation strategy for those affected by a data breach flowing from the introduction of the Data Retention Bill it was considering. The Joint Committee considered that such a scheme would provide a strong incentive for telecommunications service providers to implement robust security measures to protect data retained under the data retention regime. It did not recommend a scheme beyond the immediate need for a data breach notification scheme for the Data Retention Bill.

1.2 ALRC Report 108 May 2008

This report is almost 8 years old. The Joint Committee noted that the Government was considering a wider scheme covering more than simply the telecommunications sector. It appears to have based its decision on the 2008 report of the ALRC.

The trigger for the requirement to notify proposed by the ALRC was where 'specified personal information has been, or is reasonably believed to have been, acquired by an unauthorised person and the agency, organisation or Privacy Commissioner believes that the unauthorised acquisition may give rise to a real risk of serious harm to any affected individual'.

The ALRC also noted that the relevant agency or organisation (now APP entity) would decide whether the triggering event had occurred. The ALRC's view was that this would allow organisations and agencies to develop their own standards about what constitutes a real risk of serious harm in the context of their own operations. Oversight by the Privacy Commissioner with a decision to notify affected individuals in uncertain circumstances could be made in consultation with the Privacy Commissioner, and that the Privacy Commissioner would be able to require notification where it believed that the unauthorised acquisition of information would give rise to a real risk of serious harm to any affected individual.

The ABA makes further comments about this aspect under "Specific comments on the Bill" later in this submission with respect to clause 26WC (1).

1.3 Draft Regulation Impact Statement (RIS)

The draft RIS provided with the consultation materials notes that the existing Data Breach Notification Guide overseen by the OAIC has since its inception in 2010 seen a 250% increase in data breach notifications to the OAIC's privacy regulator. There does not appear to be data in the RIS on the notifications by private sector entities to affected customers.

Banks have procedures for notifying customers where there has been a compromise of their personal information particularly in cases where credit cards or other transactional banking services information have been compromised.

In the overwhelming majority of reported cases where these compromises or unauthorised acquisitions of personal information have occurred, it is not the bank's data systems or security protections which have caused or facilitated the acquisition. Many examples are seen where third parties (e.g. merchants) have failed to take reasonable steps (or have otherwise been unable) to protect their own customer's information, relevantly credit or debit card data, provided to the business for the purpose of payment for good or services. This results in unauthorised acquisitions or disclosures of personal information including account information, held by the third party often due to inherently weak security systems or avoidable human error.

Some of these third parties are 'small business operators' which are exempt entities under the Privacy Act (see ss. 6(1) and 6D).

The Act requires that an APP entity takes reasonable steps to protect the personal information it holds from misuse, interference and loss and from unauthorised access, modification or disclosure.

Under the Bill the proposed notification scheme is intended to apply to APP entities; that is, entities covered by the Privacy Act. It follows that if a small business is not an APP entity it will have no data breach notification obligation.

Notably, as at June 2014, the Australian Bureau of Statistics reported that only 5.9% of Australian businesses had an annual turnover of more than $2 million. [1]'Small business operators' as defined in the Privacy Act are businesses that have an annual turnover of less than $3 million. Accordingly, the

[1] Section 6D(1)
http://www.abs.gov.au/AUSSTATS/subscriber.nsf/log?openagent&81650do001_2010201406.xls&8165.0&Data%20Cubes&7760658D9DDEE18DCA257DF9000E3F3A&0&Jun%202010%20to%20Jun%202014&02.03.2015&Latest

vast majority of Australian businesses – substantially fewer than 5.9% - would not be covered by the scheme.

Further, small businesses often have the least mature privacy and security capabilities; nevertheless, in the information economy and with modern computing tools, a small business may still have a large customer base, or collect personal information about large numbers of individuals.

The ABA is concerned to confirm that this gap in the privacy regulatory regime does not become a legislative requirement for an APP entity to fill with respect to notification of affected individuals. For example, where a merchant that is a small business operator experiences a breach involving payment information, the scheme should not require the relevant APP entity to notify simply because the merchant is not covered by the scheme. Our understanding is that, under the scheme as currently set out in the Bill, the APP entity has no obligation to notify because it does not hold the specific copy of the information that was subject to the breach. An APP entity may choose to voluntarily adopt that course in the interests of its customers but it should not be mandatory or otherwise regulated under the scheme.

In addition, the ABA observes new businesses and start-ups may fall under the $3 million threshold; this could create a situation in which new entrants to an industry will be granted an unreasonable commercial advantage by not being required to comply with the notification obligation (to the detriment of their customers).

2. Specific comments on the Bill

The ABA has a number of drafting concerns with the Bill.

In discussions with your Department, it was indicated that it is not the Government's intention to increase the obligations of APP entities under the APPs or to change the import of fundamental provisions and scope of the Act.

The ABA is concerned that one aspect of the Bill may change and result in an increase of an APP entity's obligations under APP 11 and create inconsistent standards of compliance under the Act. This is discussed further in 2.4 below.

2.1 Types of information covered and scope

We note the draft Bill refers in a number of places to personal information "or certain other information" and also refers to credit reporting and tax file number information. The ABA recommends removal of all references to "certain other information". The reasons are that that the regime applies only to 'personal information' as defined in the Privacy Act. These additional references are confusing and, if retained, would amount to substantial overreach of the Act.

2.1.1 Banking industry specific guidance

In consultative discussions to date, the Department has indicated that it expects the OAIC to develop guidance following the passage of the Bill. The ABA requests that this guidance is published well in advance of when the regime commences, to give sufficient time for APP entities to prepare for the new rules. The ABA also requests that serious consideration is given to providing industry specific guidance. This is particularly relevant for the banking and broader financial services sectors given the fact that these industries are custodians of large volumes of personal information and have very specific commercial and regulatory obligations applying to their respective operations. Industry specific guidance would assist to provide certainty and transparency to potentially overlapping principles. The ABA is happy to work with officers of the Privacy Commissioner to help develop such guidance and update it as required.

2.2 Definition of 'real risk of serious harm'

2.2.1 "real risk"

This expression was used in the former Government's Privacy Amendment (Privacy Alerts) Bill 2013.

The ABA raised its concerns over the uncertainty for APP entities with the Department and with the Senate Standing Committee on Legal and Constitutions Affairs which conducted a short inquiry into the 2013 Bill.

The concerns were not addressed in respect of the 2013 Bill, and do not appear to have been addressed in the current Bill. The guiding principle is that the threshold test - where notification is required when there has been a serious data breach because it would result in a real risk of serious harm - should strike an appropriate balance between the interests of customers while minimising the impact of notification on businesses by being a test that is clear and can be relied on with certainty.

A 'real risk' is defined as 'a risk that is not a remote risk'. Standard dictionary definitions of "real" refer to something that is "actual". Using the distinction with a risk that is "remote" introduces a spectrum of risk where the point on the spectrum at which a risk is real and not remote creates potential uncertainty. Either "real" could be left to normal interpretation or it would be clearer to use the language of likelihood, which appears in the OAIC's Data Breach Notification Guide. This would be in line with ALRC Report 108 recommendations and the international approach. The ALRC noted that, in international jurisprudence, the term 'real risk' has been defined to mean a "reasonable degree of likelihood"; "real and substantial risk"; "real and substantial danger".

In the course of the consultation process it was suggested that for greater certainty "real risk" might be replaced with "likely risk" or "probable risk" of serious harm.

For banks, there is the possibility that a data breach could involve a very large number of a bank's customers' data and could involve multiple parties. It would be practically very difficult for the bank to identify the individuals who may be at risk of serious harm. Yet to notify all affected customers could lead to or contribute to "notification fatigue" and, more concerning, customers developing a form of "immunity" to numerous notifications particularly where there may not be steps a customer could take to mitigate their own risk.

The ABA is concerned that the test is still too vague and specific guidance, including case study examples of where the threshold is and is not met, is explicitly needed in the Bill or must be developed and published by the OAIC well before the scheme commences.

The ABA requests the opportunity for further dialogue with your Department on this critical trigger for the obligation to notify.

2.2.2 'real risk of serious harm'

Tests such as a 'real risk of serious harm' can be subjective and will be interpreted differently by different institutions and in varying circumstances. Where there is the risk of civil penalties it will be interpreted differently by different APP entities and in varying circumstances. We note that in the course of consultative discussions to date, the Department has indicated that the 'real risk of serious harm' test is intended to require an objective, 'reasonable person' assessment of the risk of harm. However this does not address the key question of whether the test requires APP entities to consider:

- what a 'reasonable person' would consider is the risk of harm if the data breach incident happened to information relating to an average person; or
- what a 'reasonable person' would consider is the risk of harm for the actual individual whose data has been accessed or lost.

Further, where there is the risk of civil penalties it will be interpreted differently by different APP entities and in varying circumstances.

For example, what is considered to be serious emotional harm, serious financial harm, or serious physical harm?

One suggestion from ABA members has been to either simplify the categories of serious harm or simply delete the definition altogether.

Another suggestion has been to include a clearer test under which the APP entity would determine whether a potential harm is a harm that a reasonable person would consider to be a serious harm.

The ABA would appreciate having further discussions with the Department with the objective of replacing the current test in the Bill with one or a combination of these options.

At the least, more detailed guidance and case study examples of serious harm could be made available well before the scheme comes into force as an aid to interpretation. Without addressing the current uncertainty, conservative, risk averse entities with mature risk management frameworks, such as banks, will be more likely to generally adopt a strict approach to notification and take a narrow interpretation of what constitutes a 'real risk of serious harm' to minimise the risks associated with non-compliance. As mentioned above, one potential outcome if the provision is not made clearer is the exacerbation of "notification fatigue" and the associated desensitising of customers particularly where there is nothing the customer is able to do to mitigate the risk. Too broad a scheme could also contribute to an unjustified, unreasonable and unproductive erosion of public confidence in the digital economy.

In short, the notification threshold (including the interpretations of the terms that comprise the threshold) needs to be set at an appropriate level to avoid these possibilities (and resourcing issues for APP entities and for the OAIC.

If any of the alternative suggestions above are not adopted, the ABA considers it critical for the OAIC to develop guidelines in consultation with industry on this matter. This direction should be covered in the Bill or in the Explanatory Memorandum (EM).

The following hypotheticals demonstrate the difficulties in assessing 'real risk of serious harm':

Shared account:

- A and B are married. They hold a shared home loan and offset account with a bank.
- They separate, but maintain the account pending divorce proceedings. They ask for their details to be maintained separately. The bank mistakenly gives A access to B's personal information associated with the shared account, include B's recently changed residential address.
- The bank immediately notifies B of this error, updates its records and cautions the staff member that made the error.
- The bank is not aware of the details of A and B's separation – whether it is amicable or not. B does not volunteer any information to this effect. On the information available to the Bank at the time of the breach, there is no apparent risk of harm to B as a result of the disclosure.
- **Question:** Under the proposed scheme, is the bank obliged to actively investigate whether A's knowledge of B's address presents a risk (for example, collect information that A is abusive and has threatened B) in order to determine whether the disclosure should be notified to the regulator? Or is the bank intended to assume that, as domestic abuse is not uncommon in divorce scenarios, that there is a real risk of serious harm that requires notification to the regulator in the absence of specific evidence to that effect?

Multiple affected individuals:

- One of the bank's mail house service providers experiences a mail-merge error, resulting in 1000 customers receiving misaddressed transaction statements.
- One of the recipients contacts the bank to inform it of the error.
- The bank traces the error to the mailing house and identifies the other recipients of misaddressed statements. The bank contacts the recipients and asks them to destroy the statements. They agree.
- The bank notifies the intended recipients of the error, and apologises. The bank makes itself available to the affected individuals to answer questions and respond to concerns.
- Some but not all affected individuals contact the bank to ask questions.
- On the information available to it at the time of the breach, the bank is not aware of the risk of serious harm to affected individuals.
- Under the proposed scheme, is the bank obliged to actively investigate each affected individual and recipient to determine whether the misaddressed statement presents a real risk of serious harm?
- Question: Does the number of affected individuals give rise to a presumption of a real risk of serious harm requiring notification to the regulator? If so, would that presumption apply if a smaller number of individuals (for example - 100) were affected?

2.3 Clause 26WB (a) Serious data breach

2.3.1 Implications for whether there has been compliance with APP 11.1

Under APP 11.1 an APP entity's obligation is to take such steps as are reasonable in the circumstances to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. OAIC guidance indicates that this obligation may include taking reasonable steps to protect information against unauthorised access, interference, modification or disclosure in the event that the information is lost.

Section 15 of the Act provides that an APP entity must not do an act, or engage in a practice, that breaches an APP.

Data breaches can result in a number of ways without any act or practice engaged in by the APP entity as has been described above in 1.3. See also, for example, the Privacy Commissioner's determination in his investigation of Sony PlayStation Network/Qriocity, in which the Commissioner found that Sony had taken reasonable security steps as per National Privacy Principle 4, notwithstanding that it experienced a security intrusion and loss of customer information.2

As such, the ABA suggests that it would be beneficial to clarify (either in the EM or in OAIC guidance) that it is not intended that an APP entity that is required to notify a serious data breach is to be regarded as not having taken such steps as are reasonable in the circumstances to protect personal information it holds.

2.3.2 Likely to occur, may occur

Furthermore, the provisions on when information is lost (Cl26WB (2)(b) and (c) refer to 'unauthorised access to, or disclosure of, the information is likely to occur or may occur' will be difficult to apply in practice. It would be helpful to have more guidance as to when these conditions are satisfied, through case studies or examples, well before the scheme comes into force.

[2] https://www.oaic.gov.au/privacy-law/commissioner-initiated-investigation-reports/sony-playstation-network-qriocity

2.4 Clause 26WB(2)(a)(ii) and (c) (ii) - serious data breach regulations

The ABA questions whether clauses 26WB (2)(a)(ii) and (c) (ii) are necessary.

Provided the generic test of what is a serious data breach is appropriate it is unclear why a regulation making power is necessary.

The existence of this power to include data breaches of certain specific types of information as assumed "serious data breaches" will create regulatory uncertainty and for compliance measures taken by APP entities.

The consultation draft Explanatory Memorandum (EM) regarding clause 26WB (2)(c) observes it is intended to provide flexibility to deal with data breaches where loss of particularly sensitive information may result in unauthorised access or unauthorised disclosure. The EM provides that clause 26WB (2)(c) would apply "regardless of the likelihood of unauthorised access" and "regardless of the risk of harm".

There is no explanation in the EM why this regulation making power is necessary in subclause (2)(a)(ii).

Clear examples of the type of information and the associated risks which could be prescribed under this power should be provided as part of this consultation.

If there are specific types of personal information which are considered to require specific inclusion in the Bill this should be done.

The ABA understands that there are no specific regulations under consideration at this time.

Without strong evidence of the need for these regulation making powers, the ABA does not agree that these powers should form part of this amendment to the Privacy Act.

If a regulation making power is deemed absolutely necessary, then the ABA supports the proposal by the Department raised in the course of consultative discussions to date that further guidance be included in the EM. This could make reference to the categories of 'sensitive information' already contained in the Privacy Act. We also note the Department's comment in discussions to date that it is not envisaged that financial information would fall within this classification.

2.5 Entity to be "aware, or ought reasonably to be aware" - Clause 26WC(1)

The ABA is concerned about the reach of this notification provision.

2.5.1 "ought reasonably to be aware" – the problem

The provision deals with an APP entity if it is 'aware, or ought reasonably to be aware, of the existence of reasonable grounds to believe that there has been serious data breach of the entity'.

Awareness is a question of fact and is clear. In contrast, when an APP entity 'ought reasonably to be aware' is likely to be a consideration after a data breach has occurred and an APP entity has failed to satisfactorily inquire into the matter, or at all, and as a result has failed to comply with the notification requirements.

Further, the Bill does not define the meaning of the phrase 'ought reasonably to be aware'; and as such it is difficult to assess what is required of APP entities with respect to detection of data breaches, and thus when the notification obligation takes effect. For example, it is unclear whether, when an APP entity has subcontracted a function, and the subcontractor experiences a data breach and does not immediately notify the APP entity, the entity 'ought reasonably to have been aware' of the breach.

In 1.2 above, we mention the ALRC's approach that the decision is made by the APP entity if a serious date breach has occurred.

2.5.2 "Ought reasonably to have become aware" - proposed alternative approach

The ABA suggests that a more appropriate approach is needed for this aspect of awareness. Rather than the uncertain test of whether the entity ought reasonably to have been aware that there were reasonable grounds to believe a serious data breach of the entity had occurred, the ABA suggests 'becomes aware' should be the trigger for notification.

We note that APP 11.1 already requires APP entities to take such steps as are reasonable in the circumstances to protect information they hold, and that this includes reasonable steps to ensure that they are able to detect data breaches. This existing obligation could be clarified by amendments to existing OAIC guidance before the scheme comes into force.

With there being no intention by the Government to change fundamental provisions of the Act, the ABA believes that the Bill should use similar tests in the Bill as are used in the balance of the Act. This would ensure that the Bill does not inadvertently do this. The expression “ought reasonably to be aware” is not consistent and is in conflict with the test in APP 11 for taking “such steps as are reasonable in the circumstances” to protect personal information which the entity holds. The ABA reiterates that the term “holds” has an express meaning under the Act and is defined to expressly include ‘control or possession of a record that contains personal information’. It is important that the obligations in respect of notification align to obligations in respect standards of privacy compliance more broadly as these drive the standards of privacy and consumer protection and the numerous compliance programs in the banking sector that give operational meaning to these obligations to thousands of consumers in any given week, month or year as the case may be.

2.5.3 30 day assessment period

A similar concern exists with subclause 26WC (14) where an APP entity is given time to make an assessment on becoming aware (or from when it ought reasonably to have become aware) that there were reasonable grounds to believe there had been a serious data breach of the entity. Specifically, there is uncertainty as to when the 30 day assessment timeframe commences. For example, in the scenario where an APP entity engages a subcontractor and the subcontractor experiences a data breach, does the 30 day period commence when the subcontractor experiences the breach, when the subcontractor becomes aware of the breach, or when the subcontractor notifies the APP entity of the breach?

The ABA also considers that the 30 day timeframe for reporting a breach is unduly restrictive. Some complex security and privacy incidents can take longer than 30 days to assess and to gather the prescribed information for the notice. A more reasonable obligation would be ‘as soon as practicable’. Alternatively, a preliminary notification to the OAIC within 30 days could be required, with notification to affected individuals as soon as practicable thereafter.

If it were made clear that the obligation to notify arises once it is clear a serious data breach has occurred this could help to resolve this uncertainty.

2.5.4 Exemptions

The draft Bill provides an exemption from the obligation to notify where there is an inconsistency with secrecy provisions in other legislation (Cl 26WC (12).

The ABA considers that there should also be an exemption from notification if the individuals are being investigated in relation to an offence, including fraud, and notification would compromise that investigation, or when notification would breach the AML/CTF tipping off provisions.

Form of notification

The form of notification should be as flexible as possible to ensure flexibility and appropriately timely responses from APP entities.

In clause 26WC(1)(d), there are uncertainties as to what “if it is not practicable” means in regard to notification of affected individuals. It would be preferable and clearer if paragraph (d) provided for a test

such as requiring the APP entity to "take such steps (if any) as are reasonable" to notify the contents of the statement and to otherwise avail itself of the options in (d) (i) and (ii).

2.5.5 Multiple notifications

To affected individuals

The ABA considers that the current notification obligation gives rise to the risk of affected individuals receiving multiple notifications about the same incident.

For example, where a retailer experiences a data breach involving payment information (e.g. credit card details) under the current drafting of the scheme:

- the retailer, if an APP entity, would be obliged (under the Bill) to notify the OAIC and the affected individuals; these notifications would likely advise the affected individuals to contact their banks; and
- the retailer would be obliged to notify affected banks under PCI/DSS arrangements; those banks would have to contact affected individuals, about the same incident, in order to assist customers to secure their accounts according to standard business practice and to reflect the Privacy Commissioner's guidance.

This may contribute to the risk of notification fatigue.

To regulators

It is unclear whether the proposed scheme is intended to create an obligation to report incidents where the unauthorised access to or loss of personal information is due to fraud or attempted fraud.

The current description of "serious data breach" appears to capture such situations. That is, where personal information – such as account information – held by a financial institution that is subject to unauthorised access or disclosure that gives rise to a real risk of serious harm (Cl26WB(2)), including financial harm (see Cl26WF(f)).

ABA members deal with a high volume of attempted fraudulent activity. As a matter of standard industry practice, and in the process of rectifying and mitigating the incident, affected individuals are notified. However, the current notifications would not necessarily meet the requirements for notification prescribed in the draft Bill. Generally, individuals are notified that account or card details must be reissued for security reasons, and provided with further information on request. The matters prescribed by the proposed scheme may result in notifications that overwhelm affected individuals with unnecessary information in the context of fraud/attempted fraud.

Financial institutions are required to report some of these incidents to the relevant prudential regulator(s) depending on the extent and circumstances.

As such, it is unclear what objective requiring further notification to the Commissioner in respect of this category of incidents would serve. Further, the number of notifications that would be required to be made to the Commissioner relating to fraud or attempted fraud would be considerable.

If it is not intended that fraudulent activity be captured and reported under the proposed scheme, the definition of serious data breach should be amended to make this clear.

If it is intended the OAIC should receive reports of data breaches that are related to fraud or attempted fraud, the Department may wish to consider if the necessary notifications could be provided by periodic information exchange with ASIC and/or AUSTRAC.

In the alternative, the Department may wish to consider aligning the reporting mechanism of the involved regulators to minimise the reporting burden on industry.

Or, as a further alternative, the Bill could provide for periodic reporting on specified categories of incidents such as attempted fraud, rather than individual reports.

The ABA also notes that in many instances a serious data breach may involve a number of contracting parties (for example a number of banks or a bank and its service provider). The current wording of the Bill is unclear as to whether one entity may notify on behalf of multiple entities and in doing so discharge the notification obligations of these entities.

The ABA recommends that express provisions be added to the Bill that provide that where the serious data breach involves multiple entities (including the service provider of the entity) that a notice given by one APP entity or its designated service provider is taken or deemed to be given by all the entities involved.

A provision to this effect would assist with enhancing transparency and help avoid multiple notifications to the Privacy Commissioner and impacted individuals in respect of the same set of facts or incidents.

2.6 Clauses 26WC (6) and (7) Exception Commissioner's notice

The ABA agrees with the inclusion of these clauses.

In subclause (7), if the Commissioner is satisfied, it would be in the interests of an affected individual to give a notice under subclause (6), the Commissioner should have power to do so. The ABA notes Recommendation 51-1 in ALRC Report 108 which states:

'(d) An agency or organisation is not required to notify an affected individual where the Privacy Commissioner considers that notification would not be in the public interest or in the interests of the affected individual.'

The ABA believes it would be appropriate to include this further criterion in subclause (7).

Further, the ABA notes that the EM states that it is expected that the Commissioner will develop guidance in consultation with all relevant stakeholders on what factors will need to be taken into account in determining whether issuing a notice will be in the public interest. Noting the Government's concern with the possibility of notification fatigue, the ABA suggests the question of whether notification would be in the public interest should include consideration of whether notification would be effective in assisting affected individuals to mitigate their own risk (see above at 2.1).

2.7 Clause 26WD Commissioner may direct entity to notify serious data breach

If the approach recommended by the ALRC referred to in section 1.2 of this submission were adopted this would facilitate devising a process for resolving cases where the Commissioner and the APP entity disagreed that a serious data breach had occurred.

Appeals

The proposed additions to section 96 of the Act provide that a decision by the Commissioner to refuse an application for an exemption from the obligation to notify (Cl.26WC(10)), or to direct an APP entity to notify affected individuals (Cl.26WD(1)), may be appealed to the Administrative Appeal Tribunal for merits review.

To ensure that all the salient facts are taken into account in making a decision, the ABA suggests that the OAIC be required to send an APP entity a 'show cause notice' i.e. outlining the basis for a proposed decision and providing the APP entity the opportunity to present its explanation for why such a decision is inappropriate or unjustified.

Alternatively, the ABA suggests that, to ensure that APP entities are fully able to exercise their appeal rights, that the Bill require the Commissioner to provide reasons for a decision made under s26WC(10) or s26WD(1). The ABA notes that this approach is currently taken in the Privacy Act in respect to determinations under section 52. Specifically, section 52(2) provides that "([t]he Commissioner shall, in a determination, state any findings of fact upon which the determination is based".

3. Further consultation

The ABA commends the Department for extending its consultation arrangements with the opportunity for the private sector to discuss and raise questions with the Department which the ABA has taken.

From the discussions with the Department on 22 February 2016 there were several matters that the Department agreed to take away from the discussions to work through and consider possible changes to provisions of the Bill. The ABA welcomes this initiative and looks forward to hearing from the Department as these developments take form.

Yours sincerely,

[signed]

Ian Gilbert
Director Banking Services Regulation
[contact details redacted]