AUSTRALIAN
RETAIL
CREDIT
ASSOCIATION

8 March 2016

Attorney Generals' Department

Dear ,

ARCA welcomes the opportunity to provide a submission in relation to the *Privacy Amendment (Notification of Serious Data Breaches) Bill 2015*.

The Australian Retail Credit Association (ARCA) is the industry association for organisations involved in the disclosure, exchange and application of credit reporting data in Australia. ARCA's membership includes Credit Reporting Bodies (CRB) and Credit Providers (CP).

ARCA Members have expressed concern with a number of elements in the Bill. These concerns are set out below and relate to:

- The proposed regulation-making powers.
- That entities may not be aware of a breach.
- 30 day period for assessment of a serious data breach.
- The concept of 'reasonable grounds' not being adequately defined.
- Provision for joint holders of information.
- Inadequate recourse to directions from the Information Commissioner.
- The inclusive definition of 'harm' is too broad.
- The proposed definition of real risk.
- The need for review.
- A lack of safe harbour for encrypted data.

ARCA believes that these issues should be resolved and recirculated for feedback before progressing any further.

ARCA also notes that many of its Members are also members of the Australian Bankers' Association (ABA). ARCA has reviewed the draft ABA submission on the draft Bill, and

broadly endorses the submissions made by the ABA (many of which are reflected in the submissions set out below).

Regulation-making power not required - *Subsections 26WB(2)(a)(ii) and (c)(ii)*

The Exposure Draft of the Bill includes a limited number of regulation-making powers around the types of data that would automatically constitute a data breach. ARCA submits that it is both unnecessary and unworkable to define the type of information (to which serious data breach relates) by means of regulation. Instead, it recommends that the regulation-making power be removed from the draft Bill in its entirety.

Instead, the type of information covered by the serious data breach provisions ought to be defined by reference to the types of information referred to elsewhere in the draft Bill. In particular, subsection (1) of s26WB already refers to personal information held by an APP entity, credit reporting information held by a credit reporting body, credit eligibility information held by a credit provider, and tax file number information held by a file number recipient. Furthermore, given the intention is to exclude certain types of information in sections 26WC and 26WD, any definition of the types of information should also reflect these exclusions (law enforcement information likely to prejudice the activities of the law enforcement body; information prohibited from use/disclosure by Commonwealth legislation; information already subject to breach notification under the *My Health Records Act 2012*).

Entity may not be aware of breach – *section 26WC*

Section 26WC (1) of the Exposure Draft Bill provides that:

> *"If an entity… 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…* ***ought reasonably to have become so aware****… prepare a statement that complies with subsection (3)".* [Emphasis added]

As it is currently drafted, entities will be required to prepare a statement of serious data breach even though it may not be aware of a breach.

Clearly if an entity is not aware of a breach it will not be possible for that entity to prepare a statement. Noting that the Attorney General's Department has acknowledged this issue in recent consultation, ARCA would recommend that these provisions be amended to ensure that an entity must actually be aware of a breach before being required to prepare

a statement. This amendment could be achieved by removing the reference to 'ought reasonably to be aware/to have become aware' from this subsection.

Further to this issue, as the section is drafted, the concept of that an entity 'ought reasonable to have become aware' implies that entities will be required to assess existing monitoring systems to determine whether they are suitable to detect any serious data breach. Assessment will need to determine whether internal controls are sufficient, or whether externally developed and cost prohibitive detection arrangements will instead be required.

In the event that the 'reasonably aware' wording is retained (even in a modified form) in this section, ARCA recommends that any modified wording first be circulated for comment, and further that consideration be given to the impact of industry meeting this requirement using existing monitoring systems. In this regard, industry should be afforded an opportunity to consider and provide a response to address the impacts of any modified wording, before this section is finalised.

30 day period for assessment of a serious data breach – *subsection 26WC(2)*

Subsection s26WC(2) of the Exposure Draft Bill provides that entities have a 30 day assessment period for reasonable assessment once they become aware, or ought reasonably to have become so aware, of a serious data breach.

ARCA is concerned that this period of 30 days is too short. This is particularly the case when dealing with serious data breaches of a complex nature. By way of example, there will be circumstances where complex cases require specialist information technology forensic investigation or other specialist services. In those circumstances the 30 day period may be inadequate.

Noting that the Attorney General's Department has acknowledged this issue in recent consultation, ARCA would recommend that the 30 day requirement be amended to require notification 'as soon as practicable'.

The concept of 'reasonable grounds' is not adequately defined – *sections 26WC and 26WD*

ARCA Members have noted concerns with the use of the term 'reasonable grounds' (to believe that there has been a serious data breach), which prompts the data breach notification either direct by the entity to an individual (s26WC) or where a belief is held by the Information Commissioner (s26WD).

Of concern is that what constitutes 'reasonable grounds' is uncertain. Given that the notification scheme is predicated on the concept of 'reasonable grounds', it is critical that there is no ambiguity on this definition. Consequently, Members are also concerned that future guidance will need to be provided on the definition. Given the widely reported concerns that the Office of the Australian Information Commissioner has limited resources at its disposal, and the increasing complexity of the matters they regulate, there are very real concerns about whether timely guidance will be provided in a manner that enables industry compliance.

A timetable ought to be set for the development of guidance, consultation and finalisation of that guidance. Furthermore, any such guidance must be in place before commencement of the data breach regime.

Notification requirements where information jointly held – *sections 26WC and 26WD*

Sections 26WC and 26WD of the Exposure Draft Bill require an entity to provide its notification 'to each of the individuals to whom the relevant information relates', with the only exception to this notification requirement occurring where such notification is not practicable.

However, ARCA Members have noted that there may be circumstances where entities have arrangements where personal information is jointly held. These arrangements are not adequately addressed in the Draft Bill. Indeed, the provision of multiple notifications to joint information holders may result in 'notification fatigue'.

ARCA recommends that the serious data breach notification mechanism be amended to enable notification requirements for joint holders of information to be met by notification to one of the joint information holders, where that is an appropriate outcome for consumers.

Inadequate recourse to directions from the Information Commissioner – *section 26WD*

Section 26WD provides that when actioning a data breach, the Information Commissioner can direct an entity to notify them of the circumstances surrounding a breach. This direction can occur where the Information Commissioner believes on reasonable grounds that a breach has occurred.

It should be noted that there may be circumstances where an entity may not agree that notification is required. This disagreement may stem from any of the limbs required to trigger the notification - including the risk threshold, the harm threshold or another aspect.

This direction from the Information Commissioner is proposed, by virtue of amendments to Schedule 1 Item 4 after paragraph 96(1)(b), to only be subject to review by the Administrative Appeals Tribunal. This review process is at best cumbersome and does not provide a multi-tiered appeal process that encourages swift dispute resolution (where a dispute exists between the entity the subject of the direction and the Information Commissioner).

Further to that point, the current draft Bill does not provide for or require the Information Commissioner to engage with an entity before determining that it believes on reasonable grounds that a breach has occurred.

In these circumstances, the Commissioner would direct an entity to prepare a statement of serious data breach – even though that entity may not agree that one has occurred. This requirement should be amended to provide a process requiring the Commissioner to notify an entity that it is considering an instance of a potential breach. In such an instance, an entity must be given an opportunity to investigate and respond. This approach would encourage a graduated system of dispute resolution and provide for procedural fairness.

ARCA believes that in its current draft form, the notification system proposed under s26WD is not workable without enabling this graduated system through further consultation with industry.

The inclusive definition of 'harm' is too broad – *section 26WF*

ARCA Members have expressed concerns about the concept of *serious* harm – and more specifically the examples of harm that are included in section 26WF of the Exposure Draft Bill. In particular, the inclusion of *psychological* and *emotional* harm (26WF (b) and (c)). We note that these two harms are new additions to the proposed scheme and are in addition to the concept of physical harm.

The inclusion of *psychological* and *emotional* harm is of concern, primarily because requiring entities to identify the possibility of these concepts of harm is likely to lead to increased complexity and will be difficult to administer. Both psychological and emotional harm are concepts which are largely subjective and every individual will have a differing threshold of serious psychological and emotional harm. This means that the presence of this harm will often only be able to be determined by the individual actually experiencing it. Given the experience of this harm will trigger a notification requirement (which will then be the first contact between entity and individual), it is difficult to see how an entity will be able to detect and comply with the requirements around these types of harm. In any event, these types of harm will be unlikely to occur without the presence of other types of harm, for instance, harm to reputation so the inclusion of these types of harm in the definition may have limited utility.

For these reasons, ARCA Members seek the removal of the concepts of *psychological* and *emotional* harm from the section 26WF list of types of harm.

Definition of "real risk" – *section 26WG*

ARCA Members have concerns with the concept of 'real risk' and consider the current definition (a risk that is not a remote risk) is unhelpful. It is noted that in recent consultation with the Attorney General's Department, it was noted that consideration is being given whether or not to amend the definition of 'real risk'. The Department suggested that it was considering changing the current definition from a real risk to 'likely' or 'probable' risk.

ARCA considers that while the terms 'likely' or 'probable' risk provide a greater level of certainty of meaning and application than 'real' risk, these terms still remain vague and uncertain in application. ARCA supports the ABA's submission that guidance and case study examples (set out in the Bill or developed and published by the OAIC well in advance of commencement) are required, to avoid the inevitable issues that will result from the uncertain nature of the current or amended wording. This guidance must be available and finalised in a timely manner prior to the commencement of the data breach regime.

Need for review – *not covered in draft Bill*

ARCA recommends that provision be made for a review of the proposed regime three years after it has commenced operation. The terms of reference for such a review should be developed in consultation with industry and other stakeholders. This review would ensure it is effective and responsive to the then-current operation of the proposed regime. A

review could determine, for example, the effectiveness of definitions, the need for regulation-making powers, and the interaction between the proposed regime and other regimes that relate to other types of sensitive information, including health information.

No safe harbour for encrypted data – *not covered in draft Bill*

ARCA Members are concerned that the draft Bill does not make any provision for encrypted data to be excluded from data breach notification requirements, that is, there is a lack of a safe harbour for encrypted data. There is concern that the draft Bill is unlikely to provide the certainty required to deliver a true safe harbour arrangement for encrypted data.

The concept of safe harbour for encrypted data has formed part of the overseas data breach regimes. In particular, encrypted data has been exempt from California's notification scheme since its inception in 2003[1]. The first significant change to that arrangement occurred in January 2016 when amendments to the Californian scheme commenced. These amendments re-defined "encrypted" to where it is "rendered unusable, unreadable, or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security."

The Australian Law Reform Commission (ALRC) in its review of Australian Privacy Law, considered the Californian exception for encrypted data, and recommended:

> "the provisions should state that, in determining whether there is a real risk of serious harm, consideration should be given to whether the specified personal information was encrypted adequately. The requirement that encryption be 'adequate' implicitly requires that the encryption key was not also acquired by the unauthorised person. In other words, encryption will not be adequate where there is an easy means of decoding the information. This phrasing also avoids any need to specify exactly what type of encryption is adequate. An assessment of adequacy will depend on the circumstances of the case, taking into account matters such as the type of personal information, the nature of the agency or organisation holding it, and the risk of harm that would be caused by its unauthorised acquisition. The Privacy Commissioner should issue guidance on the type and standard of encryption he or she generally will consider adequate.[2]"

In light of both the ALRC's views and the established safe harbour laws within California, it is ARCA's strong view that such a safe harbour exception for encrypted data should

[1] CA Civil Code, ss 1798.82

[2] The Australian Law Reform Commission, "For Your Information: Australian Privacy Law and Practice (ALRC Report 108), 2008, at 51.92

explicitly be provided in the Australian data breach notification regime. A safe harbour for the effective encryption of data would provide a material and tangible incentive to improve data storage security arrangements.

Any such proposal would need to acknowledge the differences between the Australian and Californian system. For example the Californian construct of "generally accepted in the field of information security" would act to exclude most custom and proprietary encryption algorithms – whereas in Australia, as indicated by the ALRC's comments, it may be more appropriate that the adequacy of encryption is addressed by a requirement for an entity to take reasonable steps to encrypt the data to reflect the type of data, the entity holding the data and the risk of harm in acquisition (and decoding) of the data.

If you have any further questions regarding submission, please contact me or ARCA Public Affairs Manager James Newbury.

Yours sincerely,

[Signed]

Matt Gijselman

Head of Government, Regulatory & Industry Affairs