Australian Finance Conference ABN 13 000 493 907 Level 8, 39 Martin Place, Sydney, 2000
Telephone: (02) 9231-5877 Facsimile: (02) 9232-5647 e-mail: afc@afc.asn.au www.afc.asn.au

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

4 March 2016

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

Dear Mr Walter

EXPLANATORY DRAFT: PRIVACY AMENDMENT (NOTIFICATION OF SERIOUS DATA BREACHES) BILL 2015

The Australian Finance Conference (AFC) appreciates the opportunity provided by the Government through your Department to assist shape the framework to implement its policy of imposing a legislative obligation in the Privacy Act to report the release of personal information in breach of a regulated entity's secure holding.

AFC Background

The AFC is a finance industry body comprising 60 plus member companies (list attached). Our Members include finance companies, specialist equipment financiers, general financiers, banks and credit unions and the three major consumer and business reporting bureaus providing (or servicing) consumer, commercial (including small business) and wholesale credit facilities to customers.

Personal information is an asset critical to the business of our Members and is handled accordingly as a matter of sound and prudent commercial practice. Consequently, while compliance with the Privacy Act remains relevant to the overall operations of our Members and their management of regulatory risk, it aligns and largely reflects existing business practices.

Mandatory Breach Reporting – Policy & Implementation

Our Members acknowledge that with advances in technology and to meet customer demands and expectations, organisations are storing vast amounts of identifying information electronically. And that this medium brings with it risk challenges that may see an organisation, even one with the highest and most sophisticated levels of data security, exposed by an unauthorised attack on their system or loss through human inadvertence that results in the release of personal information with the potential for significant financial, reputational or other damage to the individual and the regulated entity. And, further, that the voluntary data breach reporting framework that has been developed by the OAIC while a useful self-regulatory measure, may not be sufficient to ensure entities operating in other sectors act to address data breaches with the requisite priority to mitigate consumer risk. A regulatory solution targeted to protect the consumer in a manner that minimises compliance burden and therefore cost for regulated entities appears appropriate.

We understand the key objective of the policy to be implemented in the draft Bill is consumer protection and is about a timely alert to give an individual the opportunity to take steps to

mitigate potential identity fraud damage that may arise from the information's release. Further, that implementation is intended to be as simple and straightforward as possible for our Members and other regulated entities in line with the Government's commitment to red-tape reduction and best-practice regulation making.

The AFC acknowledges and supports the balanced outcome that the Government is looking to achieve through this policy initiative.

The AFC also commends the Government on the consultative approach taken to facilitate feedback. This includes the length of the consultative period provided to enable our Members and other stakeholders to fulsomely consider and respond to the draft. We have also appreciated the opportunity for engagement with the Department, in particular the teleconference with yourself and others within your Team and other industry stakeholders a week or so ago, to assist identify key areas with the draft Bill that may require further clarification or revision.

Summary of Key Areas
By way of confirmation and to assist with the Government's consideration of areas of possible revision of the final version of the draft Bill, the key areas of concerns of the AFC are summarised below:

What "Information" is covered + is it within the scope of the Notification Regime?
We note the policy intention is to regulate data that meets the current definition of "personal information" as defined by the Privacy Act and therefore regulated under it. Any references that might potentially capture information that is not 'personal information' are unintended and fall outside the scope of the current regime. Accordingly, we recommend that the draft Bill be revised to remove all references to "other information." For example, references in s. 26WA to "personal information **(or certain other information).** We understand that the Government would agree with the AFC that it is undesirable, unworkable and potentially ultra-vires to have a notification regime under the Privacy Act that extends beyond its current scope and the regime administered under that Act; and therefore would be supportive of revision to remove any unintended outcomes that might put this at risk.

Personal Information – Encryption
In relation to the concept of relevant matters in s. 26WB we note the attempts to ensure that to meet the test information has to be in an electronic form that is intelligible to the ordinary person who has access to publicly available and commonly used software. While this goes some way to providing compliance comfort for our Members, they suggest additional clarification may be useful. In this regard they note recent amendments made to the data protection laws in California (Ca. Civ. Code § 1798.82) in particular A.B. 964 and S.B. 570 which included a specific definition of information that is "encrypted" so as to presumptively exclude it from notice and disclosure requirements. Information is "encrypted" if 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*." Further, a breach of encrypted information is presumed to be outside the data breach notification requirements. However, further consumer protection has been provided by ensuring that the presumption is rebuttable, specifically so if the encryption code or method is also compromised. We suggest that the Government consider revising the draft Bill to introduce further clarification in relation to encrypted data adopting a similar approach to the Californian law.

Regulation-Making Power
The AFC also notes the potential for Governments in the future to prescribe via regulation particular types of personal information the breach of which would be immediately deemed to

be serious and trigger the notification obligation on a regulated entity. While acknowledging the policy design intention is about future-proofing the law, we would again appreciate confirmation in explanatory material that the intention is:

- That this power would only be used within the confines of the data captured within the statutorily defined concept of "personal information"; and
- That the Government has not identified any particular data sets for inclusion in a regulation at this time.

Compliance Certainty – Statutory Definitions

We note that the definition of concepts like "real risk", "serious harm" and "harm" are essential to setting the parameters and therefore compliance obligations for our Members and other regulated entities. It is therefore critical for these concepts to be clear and operationally efficient and effective. In saying this we note the challenge for the Government in defining these terms in a way that provides that compliance certainty taking into account the breadth and complexity of data management in the context of our Members' operations but equally for entities in other sectors.

We acknowledge the value of the inclusion in s. 26WB(3) of a range of examples of matters that our Members may wish to take into account when determining whether there is a "real risk of serious harm". And support further guidance from your Department or the OAIC to provide greater clarity and compliance comfort around this concept.

We also understand some revision of some of these terms is being considered and provide the following feedback in support.

Real Risk

We support revision of the definition to use language that better describes a measure of assessment that is readily operationalised. In our view, the concept of probability best meets this need. For example, our suggestion would be to revise the definition as follows:

> ***s. 26WG Real Risk***
> *For the purposes of this Part,* ***real risk*** *means a risk that is probable not a remote risk.*

We would also suggest for the same reason and in the interests of consistency, that the term "is likely in s. 26WB(2)(b)(i) should be replaced with "will probably."

Harm

The AFC acknowledges that in the absence of a statutory definition that statutory interpretation would see this term being giving meaning in line with common law principles. Further that concepts like psychological or emotional harm may be encompassed within those principles. However, the inclusion of these concepts in the proposed statutory definition (s. 26WF Harm) has highlighted the compliance challenge and complexity that our Members would face when attempting to assess whether the threshold to notify had been triggered. It has also highlighted the basis on which such an assessment should be made, though we acknowledge the intention is that it be judged from the position of a "reasonable person" rather than one susceptible to these forms of harm. And that this might be better clarified in the Explanatory Material to accompany the Bill and Guidance to be development by your Department or the OAIC. Ideally, the AFC suggests that because of the compliance uncertainty that these terms create our preference would be deletion from the definition of harm in s26WF.

Notification Obligation

If the Government proposes to retain a specific timeframe (eg currently 30 days) to be imposed on our Members to assess and take requisite notification action, we submit that the trigger from which that timeframe commences must be clear or easily identifiable. Therefore, the trigger must be based on concepts that are within the actual knowledge of the Member.

As a consequence, we submit that a trigger based on concepts like when the Member "ought reasonably to be aware" are not appropriate because of necessity they effectively require consideration from a lens outside the entity looking objectively backwards at the particular circumstances to make an assessment. This 'hindsight' approach to the trigger presents practical difficulties with compliance which is at odds with the commercial and operational realities of our members.

In our view, the better approach may be that the notification obligation should turn on either the Member:

- Being aware of information that might lead them to conclude that there has been a breach; or
- Being aware of information that may lead them to **reasonably suspect**[1] that a breach has occurred and having an obligation to investigate to determine.

And in both cases having adequate time from the time that they become aware or reasonably suspect there has been a breach to undertake an assessment to:

- Confirm that a breach has occurred; and
- Be able to measure the "seriousness" of the breach including the probability of harm to individuals to whom the information relates; and
- If determined to be serious, to be able to determine who it would be appropriate to notify and how;

before then being obliged to take action to notify. In this regard we note the work being undertaken by the OAIC on a *Guide to Developing a Data Breach Response Plan* and the value when finalised that will likely have to the assessment framework component of these amendments; including who should conduct the review or assessment.

If an entity is not aware or has cause to suspect but a third party observer looking at the particular circumstances would have and therefore, arguably, the entity "ought reasonably to have been aware" of the breach, this may be a matter that goes more to assessments around the culpability of entity for the breach and damage that might flow rather than a process of notification. Or, it may be better dealt with under the powers available to the Commissioner to require a regulated entity to notify if the Commissioner becomes aware of circumstances of a serious data breach, or of circumstances which merit further investigation to determine whether a serious data breach has occurred, and in either case oblige the regulated entity to take requisite notification action. The AFC therefore recommends omission of the concept of "ought reasonably to be aware" from the process of notification imposed on the regulated entity.

[1] We would suggest that 'reasonable suspicion' be underpinned in the Explanatory Memorandum by reference to the APP entity having implemented systems and processes as part of the APP 11 obligations that are materially consistent to an industry acceptable standard of security which would include industry standards regarding the monitoring and detection of intrusions or breaches (e.g. NIST Cybersecurity framework, ISO/IEC 27001 and 27035 etc).

Building from these comments, we suggest the following revision, for example:

> ***s. 26WC Entity must notify serious data breach***
>
> *(1) If an entity is aware, or has reasonable grounds to believe and on further investigation determines, that there has been a serious data breach the entity must as soon as practicable after becoming so aware, or so determining, as the case may be:*
>
> *(a) prepare a statement etc…*

And in our view, if a specific time frame to notify is retained that it should apply to the notification process rather than the assessment and should not commence until our Member has had the opportunity to investigate and assess and have determined that there has been a serious data breach. It is only once this decision has been made that it might be appropriate to put some restrictions around the process in relation to time limits to alert the relevant persons. And again for reasons that follow, a black-line approach of a set number of days with no availability of extension is not in our view appropriate in relation to this issue.

30 Day Time Period

In relation to a set or specific time-period for an assessment and (eg currently 30 days) – we would further note the challenge for the Government in arriving at a time that appropriately catered for the myriad of varying fact scenarios of potential serious data breaches and requisite assessments by regulated entities (and others) that would be required.

For example, we are advised by our Members that some assessments of more complex breaches may take longer than 30 days, particularly, for financial institutions that have large customer bases. Further, there are instances of sophisticated intrusions which require significant time given their complexity to assess and which an entity may not be aware of until well after the fact. For serious breaches the assessment may also require the regulated entity to notify and comply with other obligations and processes under their cyber-security insurance. And further, the volume of individuals and likely disparate geographic locations and normal means of communication with the Member may challenge a notification process being met in a 30 day window.

In our view the notification trigger and assessment period needs to take into account the detrimental effects of premature notification on regulated entities and individuals before fulsome investigation and assessment of the breach has been undertaken. Regulated entities may suffer needless reputational and financial harm and individuals may be unduly alarmed for no good reason.

Finally, given the principles-based nature on which the Privacy Act has been developed and the utilisation of concepts like “taking reasonable steps in the circumstances” it appears at odds to introduce a black-line approach of a set-time frame for response in the proposed amendments. For reasons given, the AFC recommends removal of specific time-frame and replacement with an approach based on the concept of “reasonableness” (eg must take reasonable steps to .. notify) more akin to other elements of the law and more likely to be able to be managed to cover all potential scenarios from the most simple to the most complex circumstances of serious data breach. The concept of reasonable steps includes an assessment of a time-frame for response in the particular circumstances without the necessity of specifying one that may not be appropriate.

Notification Obligation – Commissioner’s Notice – Application Declined

Removal of a set-time frame and replacement with a “reasonableness” concept would also assist overcome questions around how the set-time frame should be managed in circumstances where our Member may have determined that there has been a serious data

breach but the circumstances may warrant it to apply to the Commissioner for exemption from giving individuals notice. We understand there is some compliance uncertainty with how the time would be dealt with if interrupted by our Member applying to the Commissioner and the Commissioner declines from approving the exemption. In this circumstance, a reasonable length of time should be given to the regulated entity to comply with its notification obligations.

Notification Obligation – Commissioner's Notice – Test for Approval

The AFC notes the original recommendation by the ALRC in its FYI Report 108 allowed the Commissioner to make a decision to exempt not just based on a decision around the public interest, but also, importantly as an alternate, taking into account the interests of the affected individual (Recommendation 51-1 (d)). We submit that s. 26WC (7) should be revised to include the ability for the Commissioner to take into account the interests of the individual when making a decision whether to exempt the giving of notice as a separate and alternate ground of exemption from the public interest basis currently included.

We also believe that balancing the interests of the public, individual and the regulated entity to be of paramount importance in this legislation. While, in general, the development of a mandatory breach reporting regime engenders greater trust within the information privacy system, there are certain circumstances where it does not. For example, where notification (and the concomitant publicity) would encourage further attempts at 'hacking' or exploitation of a vulnerability. While there may be arguments that would see these circumstances fall within the "public interest" concept; in the interests of compliance certainty we submit that these exceptional circumstances, should be catered for in this provision in the draft Bill.

Notification Obligation – Relationship with Individual ceased

We understand that the Privacy Act does not operate to protect the personal information of an individual once he or she has died. We therefore understand that our Member would not have a notification obligation in relation to a serious data breach relating to personal information of a customer that has died prior to the obligation having been triggered. We suggest it would be useful for this to be clarified in either material accompanying the amendments or guidance from your Department or the OAIC.

We also suggest that it would be useful if that clarification could also encompass situations where the relationship has ceased not by death but other circumstances (eg customer has repaid the loan) and consequently our Member may no longer have up-to-date contact information to notify through. We acknowledge that alternate notification processes have been provided for in the draft Bill to cater for these type of circumstances (eg publishing a statement on a website and drawing people's attention to its content. However, additional guidance would be useful.

Notification through Website + Publication of Statement Content

We note the intention to facilitate a means of notifying where it may not be practicable to directly notify affected individuals directly. And as we understand a two stepped compliance obligation is intended; a requirement to publish the statement on the website coupled with an obligation to publicise the statement contents elsewhere.

We acknowledge the objective of the two-layers as noted in the draft Explanatory Memorandum is to "*increase the likelihood that the serious data breach described in the statement comes to the attention of the affected individuals.*" However, while understanding and supporting this objective, we query whether how that aspect of the policy has been designed in the amendments is effective.

For example, we suggest that it should be open to our Members to publicise the statement utilising whatever means they believe appropriate for the circumstances, for example notification in a more secure online banking / service center environment. And that more than one means might be appropriate (eg in newsprint and e-media). We could also understand a regulated entity might have an obligation to publicise beyond publication of the statement on their website. However, we submit that the obligation should be to draw individual's attention to the publication of the statement on the website rather than obliging an effective re-iteration of the content of the statement on the website in another publication. The obligation to do the latter effectively removes the need for the former requirement to publish on the entity's website.

Notification Statement s. 26WC(3)

The AFC suggests that further guidance from your Department or the OAIC to clarify how extensive the recommendations about steps to mitigate damage that are required to be given to the individual would be useful and the potential consequences if a particular recommendation is not included.

Who has the obligation to notify?

We again note the complexity that the digitisation of information coupled with often complex business models brings to the design of the regulation to implement the Government's policy. This is true for our Members whether the product or service being distributed is financial or whether they are merely participants in part of broader supply of a non-financial product or service (eg, the acquisition of an asset on finance).

It is not uncommon for our Members to be part of such a distribution network. They may offer a credit card facility, for example, that allows a customer to purchase goods or services on credit. Or they may facilitate the access by the merchant to sales to a customer on credit by accepting transaction using those facilities.

Should the merchant collect and retain in its records personal information from a customer (including the credit card details) which is released to an unauthorised third party (eg hacker), we assume that the merchant would have the obligation to notify the customer. However, if the merchant meets the statutory definition of a "small business" then they may be exempt from compliance with this obligation. They may alert our Member as the card-issuer to the fact that customer's personal information has been compromised. Our Members may therefore be challenged with questions around whether they separately have an obligation to notify their customers to be compliant with the law's requirements. Or, regardless, if they become aware independently that one or more of their customers credit card information has been compromised whether they have an obligation to notify despite the fact that it was not their information holdings that had been breached, but those of a third party containing information material to our Member's customer also.

And further, some of our Members have a number of white label credit provision / retail partnership arrangements. While, in most cases it will be clear who holds personal information in those arrangements, it may also be the case that there are arrangements where personal information is jointly held, particularly, for entities in the payments value chain noted above.

In those circumstances of "joint holding" where there has been a serious data breach the AFC recommends that a provision is included in the draft Bill to facilitate a means by which the obligation to notify which arguably falls on both, may be discharged by one of the parties. We acknowledge that this could be dealt with in contractual arrangements between our Members and their service providers. However, in the AFC view, a legislative provision for such circumstances would give greater compliance clarity and regulatory safety for our

Members and other regulated entities more generally. Specifically, it would be beneficial to make it clear that a notification by an entity in respect of a potentially serious data breach that involves multiple entities will be taken to be a notification under the Act by the other entities involved.

Transition Period

We note and commend the Government for indicating an intention to give a 12 month transition period from the date of assent to facilitate the implementation processes that will flow to our Members from the amendments.

We note that there are a range of areas that it may be useful for our Members and others to have further guidance from the OAIC. To maximise the potential for implementation to be designed taking that guidance into account, we encourage the Government to provide the OAIC with adequate resources to facilitate the work being undertaken as soon as possible following the passage, enactment and consequently final form of the amendments being available to them to build from.

We would be happy to discuss our comments in further detail, or provide further information to assist the Panel. Please feel free to contact me through the AFC Office 02 9231 5877 or via email[redacted]

Kind regards.

Yours truly

[redacted]

HELEN GORDON
Deputy Executive Director

Attachment:
AFC Member List

AFC MEMBER COMPANIES

AlliedCredit
American Express
ANZ t/as Esanda
Automotive Financial Services
Bank of China
Bank of Melbourne
Bank of Queensland
BMW Australia Finance
Branded Financial Services
Capital Finance Australia
Caterpillar Financial Australia
Classic Funding Group
CNH Industrial
Commonwealth Bank of Australia
Credit Corp Group
Custom Fleet
De Lage Landen
Dun & Bradstreet
Experian Asia Pacific
Eclipx Group
Finance One
FlexFleet
FlexiGroup
Genworth
HP Financial Services
HSBC Bank
Indigenous Business Australia
International Acceptance
John Deere Financial
Kubota Australia Finance
Komatsu Corporate Finance
Latitude Financial Services
Leasewise Australia
Liberty Financial
Lombard Finance
Macquarie Equipment Rentals
Macquarie Leasing
Max Recovery Australia
ME Bank
Mercedes-Benz Financial Services
MetroFinance
Nissan Financial Services
Once Australia t/as My Buy
PACCAR Financial
Pepper Australia Pty Ltd
Qantas Credit Union
RABO Equipment Finance
RAC Finance
RACV Finance
Ricoh Finance
Selfco Leasing
Service Finance Corporation
Sharp Finance
SME Commercial Finance
St. George Bank
Suttons Motors
Suncorp
Thorn Group/Radio Rentals
Toyota Financial Services
Veda
Volkswagen Financial Services
Volvo Finance
Walker Stores
Westlawn Finance
Westpac
Wex Australia
Wingate Consumer Finance
Yamaha Finance

<u>Professional Associate Members</u>:

CHP Consulting
Clayton Utz
Dibbs Barker
Henry Davis York
White Clarke