AUSTRALIAN BANKERS' ASSOCIATION INC.

Ian Gilbert
Policy Director

AUSTRALIAN BANKERS' ASSOCIATION INC.
Level 3, 56 Pitt Street, Sydney NSW 2000
p. +61 (0)2 8298 0406 Ext **f.** +61 (0)2 8298 0402

www.bankers.asn.au

20 June 2013

Tim Bryant
Inquiry Secretary
Senate Standing Committee on Legal and Constitutional Affairs
PO Box 6100
Parliament House
Canberra ACT 2600

Email to: legcon.sen@aph.gov.au

Dear Mr Bryant,

Privacy Amendment (Privacy Alerts) Bill 2013

The Australian Bankers' Association (ABA) appreciates the opportunity to provide information to your Committee to assist with its inquiry into the Bill.

1. Preliminary comments on the Bill

The following comments are intended to assist the Committee in understanding some of the context for this Bill.

On 30 November 2012 the ABA provided its views on the government's Discussion Paper to inform the government's response to the Australian Law Reform Commission's (ALRC) recommendation 51-1.

The ABA queried then why this proposal had been brought forward rather than together with the government's complete response to its second stage consideration of the ALRC's recommendations in its May 2008 Report 108. The apparent urgency on the part of the government in bringing only this recommendation forward remains unclear.

The ABA mentioned in its November 2012 submission the voluntary scheme of data breach notification initiated by the Privacy Commissioner which has been operating for several years. The government had acknowledged in its November Discussion Paper that one of the arguments supporting the status quo is that the voluntary scheme had been operating effectively and that more entities were using the voluntary guidelines provided by the Privacy Commissioner.

The ABA had considered this to be an important factor for the government to consider in completing its regulatory impact assessment of this proposal including why at this stage this matter cannot await the government's second stage response to the remaining ALRC recommendations that was announced by the then Minister in October 2008.

In contrast, the Minister's Second Reading speech states on this aspect –

"The Commissioner has voluntary guidelines encouraging notification, but is concerned that many data breaches – perhaps a majority – are going unreported. The Bill stops this gap in Australia's privacy laws."

The ABA's November 2012 submission also mentioned three other aspects that are considered relevant to the government's decision and the possible impact on the business community. They are:

1. The Government is taking a far wider scope for mandatory notification than has occurred so far overseas.
2. There is an absence of empirical evidence to suggest that notification of itself has been effective in reducing the likelihood or impact of a data breach in overseas countries and raises questions whether filling a perceived "gap" in Australia's privacy laws is warranted.
3. Australia has and will continue to have robust privacy information protection laws including increased powers of the Privacy Commissioner to enforce those laws that of themselves are strong inducements to Australian organisations to comply.

There is the further element that under the Bill a business such as a bank may incur the liability for a data breach and the subsequent compliance obligations under the Bill despite the fact that the data breach was not as a result of any act or failure of the business but by another entity. A data breach can occur as a result of a customer's own act, for example, by disclosing a financial product access code to a third party or as a result of the inadequacy of a merchant's security measures which provides payment services to its customers who also are customers of a bank or other financial institution.

The ABA has no objection to banks providing appropriate notification to the Privacy Commissioner in the event of a serious data breach. Deciding whether a bank should provide notification to its customers who are assessed at real risk of serious harm and at risk of being significantly affected by the breach should take account of the exercise of judgment by the bank involved and its attention to the management of its customers' interests. This discretion and a bank's assessment prior to exercising its judgment will be based on a number of factors which should be reserved for the bank.

2. Complying with the Bill if passed

2.1. Definition of "real risk of serious harm"

What is a "real risk of serious harm"? The meaning of this relevant criterion in the Bill will be unclear in an entity's operational environment. The fact that the "real risk" is limited only to those individuals who are "significantly affected" by the breach does not help to clarify the primary criterion that there must be a real risk of serious harm.

The issue for entities is going to be determining what to report and what not to report. Experience with mandatory breach reporting to a regulator in unrelated areas of business activity indicates that entities often will need to seek legal advice whether there is an obligation to report a breach. Often the legal advice is uncertain with a decision by the entity to report irrespective of whether this is required by the law.

A more certain threshold test of what is a *serious data breach* which would result in a real risk of serious harm could strike an appropriate balance between the interests of customers while minimising the impact of notification on businesses. It could allow organisations to adopt a risk based approach.

However, clause 26ZF defines of "real risk" as "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 Privacy Commissioner's Data Breach Notification Guide. This would be in line with ALRC recommendations and the international approach. ALRC recommendations include: "reasonable degree of likelihood"; "real and substantial risk"; "real and substantial danger".

That said, 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 applying, conservative institutions like banks will generally adopt a risk adverse approach to notification and take a narrow interpretation of what constitutes a 'real risk of serious harm'. These interpretations need to be of a high enough standard to avoid notification fatigue (and resourcing issues at the OAIC) to avoid notifications to the Privacy Commissioner or customers where there was simply any risk of serious harm.

If the Bill becomes law, the ABA considers it is critical for the Privacy Commissioner to be required to develop guidelines for industry on this matter. This direction to the Privacy Commissioner should be included in the Bill or Explanatory Memorandum.

In developing this guidance on what should and should not be reported, the Privacy Commissioner should take into account examples provided by industry of what can actually occur in practice.

Further, there is a particular concern that the Bill contemplates there will be regulations prescribing a type of personal information, the unauthorised access, disclosure or loss of which will automatically constitute a *serious data breach* without necessarily involving any risk of serious harm to the individual concerned who under additional regulations could be taken (presumed) to have been significantly affected by the breach.

There has been no consultation on what may be contained in these regulations or whether there is any intention to develop these regulations. The Explanatory Memorandum to the Bill states in respect of this regulation making power in clause 26X(1)(d)(ii) of the Bill –

> *"The ability to make regulations to specify particular situations that may also be serious data breaches is intended to provide flexibility to deal with data breaches that may not reach the threshold of a real risk of serious harm but should nevertheless be subject to notification. These could include the release of particularly sensitive health information such as health records which may not cause serious harm in every circumstance but would be subject to the highest level of protection."*

This statement contradicts the policy basis of this Bill that only a "serious data breach" as defined in the Bill to the extent that an individual is "significantly affected" by the breach must be reported to the Commissioner and the individual notified accordingly.

There is also a risk that there may be types of information (e.g. bank details) prescribed in the regulations that may always warrant notification.

The ABA suggests this is an unsatisfactory approach to business regulation. Organisations will have to adjust existing compliance systems for reporting and notification of serious data breaches significantly affecting identifiable individuals without the knowledge of the scope of other circumstances which are later defined by regulations. The ABA believes in seeking to extend the scope of the Bill after it has been considered by the Parliament and with no limitation on the exercise of this regulation-making power the government is not acting consistently with the accepted tenets of best practice regulation.

Therefore, the Bill should include a mandatory obligation on the minister to consult on any proposed regulations and to specifically take into account industry submissions on the timing for commencement of those regulations.

2.2. Notification to affected individuals

As a general comment the financial impact for banks is dependent on what will constitute "a real risk of serious harm" which is discussed above.

The real cost to banks involved with this legislation is the actual notification to affected customers. If a bank, for example, suspected a possible data breach of part of its customer base, it may need to communicate with many individuals even if they are only those who have been significantly affected by the data breach. As already mentioned the breach may have arisen beyond the bank's control. For organisations with large customer bases, the notification requirement may result in a disproportionate cost to the organisation compared with the possible harm caused by the breach.

Further, the Bill is unclear in what circumstances a bank would be required to notify affected individuals where, for example, a third party such as a merchant is responsible for the unauthorised access to or disclosure of its customers' credit card data held by the merchant. These data also will be held by the relevant bank. Yet again, some of these details possibly may be held by a range of other entities including other merchants and possibly government agencies. Is it the case that these other entities would be obliged to notify affected individuals and how would duplication of these notifications be avoided so as not to confuse or unnecessarily concern those significantly affected individuals?

The Bill should make it clear on which entity responsibility for notifying significantly affected individuals falls including any change in that obligation when the entity that was responsible for the data breach which, for example, lost or disclosed the information, has only incomplete information. For example, the entity may have an individual's name and credit card number, but no contact details for the card holder who is the significantly affected individual.

While this could be covered in Privacy Commissioner's industry guidelines, these guidelines are no substitute for compliance with the law. The ABA considers that the Bill should be amended to cover these situations.

It is important that the reporting and notification provisions in clause 26ZB of the Bill provide certainty for entities in complying with these requirements. As currently drafted clause 26ZB triggers an entity's reporting and notification obligations once the entity has formed a belief on reasonable grounds that a serious data breach has occurred. The entity must then as soon as practicable take steps to comply with the section. The Bill as drafted does not directly deal with the situation where an entity discovers a breach but does not at the time know the scope of the breach and therefore how many and which individuals will be significantly affected. An entity that fails to notify all significantly affected individuals as soon as practicable after becoming aware of the breach for this reason could arguably be at risk of breaching mandatory breach reporting requirement. The Bill should make it clear that the timing of the reporting and notification obligations is conditioned by the time that an entity reasonably requires to identify the scope of the breach and the individuals that are significantly affected by the breach.

There is a critical element of the notification model in the Bill that is missing because it is unclear what "general publication conditions" will mean if these conditions are satisfied. Without this definition, the real impact of the Bill cannot be assessed because the meaning of this expression will be covered by a regulation-making power in the Bill. Regulations dealing with this aspect have not been provided with the Bill. The administrative and compliance implications and costs for banks and other entities will depend upon when organisations are able to notify data breaches by public announcement, rather than having to individually write to each affected customer. This will also have an effect on the timing for commencement of the Bill, if it is passed.

Proposed regulations defining what is meant by "general publication conditions" in the Bill should be made available.

2.3. Commencement

In the government's confidential targeted consultation (referred to on page 7 Explanatory Memorandum Regulatory Impact Statement) on a more detailed legislative model in April 2013, the ABA considered at that time there would be a benefit if this regime were to commence at the same time as the amendments to the Privacy Act that were given the Royal Assent in December 2012.

In the targeted consultation the ABA had pointed to the lack of certainty concerning the scope of the "general publication conditions" notification model.

This has not been resolved and with the possibility of regulations extending the scope of the Bill the ABA recommends that the commencement date of this Bill, if passed, should be extended to 1 July 2014.

The ABA again thanks the Committee for this opportunity to comment on the Bill.

Yours sincerely,

_____

Ian Gilbert