AUSTRALIAN RETAIL CREDIT ASSOCIATION

The Office of the Australian Information Commissioner

GPO Box 5218

SYDNEY NSW 2001

By email: consultation@oaic.gov.au

23 October 2017

Dear Sir/Madam,

NOTIFIABLE DATA BREACH RESOURCES CONSULTATION

Thank you for the opportunity to provide feedback on the second tranche of draft Notifiable Data Breach (NDB) Resources.

Again, we appreciate the efforts of the OAIC in preparing these resources.

We have the following feedback on the resources:

OAIC Resource: Exceptions to notification obligations

Declarations by the Australian Information Commissioner

The draft resource states that the 'purpose' of a declaration under s26WQ is to provide an exception where the NDB notification requirements would conflict with the public interest. This appears to be an unnecessarily restricted interpretation of that section as the reference to 'public interest' is only one of the relevant factors to which the OAIC is to have regard (see s26WQ(3)).

Relevantly, the Commissioner is to have regard to the public interest (s26WQ(3)(a)) and also 'such other matters (if any) as the Commissioner considers relevant'. We note that the draft resource does not provide guidance on what those matters will include. However, we are concerned that the presentation of the 'public interest' being the sole purpose behind the section is likely to limit the matters that are considered by the Commissioner.

OAIC Resource: Assessing a suspected data breach

When must entities assess a suspected breach?

In placing emphasis on the need for an entity to quickly assess a suspected breach, the resource infers that the decision ought to be made outside of an entity's ordinary incident management

349/1 Queens Road, Melbourne, VIC, 3004 | +61 3 9863 7859 | info@arca.asn.au | www.arca.asn.au | ABN 47 136 340 791

processes, and potentially, by employees that are not in a position to speak publicly on behalf of the entity.

Given the nature of a data breach – particularly one that is significant enough to warrant being an eligible data breach – there will be a real risk of significant reputational and financial loss to the entity resulting from the breach. Many entities will be subject to continuous disclosure obligations and, prior to making information regarding a data breach public, will need to consider whether that information is likely to have a material effect on the price or value of the entity's securities. Such entities will have processes to ensure proper compliance with those obligations that recognise both the urgency of the matter and the need to involve the appropriate decision makers within the entity.

Further, a credit provider that is prudentially regulated (e.g. a bank or credit union) will be under an obligation (see Prudential Standard CPS 220 Risk Management) to maintain appropriate incident management processes. Such processes should themselves ensure that the breach is treated with an appropriate degree of urgency, while also ensuring that the appropriate management are aware of the incident and participate in the response.

We suggest that this resource include an explicit acknowledgment that an entity may be subject to other considerations – including those under prudential standards and continuous disclosure obligations – that must be considered as part of the process to notify an eligible data breach.

OAIC Resource: What to include in an eligible data breach statement

The resource includes an example of a data breach that involved unencrypted or partially encrypted credit card information. One of the suggested recommendations to individuals is to contact a credit reporting body to establish a credit alert. While this may be an appropriate recommendation in response to some data breaches, we are unclear why it would be appropriate for this particular type of breach. We would not expect the release of such credit card information to have a significant risk of identify takeover.

In addition to a credit alert, we suggest that the resource reference the potential for individuals to ask for a ban period on their credit report if there is a risk of identity takeover. We note that a simple way for entities to include this information would be to link to relevant information on the OAIC website, or to the CreditSmart website (www.creditsmart.org.au) established by ARCA.

OAIC Resource: Notifiable Data Breach statement

We have the following comments and questions in relation to the proposed form:

1. The form lists 'gender identity' as a form of sensitive information. We are unsure of the basis for the inclusion of this type of information as an example of 'sensitive information' as it is not included in the list of sensitive information in the *Privacy Act*. We note that this could include any indication of a person's gender that was included in a release of data (including, potentially, the mere inclusion of a relevant honorific such as Mr, Miss or Mrs). We suggest that the form either removes the reference to 'gender identity' or provides more context on what is meant by that term (and how it relates to the definition of sensitive information).
2. The section 'Other entities affected', although stated as being optional, appears to require entities to provide the name and contact details of any other entity affected. This is inconsistent with the guidance in the resource *What to include in an eligible data breach statement*. We suggest that the form more clearly set out the fact that the details of a third party are not required and gives entities the ability to provide the details of the commercial relationship between the entity and the third party. We note that it may be appropriate to

349/1 Queens Road, Melbourne, VIC, 3004 | +61 3 9863 7859 | info@arca.asn.au | www.arca.asn.au | ABN 47 136 340 791

also include the details of the third party in Part 2 of the form (i.e. so that they may be shared with the Commissioner but not individuals).

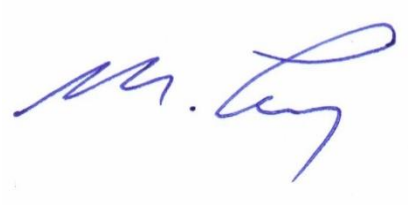
3. Will an entity be required to complete all fields prior to submission of the form? Given the time sensitive nature of the data breaches, it is likely that entities may not have all relevant information immediately and requiring all information to be completed could delay notification.
4. Likewise, we note that the SmartForm version of the form appears to require entities to enter precise dates (i.e. in the format DD/MM/YYYY) which may not be known at the point of notification. These dates (particularly the date the breach was discovered), may be relevant to any subsequent legal action in respect of the breach and entities should not be put in a position to guess those dates at the point of notificaiton. We suggest that entities be given the ability to nominate approximate dates.

OAIC Resource: Guide to OAIC Privacy Regulatory Action – Chapter 9: Data breach incidents

We have no feedback on this resource.

Again, thank you for the opportunity to provide feedback on these resources. If you have any questions on what we have set out above, please contact Michael Blyth, Head of Government, Regulatory and Industry Affairs on 0409 435 830 or mblyth@arca.asn.au.

Yours sincerely



Mike Laing

Executive Chair

Australian Retail Credit Association (ARCA)

349/1 Queens Road, Melbourne, VIC, 3004 | +61 3 9863 7859 | info@arca.asn.au | www.arca.asn.au | ABN 47 136 340 791