

The Office of the Australian Information Commissioner

By post and by email

14 July 2017

Dear Sir/Madam,

#### **NOTIFIABLE DATA BREACH RESOURCES CONSULTATION**

Thank you for the opportunity to provide feedback on the OAIC's draft Notifiable Data Breach (NDB) Resources.

Generally, these resources are comprehensive and will prove extremely useful to our Members as they prepare for commencement of the NDB scheme on 22 February 2018. We are extremely appreciative of the efforts of the OAIC in compiling these important resources.

In terms of specific feedback, we have the following:

##### OAIC Resource: Identifying eligible data breaches

In its original submission to the draft bill, ARCA raised issue with the concept of 'serious harm' extending to psychological or emotional harm on the basis that these concepts are largely subjective, will differ depending on the individual, and are only able to be determined by the person experiencing this type of harm.

Further, these types of harm are unlikely to occur without the presence of other types of harm, such as harm to reputation.

In line with this original submission, our view remains that the reference to these types of harm ought to be removed from this guidance resource.

In addition, one of the factors identified as significant to assessing the circumstances of the data breach, is whether or not the data involves 'vulnerable individuals' or a 'vulnerable segment of the community' (with the result being the breach is more likely to increase the risk of serious harm). Other than noting that 'young persons' may be vulnerable individuals, no other guidance is provided about how a 'vulnerable segment of the community' may be identified.

Furthermore, the proposal that a ‘vulnerable segment of the community’ may be at greater risk of harm by reason of data breach must be measured with reference to the type of data. For instance, the release of sensitive financial information of high-wealth individuals (who would be unlikely to be classified as ‘vulnerable’), may still result in serious harm.

Our view is that further guidance should be provided about identification of ‘vulnerable individuals’ or a ‘vulnerable segment of the community’ to answer these concerns.

Another factor identified as a consideration in the ‘nature of the harm’ is the likelihood of the individual suffering workplace or social bullying or marginalisation. For an entity to make this assessment would be difficult, as this is a highly subjective assessment (dependent upon knowledge of the individual’s workplace, and social groups). Further the examples of ‘loss of business or employment opportunities’, and ‘humiliation, damage to reputation or relationships’ adequately addresses the necessary considerations.

This example ought to be removed from the resource.

To summarise, ARCA’s seeks the following changes to this resource:

- Removal of psychological or emotional harm as types of serious harm
- Inclusion of further guidance about what factors would be relied upon to identify a vulnerable individual or vulnerable segment of the community
- Removal of ‘workplace or social bullying or marginalisation’ as an example of a potential harm.

#### OAIC Resource: Notifying individuals about an eligible data breach

Again, in our original submission to the draft bill, ARCA raised the need for guidance to be provided to deal address notification requirements where information is jointly held by individuals. This needs to be addressed in this resource.

In our view, it should be appropriate that notification of one of the joint information holders ought to be sufficient, where that is an appropriate outcome for consumers. Further, it should be clear that notifying both information holders in a single mail out (for instance, a letter to a couple residing at the same address with both individuals listed as addresses) is sufficient to meet notification requirements.

We have no specific feedback to provide for the Entities covered by the NDB scheme and Australian Information Commissioner’s role in the NDB scheme resources.

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 our Legal and Regulatory Affairs Manager, Elsa Markula.

Yours sincerely

Mike Laing

Executive Chair

Australian Retail Credit Association (ARCA)