

23 October 2017

Office of the Australian Information Commissioner
Level 3, 175 Pitt Street
Sydney NSW 2000

By email only:
consultation@oaic.gov.au

Dear Colleagues

New Draft Resources for the Notifiable Data Breaches (NDB) Scheme: 29 September 2017

The Financial Services Council (**FSC**) has over 100 members representing Australia's retail and wholesale funds management businesses, superannuation funds, life insurers, financial advisory networks and licensed trustee companies. The industry is responsible for investing more than \$2.7 trillion on behalf of 13 million Australians. The pool of funds under management is larger than Australia's GDP and the capitalisation of the Australian Securities Exchange and is the fourth largest pool of managed funds in the world. The FSC promotes best practice for the financial services industry by setting mandatory Standards for its members and providing Guidance Notes to assist in operational efficiency.

Thank you for the opportunity to provide a submission on this topic. Our comments are set out below.

The FSC Working Group on Privacy has assessed the following OAIC draft resources on the NDB scheme published 29 September 2017;

1. Assessing a suspected data breach
2. What to include in an eligible data breach assessment
3. Exceptions to notification obligations
4. A draft form to assist organisations in preparing a statement about an eligible data breach to the Australian Information Commissioner
5. A new chapter (chapter 9) to the OAIC's guide to privacy regulatory action on data breach incidents

Our comments on the draft resources are set out below:

1. Assessing a suspected data breach

It is noted that this draft document specifies two timeframes for the assessment of a suspected data breach. The first timeframe specifies that the

New Draft Resources for the Notifiable Data Breaches (NDB) Scheme: 29 September 2017:FSC Submission 23 October 2017

assessment must be “reasonable and expeditious” and the second specifies, “an entity must take all reasonable steps to complete the assessment within 30 calendar days after the day the entity became aware of the ground (or information) that caused it to suspect an eligible data breach. Given the significantly diverse range of data breaches it is our position that in some circumstances, the 30 calendar day’s timeframe may be logistically feasible for the completion of the assessment and in some circumstances it will only be possible to conduct an initial or partial assessment within that timeframe. For example, a single lost file, misdirected email about one customer should be relatively quick and simple to investigate, whereas a global hacking attack into one or more computer systems of an entity may require the assistance of information technology forensic teams and may take a significant period to complete fully the assessment. Our position is that preliminary notification should only be required where there is some indicator for likelihood of serious harm. In such cases where the assessment process is likely to take more than 30 calendar days it would be reasonable to make a preliminary notification to the OAIC with periodic updates at agreed timeframes. Thus, data breach cases that require specialist knowledge to investigate greater than a 30 day period from the breach should not be reportable where there is an indication of a likelihood of serious harm for any individual. This is consistent with the approach taken by other financial services regulators such as ASIC and APRA.

The other point we wish to raise regarding the assessment, is that as financial services providers, we will often only have limited information about a customer such as their banking and insurance details and we may not know their individual circumstances that would be likely to lead to a real risk of likely serious harm to a particular person or group. For example, the unauthorised disclosure of a telephone number or postal address could have different consequences for particular individuals, if a customer ran their own business from that address and using that telephone number they are unlikely to suffer any serious harm due to the disclosure, as the information may be publicly available anyway in their marketing communications. However the consequences of the same disclosure to another customer could be significant; for example, if they were in a witness protection plan or had an apprehended violence order against a violent ex-spouse. In many cases a financial services provider would not know this level of detailed information about its customers which may impact on its ability to assess the risk of harm to them. It is our position that if the assessment is conducted based on the information that the financial service provider actually has available to it (whether provided by the customer or an authorised agent); the result of that assessment should be deemed to be reasonably made irrespective of the particular circumstances of an individual.

It is our position that this draft resource should reflect the wording in section 26WG of the *Privacy Amendment (Notifiable Data Breaches) Act 2017*, specifically regarding subsections (e) and (f) regarding the security measures taken by the entity to protect the information such as encryption, password protection, secure portals etc. and the likelihood that the security measures could be overcome. The assessment of a privacy or data breach would need to address if the information is unintelligible to the unintended recipient, for example if they could read a cover email that simply tells them to open an attachment, but they are unable to open the attachment or decipher the

New Draft Resources for the Notifiable Data Breaches (NDB) Scheme: 29 September 2017:FSC Submission 23 October 2017

information without the encryption key. It is our position that the draft resource on assessing a suspected data breach should either mention or cross reference the provisions of section 26WG regarding the following:

- the likelihood of harm;
- the type of information involved;
- the security measures used to protect the information, where relevant;
- the strength of those security measures;
- the persons who have obtained or could obtain the information;
- if a security technology or methodology was used in relation to the information and if so, if it was designed to make the information unintelligible or meaningless to unintended recipients; and
- the likelihood that unintended recipients have of causing harm to the impacted individuals; and
- the nature of the harm.

It is our position that updated guidance materials on data breach response plans would be useful to inform APP entities about the OAIC's expectations about the content of those plans to incorporate the NDB scheme obligations such as the points made in this submission.

2. What to include in an eligible data breach assessment

It is noted that the wording in the last of the five dot points under the heading "Description of the eligible data breach" uses the word "contain" and it is our position that this point be extended to include wording about the steps the entity this has taken to remediate the likely impacts of the breach, where relevant. Alternatively, a sixth dot point could be added to reflect the remedial action exception in section 26WF of the *Privacy Amendment (Notifiable Data Breaches) Act 2017*. In some circumstances it may not be practicable for the entity to take remedial action before any serious harm is caused by the breach; however, in circumstances where an entity has taken proactive and expeditious action to remediate the likely risk of harm it is our position that information about those steps warrant a mention in the statement to the OAIC. For example, if a bank identifies suspicious activities involving an account and freezes that account until it can contact the customer and verifies the transactions; this is likely to remediate the real risk of serious harm that may occur to this customer.

We reiterate our comments about the various timeframes in point 1 above as this draft resource also uses different timeframes such as "as soon as is practicable" and "promptly" and our position is that for clarity it should include wording about the assessment being made within 30 calendar days.

3. Exceptions to notification obligations

Organisations may wish to make it clear about their respective NDB scheme notification responsibilities when dealing with other entities such as related bodies corporate and outsourced service providers. A pragmatic approach would be for the entity at fault to have the notification responsibilities. For

New Draft Resources for the Notifiable Data Breaches (NDB) Scheme: 29 September 2017:FSC Submission 23 October 2017

example, if an organisation outsources their customer correspondence to a mailing company and customer correspondence is sent to the wrong addresses the mailing company may be expected to make the notification to the OAIC, however, the organisation may wish to directly notify their customers to maintain their relationship with the customers as they may be unaware that mail services are outsourced. The draft resource refers to the service level agreement and contractual arrangements, which is ordinarily where the respective responsibilities would be formally documented. However, ongoing communications between related body corporates could be used to identify any notification requirements and vendor management processes for outsourced service providers could include assurance questions that all relevant items have been communicated to the organisation that is using that outsource so that they can meet their notification obligations. It is noted that organisations may outsource business functions to service providers that are not bound by the *Privacy Act 1988* (Cth) or the 13 Australian Privacy Principles and it follows that the notification obligation would fall on the organisation that is bound by the legislation. It may be prudent to note this fact in the draft resources.

4. A draft form to assist organisations in preparing a statement about an eligible data breach to the Australian Information Commissioner

It is our position that this form should include a section about the steps an entity has taken to protect the data and where, relevant the steps the entity has taken to remediate the likely risk of serious harm as raised above. It is noted that section 9 of the form requires a "description of any action you have taken to prevent reoccurrence"; however this wording does not reflect the wording of the draft resource and should reflect the wording in sections 26WF and 26WG of the *Privacy Amendment (Notifiable Data Breaches) Act 2017*.

5. A new chapter (chapter 9) to the OAIC's guide to privacy regulatory action on data breach incidents

It is noted that in Chapter 9 the list of the factors that the Commissioner will consider when reviewing a possible interference with privacy includes:

- "Steps the notifying entity has taken, or is taking, to mitigate the impact on individuals at risk of serious harm" and
- "Measures that the entity has taken, or is taking, to minimise the likelihood of a similar breach occurring again".

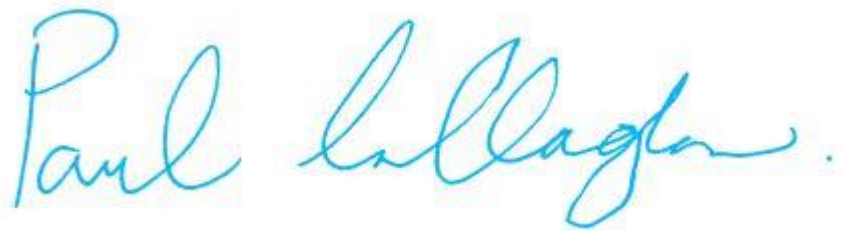
As pointed out above, it is our position that the draft resources and form reflect these points made in Chapter 9 to ensure consistency. We do note that Chapter 9 includes detail on how the Commissioner will deal with a situation in which the OAIC and the entity in question disagree on whether the data breach is notifiable.

It would be useful if at all practicable if this chapter included greater guidance about the relevant considerations, in circumstances when the "Commissioner will have regard to the impact on the entity" in assessing a data breach.

**New Draft Resources for the Notifiable Data Breaches (NDB) Scheme:
29 September 2017:FSC Submission 23 October 2017**

Should you have any questions, please contact the writer on 02-9299 3022.

Yours Faithfully

A handwritten signature in blue ink that reads "Paul Callaghan." The signature is written in a cursive style with a period at the end.

Paul Callaghan

General Counsel