JONES DAY

COMMENTARY

APRIL 2019

Key Lessons From Australia's Notifiable Data Breach Scheme

IN SHORT

The Situation: The Notifiable Data Breach scheme, introduced by amendments to the Privacy Act 1988 (Cth), requires an assessment when an entity suspects that there may have been loss of, unauthorised access to or unauthorised disclosure of personal information. The scheme has been in place for just over one year.

The Result: Recent publications by the Office of the Australian Information Commissioner ("OAIC") indicate that a significant number of data breaches have been notified since the introduction of the scheme.

Looking Ahead: The anniversary of the introduction of the scheme provides a useful opportunity for entities that hold personal information to: (i) consider how best to respond to data breaches given the OAIC's approach to them; (ii) review their management of that information; and (iii) ensure that their management is consistent with best practice.

On 22 February 2018, the Office of the Australian Information Commissioner ("OAIC") marked the one-year anniversary of the enactment of the *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth), which introduced Part IIIC to the *Privacy Act 1988* (Cth). Part IIIC is referred to as the Notifiable Data Breach Scheme. The Scheme requires notification of "eligible data breaches." Notification of a data breach is required when "serious harm" is likely to result from the breach.

OAIC's publications concerning the Notifiable Data Breach Scheme indicate that the largest cause of data breaches notified is "malicious or criminal attack." In light of the risk of data breaches, entities should review their information technology systems to ensure that they meet industry standards, and review their response plans for data breach events to ensure that they are adequately prepared.

WANT TO KNOW MORE?
Read the full version.

FIVE KEY TAKEAWAYS

1. The Notifiable Data Breach Scheme requires notification of data breaches in particular circumstances—not all data breaches need to be notified.
2. Data breach notification statistics show that data breaches are an ever present risk to businesses.
3. Preparation for data breach events is imperative for entities that hold personal information.

Adam Salter
Perth

Prudence Smith
Sydney

YOU MIGHT BE INTERESTED IN: [Go To All Recommendations >>]

[Jones Day Presents: The Blockchain Series]

[Navigating Public–Private Partnerships Around Connected Technology]

[The FDA and Cybersecurity: How the Agency is Addressing Cybersecurity Risks to Medical Devices]

SUBSCRIBE SUBSCRIBE TO RSS

Jones Day is a global law firm with more than 2,500 lawyers on five continents. One Firm Worldwide℠