FEBRUARY 2016

COMMENTARY

Data Breaches are on the Rise in Australia: What if it Happens to Your Company?

Data breaches are becoming more prevalent in Australia. While the reporting of data breaches to regulators or affected customers or clients is presently not mandatory, the Office of the Australian Information Commissioner ("OAIC") received 110 voluntary data breach notifications in the 2014-15 financial year. This was an increase of 64 percent on the previous year.[1]

Responding efficiently and effectively to a data breach, both internally (including by reviewing and strengthening computer systems, and policies and procedures) and externally (including by reporting to regulatory authorities and affected customers or clients) is imperative. There are a suite of options available to do so. The right fit to satisfy legal and commercial matters will depend upon the circumstances of the breach and requires keeping up to date with the changing regulatory and legal landscape governing privacy and data protection in Australia.

Recent High-Profile Australian Data Breaches

Kmart Australia recently announced that it had become the latest Australian company to have experienced a data security breach as a result of online hacking. Information stolen in the breach included the names, email addresses, delivery and billing addresses, and product purchase details of customers that had shopped online with Kmart Australia. In response, Kmart Australia notified all customers affected, engaged IT forensic investigators to review the breach and also reported the breach to the OAIC and the Australian Federal Police ("AFP"), (Australia's federal police agency).

Kmart is not the only large Australian company to have recently been subject to an online attack resulting in a data breach. In October 2015, David Jones (a nationwide Australian retail company) reported a similar online attack. As with the Kmart Australia breach, names, email addresses, physical addresses, and product purchase details were hacked online. Other high-profile Australian companies reporting data breaches of their online systems this year include Vodafone—which included a hack of customers' bank account details; and Woolworths (another nationwide Australian retail company)—that resulted in an email being circulated that included approximately $1.4 million in gift card voucher details.

How to Respond to a Data Breach

Beyond a company's internal response, there are a number of issues a company needs to consider when determining what to do in response to a breach and, in particular, who to report a breach to.

The Australian Privacy Principles ("APPs"), the key piece of Australian law governing privacy and data protection, require APP entities to take reasonable steps in the circumstances to protect information from misuse, interference and loss, and from unauthorised access, modification, or disclosure. However, the APPs do not proscribe any mandatory requirements in response to a data breach. The OAIC published *Data breach notification: A guide to handling personal information security breaches* ("Data Breach Guide") in April 2012. The Data Breach Guide provides general guidance to APP entities on how to respond to a data breach involving personal information.[2] The Data Breach Guide states that an APP entity's response to a data breach will depend upon the circumstances, including the sensitivity of the personal information in question, the harm likely to result from breach, the harm to the APP entity's reputation if notification occurs, and the way the entity stores and uses the information.[3]

There is currently no requirement to notify those whose personal information has been misused or lost. The OAIC recommends that companies who are subject to a data breach should notify not only the Australian Information Commissioner but also the individuals whose personal information has been lost "if a data breach creates a real risk of serious harm to the individual".[4] This is an important step in preventing further misuse of the personal information by allowing individuals to take steps to regain control of their private information by changing passwords or account numbers, or notifying other organisations that may be able to assist.[5] Presently, however, notification in the event of breach of privacy is voluntary in Australia.[6]

Data Breach Notification is Closer to Becoming Mandatory in Australia

In 2008, the Australian Law Reform Commission recommended that the *Privacy Act 1988* (Cth) (the key piece of Australian privacy legislation) be amended so that APP entities would be required to notify individuals (as well as the OAIC) whose personal information had been lost or misused.[7] A bill was introduced in 2014 which proposed that a mandatory data breach notification scheme be made into law in Australia. However, with a change in Australia's Federal Government the bill did not progress any further.

In December 2015, the Federal Government released a discussion paper and an exposure draft of the P*rivacy Amendment (Notification of Serious Data Breaches) Bill 2015* (Cth) ("the Bill") for public consultation. Submissions from the public close on 4 March, 2016. The Bill is likely to go before the Australian Parliament for debate in around the second quarter of 2016. The Bill could become law, subject to any revisions based upon consultation and debate, around mid 2016.

The Bill applies to APP entities (including a related body corporate that collects personal information from an APP entity) that have an annual turnover of more than AUD3 million and an "Australian link"—this includes an entity that, while not incorporated or registered in Australia, carries on business in Australia and collects or holds personal information in Australia. The Bill uses the definition of APP entity from the APPs.

If the Bill is enacted, APP entities will be required to notify affected individuals and also the OAIC in the event that there is a "serious data breach"—namely, if there is unauthorised access to, disclosure of, or loss of personal information and as a result there is a real risk of serious harm to any of the individuals to whom the information relates. The Bill also provides that the attorney-general may make regulations that deem particular breaches as "serious data breaches", regardless of whether the data breach resulted in a real risk of serious harm. The Bill contemplates that such regulations could be made in respect of health records.

If an APP entity suspects but is not certain a serious data breach has occurred, the entity has 30 days to assess if notification is required. An APP entity would fail to comply with its notification obligations where it is not aware of a serious data breach, however it reasonably should have detected it.

Failure to comply with the notification requirements will be deemed to be an interference with the privacy of the

individual concerned, and will engage the Australian Information Commissioner's powers to investigate, make determinations, seek enforceable undertakings, and impose civil penalties (of up to AUD1.8 million) for serious or repeated infringements.[8] Civil penalties would be imposed by the Federal Court or Federal Circuit Court on application by the Australian Information Commissioner. This is in addition to the enhanced regulatory powers granted to the Australian Information Commissioner in 2014, including the ability to conduct an assessment of whether an entity is lawfully maintaining and handling personal information and to investigate (on the Commissioner's own initiative) acts or practices that may interfere with the privacy of an individual.

Lawyer Contacts

For further information, please contact your principal Firm representative or one of the lawyers listed below. General email messages may be sent using our "Contact Us" form, which can be found at www.jonesday.com/contactus/.

Adam Salter
Partner
Sydney
+61.2.8272.0514
asalter@jonesday.com

Peter Brabant
Associate
Sydney
+61.2.8272.0509
pbrabant@jonesday.com

Nicola Walker
Associate
Sydney
+61.2.8272.0546
nwalker@jonesday.com

Endnotes

1 Office of the Australian Information Commissioner, *Annual Report 2014-15*, p. 77.

2 Personal information is defined in the Privacy Act 1998 (Cth) as "*information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable.*" Common examples are an individual's name, signature, address, telephone number, date of birth, bank account details and commentary or opinion about a person.

3 Data Breach Guide at p. 6.

4 Data Breach Guide at p. 22.

5 Data Breach Guide at p. 22.

6 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) vol 2, p. 1667 [51.2].

7 Australian Law Reform Commission (2008), pp. 1690-1692 [51.83]-[51.90].

8 Consultation Draft Explanatory Memorandum, *Privacy Amendment (Notification of Serious Data Breaches) Bill 2015* (Cth), p. 5.