BROADLEY REES HOGAN | NEWS

Post navigation Do I need to notify anyone when personal information goes missing?

By Peter Bolam, Special Counsel

Losing an expensive company laptop or having your client data base 'hacked' can be costly to remedy, and embarrassing. But have you assessed the *Privacy Act*implications? Organisations bound by the Act need to consider how they can minimise any damage caused by personal information going astray, including by notifying those affected.

Data Breaches

Data breaches can occur in a variety of ways. The Office of the Australian Information Commissioner **(OAIC)** has issued a *Guide to Handling Personal Information Security Breaches* which gives the following examples:

- lost or stolen laptops, removable storage devices or paper records containing personal information;
- hard disc drives and other digital storage media (for example, multifunction printers) being returned to equipment lessors without the contents first being erased;
- data bases containing personal information being hacked; and
- organisations mistakenly providing personal information to the wrong person, for example by sending details out to the wrong address.

OAIC Guidance

The OAIC Guide is guidance, not legislation, and the OAIC acknowledges that while compliance with the Guide is not mandatory, it is strongly recommended. Furthermore, compliance with the Guide may ensure that Australian Privacy Principle 11 **(APP 11)**(which is legislative) is satisfied. APP 11 is one of thirteen Australian Privacy Principles that could apply to an organisation.

By APP 11 an organisation that holds personal information must take such steps as are reasonable to protect the information from:

(a) misuse, interference and loss; and
(b) unauthorised access, modification or disclosure.

Personal information is information or an opinion about an identified or identifiable individual.

When a data breach occurs, the steps that an organisation should take to comply with APP 11 will depend upon the circumstances and be determined primarily from an evaluation of the risks associated with the breach. An important reasonable step to be considered by an organisation is notification of affected individuals and the OAIC.

The Australian Law Reform Commission has noted that the primary rationale for notifying people that their personal information has been breached is to help minimise the damage caused by the breach. The ALRC has also commented that as a result of the reputational damage to organisations that notification can cause, they may not have sufficient incentives to voluntarily notify customers of a data breach.

In June 2015 the OAIC reported that it has finalised enquiries into Australian retail company Catchoftheday.com.au Pty Ltd (COTD) following a data breach notification received in June 2014 in respect of a breach which occurred in 2011 that compromised the personal information of the COTD customer base. In the statement the Commissioner *"expressed concern about the size of the breach, the possible compromise of financial information, and the significant delay between COTD becoming aware of the incident and notifying affected individuals"*.

Faced with this disclosure dilemma, is it mandatory for an organisation to notify affected individuals of the breach?

Is Notification Mandatory?

There is no specific provision of the *Privacy Act* that requires notification. In its 2008 Privacy Report, the Australian Law Reform Commission recommended the inclusion of a data breach notification obligation in the *Privacy Act*. However, this recommendation was not implemented in the first stage response to the ALRC Report. Further attempts were made in 2013 and 2014 when Bills were introduced by Labor while in government and subsequently while in opposition to mandate data breach notification. The first Bill lapsed when it had not been heard by the Senate on the last day of Parliamentary sittings and the second was blocked by Coalition senators when the Bill was introduced in the Senate.

It was reported that while the Coalition senators rejected the legislation proposed by Labor because of insufficient consultation and discussion, they did support the principle of requiring businesses and government to notify the public of data breaches.

So, absent amendment of the *Privacy Act* to require data breach notification, are organisations free to choose whether to notify affected individuals of the breach?

More OAIC Guidance

The Office of the Australian Information Commissioner points out that notification of the individuals who are or may be affected by a data breach, and the OAIC, may be a reasonable step required by APP 11. Furthermore, a new *Guide to Privacy Regulatory Action* issued by the Commissioner makes clear that data breach incidents may in certain circumstances result in Commissioner-initiated investigations under the *Privacy Act*.

Importantly for organisations considering whether to make a data breach notification is the Guide's statement of the matters that the Commissioner will take into account when deciding whether it is necessary to open a Commissioner-initiated investigation into a data breach incident. Those factors are whether:

- the entity has voluntarily and proactively notified the OAIC of a data breach incident; and
- the entity responded (or is the process of responding) appropriately to the breach including by containing the breach, taking reasonable steps to mitigate harm to affected individuals, and taking steps to limit future breaches; and
- the entity cooperates fully with the OAIC's enquiries into the breach.

Should there be a Commissioner-initiated investigation; the OAIC may take further regulatory action that includes:

- seeking an enforceable undertaking under section 33E of the *Privacy Act*;
- making a determination under section 52(1A) of the *Privacy Act*; and
- where a civil penalty provision has been breached, applying to the Court for a civil penalty under section 80W of the *Privacy Act.*

Do you need advice?

Organisations that have suffered a data breach face a difficult decision. Uncertainty remains as to whether notification is mandatory. It is clear that without amendment of the*Privacy Act*, there is no specific requirement in the Act for a data breach to be disclosed. However, notification may be a reasonable step required for compliance with APP 11 and will be a factor considered by the Commissioner when determining whether to open a Commissioner-initiated investigation that may in turn result in penalties for the organisation.

Should you wish to discuss any matters arising out of this article, please contact the author:

Peter Bolam, Special Counsel
D +61 7 3223 9139
F +61 7 3221 5518
M +61 0427 448 562
E peter.bolam@brhlawyers.com.au

Broadley Rees Hogan (BRH Lawyers) is an independent boutique firm, specialising in corporate, commercial, property, construction and litigation. Based in Brisbane, we act for clients across the country and internationally – **for an unassuming firm, we know how to deal big**.

For more information, please visit **www.brhlawyers.com.au** or **contact us** on (07) 3223 9100.