Travel insurer hacked: Implications under the Privacy Act 1988 (Cth)

By Andrew Moore, Partner and Jack Geng, Associate
3 February 2015

It has recently emerged that the Australian travel insurer, Aussie Travel Cover (**ATC**) has been the subject of a cyber attack. It is understood that the attack compromised 770,000 personal data entries in the ATC database (**the Data Breach**).

ATC became aware of the Data Breach on 18 December 2014, and notified the Privacy Commissioner on 22 December 2014. On 23 December 2014 ATC notified third party travel agents. However, ATC did not notify its former and current policyholders of the Data Breach.

This attack on ATC represents a real life case study with which we can examine the likely impact of the Data Breach under the **Privacy Act 1988 (Cth)** (**the Privacy Act**).

Regulatory investigation

Under the Privacy Act, the Australian Information Commissioner (**the Commissioner**) has the regulatory power to investigate any alleged breaches of the Privacy Act including breaches of the **Australian Privacy Principles** (**APP**). Specifically, the Commissioner can commence an investigation following a complaint or commence an investigation under its own initiative.

Currently there are no mandatory notification requirements under the Privacy Act and it is unclear how many former and current ATC policyholders are aware of the Data Breach. However, based on initial media reports, some customers have reacted negatively to ATC's failure to notify them of the Data Breach and unfortunately it may be inevitable that complaints are made to the Commissioner.

It is possible that the Commissioner may elect to commence an investigation. Such an investigation is not without precedent. For example in 2013, the Commissioner commenced an investigation against Cupid. Cupid is an internet dating company that was the subject of a cyber attack, which compromised the personal details of 254,000 customers[1].

Reasonable steps

If an investigation were to be instigated, the Commissioner will examine ATC's compliance with the Privacy Act and the APP, including whether ATC had taken reasonable steps to protect the personal information of its former and current policyholders.

Preliminary investigations indicate the Data Breach was carried out using a 'SQL injection' attack. This is a relatively common hacking technique that usually targets known vulnerabilities in computer software.

Whilst it remains to be seen whether ATC had taken reasonable steps to guard against the 'SQL injection' attack, the Commissioner published in January 2015 the updated "*Guide to securing personal information*" (**the Guide**). Under the Guide, what is 'reasonable' will depend on the circumstances, including factors such as:

- the nature of the entity;
- the amount and sensitivity of the personal information held;
- the possible adverse consequences for an individual in the case of a breach;

[1] See Cupid Media Pty Ltd, Own Motion Investigation Report, Australian Privacy Commissioner, June 2014.

- the practical implications of implementing the security measure, including the time and cost involved; and
- whether a security measure is itself privacy invasive.

Interestingly in the Cupid investigation, the Commissioner found Cupid failed to take reasonable steps to protect its customers' personal information[2]. Specifically, the Commissioner found that the storage of passwords in an unencrypted document to be a failure to take reasonable steps.

Civil penalties

Under the Privacy Act, the Commissioner has the power to:

- impose civil penalties for serious or repeated breaches, including fines of up to $1.7 million for businesses and $340,000 for any individuals; and
- accept enforceable undertakings from businesses.

Whilst the Commissioner did not impose any civil penalties in its Cupid investigation, the Commissioner has awarded compensation (between $7,500 and $8,500) in other complaints involving failures to take reasonable steps to protect personal information. However, those complaints did not involve mass data breaches. Accordingly, it remains to be seen whether the Commissioner will compensate consumers for mass data breaches such as those in Cupid or ATC.

Financial costs

It is generally accepted that cyber attacks have the potential to cause large scale losses for businesses. By way of example, the Ponemon Institute[3] estimates that the average cost of a data breach in Australia in 2014 is approximately $145 per breach. The Ponemon Institute report was based on known data breaches in Australia involving 22 companies in 11 industry sectors. This figure increased to $161 per breach when the breach involved a malicious or criminal attack.

Final thoughts

Large scale data losses tend to dominate media headlines, and potentially cause enormous losses for any affected businesses. It is important from a risk management perspective that businesses have an up-to-date computer system and hold an appropriate cyber insurance policy to guard against such losses.

As the fallout from the ATC Data Breach continues to unfold, it may be only a matter of time before we see another large scale data breach in Australia. When such losses occur, any affected businesses must not only deal with the inevitable public backlash, but also face the full regulatory fall out under the Privacy Act. The question is 'are we prepared'?

Andrew Moore, Partner
e: andrew.moore@wottonkearney.com.au
p: +61 2 8273 9943

Jack Geng, Associate
e: jack.geng@wottonkearney.com.au
p: +61 2 8273 9910

---

[2] ***'BO' and AeroCare Pty Ltd*** [2014] AICmr 32 and ***'CM' and Corporation of the Synod of the Diocese of Brisbane*** [2014] AICmr 86.
[3] See Cost of Data Breach Study: Australia, Ponemon Institute, May 2014.