MARSH

February 2018

CLIENT ALERT

INTRODUCTION OF THE NOTIFIABLE DATA BREACHES SCHEME

On **22 February 2018** *the Privacy Amendment (Notifiable Data Breaches) Act 2017* will come into effect. Prior to this legislation there was no statutory requirement in Australia, other than for eHealth data breaches, for businesses to notify either affected individuals or regulatory bodies of any data breach.

BACKGROUND ON LEGISLATIVE CHANGES

The Act introduces the Notifiable Data Breaches ("NDB") scheme which establishes mandatory reporting protocols of all *eligible data breaches* for entities bound by the Australian Privacy Principles. These include any private sector and not-for-profit organisations with an annual turnover greater than $3million, and all Commonwealth Government and Australian Capital Territory Government agencies. We note that some organisations with less than $3million turnover may also be subject to the scheme.

An eligible data breach occurs:

1. When both of the following conditions are met:

- There is unauthorised access to, or unauthorised disclosure of personal information, and
- The breach would lead a reasonable person to conclude that there is a likely risk of serious harm to any of the individuals to whom the breached information relates;

OR

2. The data is lost in circumstances when:

- unauthorised access to, or unauthorised disclosure of, personal information is likely to occur, and
- if the above were to occur a reasonable person would conclude that there is a likely risk of serious harm to any of the individuals to whom the breached information relates

Accidental errors in processing or transmitting personal information may also be deemed as eligible data breaches under the NDB scheme.

The Privacy Act defines *personal information* as information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not and whether the information or opinion is recorded in a material form or not.

Examples of personal information include:

- Health information
- Employee records
- Tax file numbers
- Credit information

Following an increase in the penalty unit value the Privacy Act now allows for the following civil penalty provisions:

- A serious or repeated interference with privacy of 2000 penalty units (current total is $420,000), or up to 2000 penalty units for a privacy breach
- The maximum penalty that the court can order for a body corporate is five times the amount listed in the penalty provisions (current maximum $2.1million)

WHO MUST BE NOTIFIED IN THE EVENT OF AN ELIGIBLE DATA BREACH?

Notification of affected individuals is required to be made as soon as practicable in the event of an eligible data breach. Notification is also to be made to the AIC.

Where there are reasonable grounds to suspect that a breach has occurred, organisations are also obliged to assess whether an eligible data breach has occurred and whether there is a likely risk of serious harm to affected individuals. The Office of the Australian Information Commission ("OAIC") expects that such assessments are conducted within 30 days of a suspected data breach.

WHAT DETAILS MUST A NOTIFICATION INCLUDE?

Notification to the OAIC should be made in the form of a Notification Data Breach statement, with the draft template available on the Australian Government website. The form should include:

- The identity and contact details of the entity
- A description of the eligible data breach
- The kind or kinds of information involved in the eligible data breach
- What steps the entity recommends that individuals take in response to the eligible data breach

There are three options to consider in notifying affected individuals:

Option 1: Notify all individuals

- If it is practicable, an entity can choose to notify each of the individuals whose personal information was part of the eligible data breach

Option 2: Notify only those individuals at risk of serious harm

- If it is practicable, an entity can notify only those individuals who are at risk of serious harm from an eligible data breach

Option 3: Publish notification

- If neither option 1 or 2 are practicable, an entity must publish a copy of the statement prepared for the OAIC on their company website and also take proactive steps to publicise the core details of the eligible data breach to increase the likelihood it will come to the attention of individuals at risk of serious harm

THIRD PARTY SERVICE AGREEMENTS

In preparing for the NDB scheme introduction, it is critical for an organisation to review its third party supplier relationships to establish where notification responsibilities would lie in the event of an eligible data breach. Even if a business outsources its data storage and/or processing, it will still be subject to the NDB scheme.

When entering into new contractual arrangements or reviewing existing ones, a business should ensure clear procedures are established for complying with the NDB scheme. Generally speaking it is recommended that the entity with the most direct relationship with the individuals at risk of serious harm be the one to notify.

If a single eligible data breach applies to multiple entities, the scheme only requires one entity to notify the AIC and the individuals at risk of serious harm. However if the correct process is not followed, then all entities may be held to be in breach of the legislation.

LEGAL RISKS

In addition to the regulatory implications following a data breach, a business may also face legal liability arising from third party litigation. This may result from breach of confidentiality obligations that are owed to customers, who can pursue the entity for financial compensation following loss or theft of their personal information.

The risk of class actions has also been highlighted by cases in the US, where consumers have sought damages for personal injury, mitigation costs and aggravated damages for failure to maintain appropriate data security measures, failure to notify affected individuals and violation of legislation.

Litigation can also arise from financial institutions (banks, credit unions) alleging negligence and failure to adopt adequate Payment Card Industry Security Standards.

INSURANCE RESPONSE

- An insurance policy should not act as the primary solution for managing a company's exposure to cyber-attacks or data breaches, however, mitigating cyber risk through insurance plays an important role in the overall risk management protocols of a business. There are many costs that can impact a company in the event of a privacy breach and insurance can assist in providing support for these costs. Some examples are shown in the following table:

DATA BREACH CONSEQUENCE	FINANCIAL COST / LOSS	CYBER INSURANCE PROTECTION
IT forensic costs to assess and remediate the data breach	Expected	Yes
Notification costs incurred in advising affected individuals	Expected	Yes
Legal costs to notify regulators (breach coach)	Expected	Yes
Ongoing credit monitoring services to affected individuals	Expected	Yes
PR costs to assist in reducing damage to brand	Expected	Yes
Legal defence costs and damages for liability claims arising from affected individuals	Possible	Yes
Payment Card Industry (PCI) fines or assessments	Possible if breached data includes credit card information	Yes
Extortion demands	Possible	Yes

**the above summary represents a general overview of available insurance coverage and should not be relied upon in the event of a claim. Please refer to the specific terms and conditions of your insurance policy for full terms and conditions.*

MARSH CONTACT:

Kelly Butler
National Cyber Leader
+61 3 9603 2194
kelly.butler@marsh.com

Kristine Salgado
Managing Principal – FINPRO and Cyber
+61 3 9603 2871
kristine.salgado@marsh.com

S_AM_18-0135