PRESENTED BY

K&L GATES

There's a *breach*

K&L Gates' **Cameron Abbott**, **Rob Pulham** and **Keely O'Dowd** share their tips around data breaches.

THE LONG AWAITED commencement of the notifiable data breach scheme (NDB Scheme) is just around the corner.

From 22 February 2018, entities bound by the Australian Privacy Principles will be required to comply with this new scheme and notify the Commissioner and affected individuals when a data breach is likely to result in serious harm to those affected individuals.

Prior to the introduction of the NDB Scheme in Australia, notification of a data breach to the Australian Information Commissioner was not mandatory under the national Privacy Act.

Why is it important to prepare for the scheme?

You may be asking yourself, what does this mean for your business and why should you care?

Well, for starters, compliance with the NDB Scheme will be mandatory for many businesses that operate in the fashion industry. Failure to comply with the scheme may attract a civil penalty (currently up to $420,000 for individuals and $2.1 million for corporations). The Commissioner can also pursue enforceable undertakings against non-complying businesses.

Fashion brands and retailers are targets for hackers, as they handle and store a high volume of personal information. The names, contact information and credit card details of customers are valuable to hackers, who can steal and then sell this material on the dark web for a nominal amount. The greater the volume of information a hacker can appropriate, the more profit to be made.

The recent data breaches that have affected Forever 21 and Kmart, amongst others, serve as a reminder that data breaches are costly and can have significant wide reaching operational, financial, legal and reputational consequences for fashion businesses.

What do I need to do to prepare for the scheme?

If your business is required to comply with the NDB Scheme, at a minimum, it should make an upfront investment to:

- Review its current privacy and data security policies and procedures and incident/breach response plans.
- Assess whether the policy and procedures set out a plan that can be followed in the event that a data breach occurs. We recommend all businesses have a clear breach response plan. The Commissioner expects this and businesses who have done so have found such plans valuable and effective in a crisis. If your business does not have a data breach response plan, we recommend that one be prepared in time for the start of the NDB Scheme.
- Increase staff awareness of your business' information security policies and procedures and conduct training to inform all staff members of the new NDB Scheme. Remember, everyone in the business has a responsibility to remain vigilant and know what to do if they become aware of a data breach.
- Have in place a communication plan that sets out a process to follow in the event that your business suffers a data breach requiring it to notify the Commissioner, affected individuals (if necessary) and other interested parties (such as your business' insurer and third party advisers) of the breach.
- Review contracts with existing suppliers that collect and handle personal information on behalf of your business. Assess if those contracts need updating to include data breach response and notification obligations that suppliers must comply with in the event that they suffer a data breach that includes the personal information it collects or handles on behalf of your business.
- If you are unsure of your business' obligations or have any queries, seek advice from a lawyer who specialises in privacy law. ■

For more information about issues relating to privacy law please contact Cameron Abbott, Partner at K&L Gates (Cameron.Abbott@klgates.com). This article is for informational purposes and does not contain or convey legal advice. The information herein should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer.