Emerging legal and regulatory risks for data breaches
Matthew Pokarier and Benjamin Di Marco
About us

Clyde & Co is a dynamic, rapidly expanding global law firm focused on providing a complete legal service to clients in our core sectors.

We advise businesses that are at the heart of worldwide commerce and trade.

Our combination of sector expertise, commercial attitude and in-depth regional understanding provides a unique perspective.

We are experts in privacy law, data breach management and cyber insurance, and have a depth of experience in handling and co-ordinating first response to cyber breaches, breach readiness audits, breach response plan development and implementation, staff training, and more broadly in relation to the privacy regime in Australia.

“They are heavily client focused. They offer a really wonderful blend of technical ability and commercial savviness.”

Chambers Asia Pacific 2015 - Australia client testimonial

“They’re highly accessible; it feels like they’re an extension of our team.”

Chambers Asia Pacific 2016 - Australia client testimonial
## Contents

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>Australia's statutory framework</td>
<td>2</td>
</tr>
<tr>
<td>Australia's Privacy Act</td>
<td>2</td>
</tr>
<tr>
<td>Introduction</td>
<td>2</td>
</tr>
<tr>
<td>Adobe Systems Software Ireland Ltd</td>
<td>3</td>
</tr>
<tr>
<td>Cupid Media Pty Ltd</td>
<td>3</td>
</tr>
<tr>
<td>Telstra Corporation Ltd</td>
<td>4</td>
</tr>
<tr>
<td>Running afoul of the Privacy Act</td>
<td>4</td>
</tr>
<tr>
<td>Mandatory Notification Bill</td>
<td>5</td>
</tr>
<tr>
<td>Australia's regulatory response</td>
<td>7</td>
</tr>
<tr>
<td>ASIC</td>
<td>7</td>
</tr>
<tr>
<td>OAIC</td>
<td>8</td>
</tr>
<tr>
<td>APRA</td>
<td>9</td>
</tr>
<tr>
<td>ASX</td>
<td>9</td>
</tr>
<tr>
<td>Third party liability</td>
<td>11</td>
</tr>
<tr>
<td>Case study of Home Depot litigation</td>
<td>11</td>
</tr>
<tr>
<td>Consumer class actions</td>
<td>12</td>
</tr>
<tr>
<td>Financial institution actions</td>
<td>12</td>
</tr>
<tr>
<td>Regulatory actions</td>
<td>12</td>
</tr>
<tr>
<td>Understanding the risk of litigation following data breaches</td>
<td>13</td>
</tr>
<tr>
<td>Claims by individuals for breaches: the overseas experience</td>
<td>14</td>
</tr>
<tr>
<td>Duty of care</td>
<td>14</td>
</tr>
<tr>
<td>Reasonable standard of care</td>
<td>15</td>
</tr>
<tr>
<td>Caution</td>
<td>15</td>
</tr>
<tr>
<td>Proof of loss and damage</td>
<td>15</td>
</tr>
<tr>
<td>Pure economic loss</td>
<td>16</td>
</tr>
<tr>
<td>Class certification</td>
<td>16</td>
</tr>
<tr>
<td>Topic</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Claims by individuals in Australia</td>
<td>16</td>
</tr>
<tr>
<td>Actions by financial institutions: the overseas experience</td>
<td>18</td>
</tr>
<tr>
<td>Actions by financial institutions in Australia</td>
<td>19</td>
</tr>
<tr>
<td>Indemnification litigation</td>
<td>19</td>
</tr>
<tr>
<td>Shareholder class actions: the US experience</td>
<td>19</td>
</tr>
<tr>
<td>Wyndham case</td>
<td>19</td>
</tr>
<tr>
<td>Target case</td>
<td>20</td>
</tr>
<tr>
<td>Heartland case</td>
<td>21</td>
</tr>
<tr>
<td>Shareholder actions in Australia</td>
<td>21</td>
</tr>
<tr>
<td>Overview</td>
<td>21</td>
</tr>
<tr>
<td>Fraud on the market</td>
<td>22</td>
</tr>
<tr>
<td><strong>Legal issues arising from response strategies</strong></td>
<td>23</td>
</tr>
<tr>
<td>Privilege</td>
<td>23</td>
</tr>
<tr>
<td>Insurance</td>
<td>25</td>
</tr>
</tbody>
</table>
Introduction

It is common knowledge that data breaches represent a significant risk to organisations, and that failing to protect personal information can expose individuals and the wider community to fraud and loss.

Australian regulators have a heightened focus on increasing organisational cyber resilience and protecting personal information. Understanding the approaches regulators are taking, and the legal obligations posed by legislation are a key part of an organisation's capacity to effectively manage risk.

While the information security industry has taken an active role in strengthening organisational ability to prevent and respond to cyber intrusions, consideration should also be given to the wider legal risks arising from breaches and emerging issues regarding:

1. how the courts are likely to ultimately apportion responsibility where a data breach occurs; and
2. the amount of organisations' exposure to legal claims by third parties in the event of a breach.

The purpose of this paper is to provide a broad outline of Australia's current legal and regulatory framework concerning data breaches, and give insights into how future legal risks are likely to evolve given the issues courts and regulators are confronting both in Australia and internationally.
Australia's statutory framework

Australia's Privacy Act

Introduction
The Australian Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth) amended the Privacy Act 1988 (Cth) (Privacy Act) by introducing the Australian Privacy Principles (APP) which imposed expanded obligations on organisations involved in the collection, handling and use of personal information.

In the context of data breaches, three provisions of the APP are most relevant being:
1. APP 6.1 which requires an APP entity holding personal information about an individual to only use or disclose the information for the particular purpose for which it was collected.
2. APP 11.1 that states APP entities must take reasonable steps to protect personal information from misuse, interference and loss and from unauthorised access, modification or disclosure.
3. APP 11.2 which requires APP entities to take reasonable steps to destroy personal information or ensure it is de-identified if it no longer needs the information for any purpose for which it may be used or disclosed under the APPs.

The definition of ‘APP entity’ extends to most government and commercial entities with more than $3 million in annual turnover and some smaller businesses such as those that are private health service providers, that sell or purchase personal information or that are operating under Australian Government agency information or contracts.

The Privacy Act defines personal information widely to include an opinion about an identified individual, or an individual who is reasonably identifiable:
1. whether the information or opinion is true or not; and
2. whether the information or opinion is recorded in a material form or not.

The Privacy Act has wide reaching jurisdiction and applies to acts done or practices engaged in which have an ‘Australian link’. This includes where an Australian citizen, a body corporate incorporated in Australia or a company carrying on business in Australia is involved, or in some cases where information is stored in Australia. The ‘Australian link’ requirement can result in a wide application of the
Privacy Act as, for example, an European citizen was able to pursue a complaint under the Privacy Act against an Australian business.¹

APP 6.1, 11.1 and 11.2 apply where an APP entity holds personal information. This includes both situations where the APP has physical control of records, and where the APP entity has the right or power to deal with a record, for example, where it relies on a third party cloud processor as part of its business.

One of an entities key obligations under the APPs is to take ‘reasonable steps’ to protect and destroy personal information. What is reasonable is a question of fact in each individual case which will turn on the type of organisation involved, the risk of injury arising from the information, and the vulnerability of the individuals whose information is stored.

In determining what constitutes ‘reasonable steps’ for the purposes of the Privacy Act, determinations made by the Australian Privacy Commissioner – which are discussed below – have indicated that entities should have regard to the following:

1. its size, structure and activities;
2. the nature of the personal information it handles;
3. the likely impact in the event the personal information was compromised;
4. its risk environment; and
5. relevant international standards.

Adobe Systems Software Ireland Ltd²

The Privacy Commissioner launched an investigation into Adobe following a statement on its website that it had been the target of a cyberattack. The Commissioner ultimately came to the view that Adobe had breached the Privacy Act by failing to take reasonable steps to protect all of the personal information it held. While the Commissioner found that Adobe generally took a sophisticated and layered approach to IT security, it had failed to implement consistently strong measures across all of its various internal systems.

Importantly, the Commissioner found that Adobe’s failure to implement consistently strong measures across all of its various internal systems was not reasonable given the resources available to Adobe. The attackers gained access to an Adobe backup system that was scheduled to be decommissioned. The exact details of the breach are ultimately not relevant to this discussion however in essence: the breach occurred because not all of the information on this backup system was encrypted. The Adobe investigation highlights that what is ‘reasonable’ will be different for every organisation, depending upon (amongst other things) the resources available to that organisation.

Cupid Media Pty Ltd³

In early 2013, attackers used a vulnerability in Cupid’s application server platform to make off with the personal information of approximately 254,000 Australian users. The Privacy Commissioner’s determination in this matter considered what would have been reasonable in the circumstances to

¹ ‘HW’ and Freelancer International Pty Ltd [2015] AICmr 86.
protect the personal information held by Cupid, focusing on Cupid's method of storing and securing passwords.

During the course of the investigation, Cupid advised the Commissioner that at the time of the breach the compromised passwords had been stored insecurely in plain text. The Commissioner considered that the storage of passwords in plain text constituted a failure to take reasonable security steps, and that Cupid should have employed basic encryption strategies – such as hashing and salting – that were available at the time of the breach. The Cupid investigation demonstrates that the Commissioner will not look kindly upon medium to large organisations that make no effort to employ basic password encryption methods.

In addition to the size of the organisation, the Privacy Commissioner was also influenced by the nature of the personal information stored by Cupid when determining what constituted 'reasonable steps' for the purposes of the Privacy Act. As Cupid stored information about customers' sexual and romantic interests, the Privacy Commissioner said that more stringent steps were required to secure this 'sensitive information'.

**Telstra Corporation Ltd**

In May 2013, the Privacy Commissioner commenced an investigation following reports – which had been confirmed by Telstra – that the personal information of Telstra customers had been made accessible online. The information was indexed by Google and made discoverable via Google search for just under a year after a third party provider inadvertently turned off the access controls on the source files.

In determining what constituted 'reasonable steps' for the purposes of the Privacy Act, the Privacy Commissioner gave weight to what he described as Telstra's 'heightened risk environment'. At the time of the breach, Telstra was undertaking a remediation program in response to a 2011 breach involving the same platform and, as a result, the Privacy Commissioner expected a heightened standard of care. The remediation program included decommissioning the third party provided platform and remediying certain deficiencies in Telstra’s practices and procedures.

**Running afoul of the Privacy Act**

Where it is established that an organisation has breached the APP's, the Privacy Act imposes a series of powers on the Office of the Australian Information Commissioner (OAIC) to:

1. order the respondent to take specified steps within a specified period to ensure that such conduct is not repeated or continued;
2. make a determination requiring the payment of compensation for damages or other remedies;
3. accept an enforceable undertaking;
4. seek civil penalties of up to (or apply for civil penalty orders of up to) $340,000 for individuals and $1.7m for companies; and
5. seek an injunction regarding conduct that would contravene the Privacy Act.

The Privacy Commissioner's ability to award compensation is broad. For example, section 52(1B) of the Privacy Act allows him to award damages for injury to the feelings and/or humiliation of the individual. Generally however the Privacy Commissioner has said he will be guided by the principles laid out in the

---

case of *Rummery and Federal Privacy Commissioner and Anor* in determining the appropriate amount of compensation, notably:

1. awards should be restrained but not minimal;
2. the principles of damages applied in tort law will assist, although the ultimate guide remains the words of the Privacy Act;
3. aggravated damages may be awarded; and
4. regard is to be given to the complainant's reaction, and not to the perceived reaction of the majority of the community or of a reasonable person in similar circumstances.

That said, the approach taken in determining the amount of the award is quite formulaic as the Commissioner makes an effort to ensure any compensation is relative to the compensation awarded in previous matters. For example, in *‘HW’ and Freelancer International Pty Limited* the Privacy Commissioner awarded the following amounts:

1. a fine of $15,000 taking into account the impact of the privacy breaches on the complainant, the multiplicity of the breaches, and that the improper disclosure was made to the general public; and
2. aggravated damages of $5,000 were imposed reflecting the repeated disregard the company demonstrated for the complainant's privacy rights and its own privacy obligations.

**Mandatory Notification Bill**

Currently, following a data breach, Australian organisations are not required to notify affected individuals or the OAIC. Breach notification is only mandatory under the *My Health Records Act 2012* (Cth) in the event of unauthorised access to eHealth information.

The Government has released a draft of amendments to the *Privacy Act 1988* (Cth) which will introduce a mandatory data breach notification regime, and intends to pass legislation for a mandatory data breach notification scheme by the end of 2016. This timetable may be impacted by the current federal election. However both the Liberal and Labour parties have committed to introducing data breach laws which should result in the legislation being finalised shortly.

Under the current draft Mandatory Notification Bill failure to comply with the notification obligations enliven the penalty framework under the Privacy Act which allows for civil penalties of $340,000 to be imposed for individuals and a maximum of $1.7 million for a body corporate.

The legislation requires notification of a serious data breach which occurs where there is unauthorised access to or disclosure of personal information and:

(a) access or disclosure will result in a real risk of serious harm; or
(b) any of the information is of a kind specified in the regulations.

Harm includes physical harm, psychological harm, emotional harm, harm to reputation, economic harm and financial harm. Real risk means a risk that is not a remote risk. The following factors are relevant in determining whether there is a real risk of serious harm:

1. the kind of information;
2. the sensitivity of the information;

---

7. [2015] AICmr 86.
3. whether the information is in a form that is intelligible to an ordinary person;
4. the likelihood that the information could be converted into a form that is intelligible to an ordinary person, if the information is not in a form that is intelligible;
5. whether the information is protected by security measures;
6. the likelihood that any security measures could be overcome;
7. the persons, or the kinds of persons, who have obtained, or could obtain, the information;
8. the nature of the harm; and
9. if the entity is taking steps to mitigate the harm, the likelihood of those steps succeeding

The Bill also has an extra territorial effect. Where an APP entity discloses personal information about one or more individuals to an overseas recipient and the overseas recipient holds that personal information, the Bill imposes the same legal obligations on that entity as if the information was still personally held by the APP entity.

The requirement to disclose a breach arises where an APP entity is aware, or ought reasonably to be aware, that there are reasonable grounds to believe that there has been a serious data breach of the entity. The notification is to be made as soon as practicable, though provision is made for an APP entity to investigate a breach to determine the extent of the intrusion so long as the investigation is completed within 30 days of the date the breach ought to have been identified.

The proposed legislation imposes a two tier notification threshold under which notification of a breach is to be provided to both the OAIC and the affected individuals. The notification provided by the APP entity should include:
1. a description of the breach;
2. information about the type of personal information involved;
3. steps the company has taken;
4. recommendations for individuals to mitigate any loss; and
5. contact details for information and assistance.

The draft Bill has been subjected to over 40 submissions in response, which have generally highlighted the need to ensure that the legislation clearly defines the threshold for a real risk of harm, and that further guidance is given to organisations in order to assess how they will meet their obligations under the proposed legislation.
Australia's regulatory response

ASIC
The Australian Securities and Investments Commission (ASIC) is responsible for regulating the Corporations Act 2001 (Cth) and the conduct of corporate entities in Australia. ASIC has shown a heightened interest in cyber risk and cyber resilience in respect of both the licensed financial services industry, and in the wider corporate community.

The strong message from ASIC is that the obligation to manage cyber resilience rests at the top, and that boards and directors must be alive to these risks. ASIC Chairman, Greg Medcraft on 26 November 2014 stated:

"Boards should also be alive to the risk of a cyber-attack as part of their risk-oversight role."

In March 2015, ASIC released Report 429 Cyber resilience: Health Check highlighting the importance of cyber resilience and setting out a list of 'Health Check Prompts' intended to assist organisations assess their cyber resilience. In its Corporate Plan for 2015-16 to 2018-19, released last August, ASIC also stated that cyber resilience will be one of its key focuses for the next three years.

In March 2016, ASIC released Report 468 Cyber resilience assessment report: ASX Group and Chi-X Australia Pty Ltd which used the NIST Framework to assess whether the ASX and Chi-X had sufficient resources to properly manage their cyber resilience. In addition to its assessment of the ASX and Chi-X, ASIC also engaged a number of other Australian financial organisations to self-assess their cyber resilience.

Amongst other things, ASIC identified ‘good practice’ as involving the board driven development of an appropriate framework to identify and manage cyber risks on an ongoing basis. As part of this framework ASIC has recommended organisations:

1. conduct periodic reviews of cyber strategy and educate board members about cyber resilience;

8 From a speech titled Conquering the new frontier: Regulating growth in the digital age, the full text of which can be found at: http://download.asic.gov.au/media/2278307/speech-to-the-bloomberg-address-sydney-published-26-november-2014.pdf.
2. specifically assess the individual risks relevant to the organisation’s business and determine what are its critical assets, and consider the consequences that the identified risks may have on the company's wider activities;

3. ensure boards have the appropriate skills and experience to have a strategic understanding of technology and its associated risks, or a background in cyber security;

4. develop risk-based assessment methods to ensure third party providers comply with security standards;

5. assess response strategies and examine what processes are in place for communicating effectively, internally and externally, and managing a breach situation;

6. adopt cyber awareness and training with a board driven cultural focus on cyber, including the development of organisation-wide training programs and conducting random staff testing; and

7. implementing the Australian Signal Directorate’s top four strategies, which include application whitelisting, patching applications, patching operating system vulnerabilities, and restricting administrative privileges.

Importantly, Reports 429 and 468 make it clear that ASIC is mindful of the actions overseas regulators are taking in relation to cyber resilience. In particular, ASIC appears to be monitoring regulatory developments in the US and the UK.

**OAIC**

The OAIC generally enforces the regulatory provisions under the Privacy Act which regulates how personal information is handled by government and private sector organisations. As part of its ambit, the OAIC has investigated a number of high profile Australian data breaches, and developed a framework and guidelines to assist an organisation in responding to a breach.

The OAIC also has the power to:

1. commence its own motion investigations into an act or practice that might breach the Privacy Act;

2. conduct a privacy performance assessment of whether an entity is maintaining and handling personal information in accordance with the Privacy Act;

3. request an entity to develop an enforceable code, and register codes that have been developed on the initiative of an entity, at the OAIC’s request or by the Commissioner directly;

4. direct an agency to give the OAIC a privacy impact assessment about a proposed activity or function; and

5. handle privacy related disputes and complaints.

The OAIC has released a data breach notification guide to handling personal information security breaches. The guide identifies four steps for organisations to consider when responding to a breach or a suspected breach, and provides guidance about notifying the individual or individuals affected by the breach.

Recently, there has been a dramatic increase in the number of determinations made by the OAIC under section 52 of the Privacy Act. Until 2014, the OAIC had made 2 determinations. Since 2014, the OAIC has made 10 determinations. Whilst the cause of this increase is unclear, it likely reflects an increase in

---

privacy complaints as well as a greater willingness on the part of the Privacy Commissioner to use its power to make determinations.

**APRA**

The Australian Prudential Regulatory Authority (APRA) regulates banks, credit unions, building societies, general insurance and reinsurance companies, life insurance, private health insurance, friendly societies, and most of the superannuation industry.

APRA has specific prudential guides relating to cyber issues – CPG 234 *Management of Security Risk in Information and Information Technology* and CPG 235 *Managing Data Risk*. These guides were released in 2010. The guides recognise that there is no 'one size fits all' approach to cyber risk management and this risk should be managed as a business would manage any risk, and should also take into account resource constraints.

At the Association of Superannuation Funds of Australia conference, APRA's General Manager of the South West region indicated that an area of significant interest for APRA during 2016 would be the extent to which superannuation funds were prepared for cyber security risks. He indicated that APRA would be conducting a thematic review of superannuation funds to collect more information about the processes that superannuation funds were putting in place to protect their funds and their members from cyber security breaches.

**ASX**

The Australian Securities Exchange Ltd (ASX) operates Australia's primary securities exchange, and provides guidelines and regulates the way in which listed entities must conduct themselves on the ASX. While the ASX has not released any direct statements concerning cyber security there has been significant recent debate on whether a cyber event would enliven the continuous disclosure obligations under the ASX listing rules.

ASX Listing Rule 3.1 requires an entity to immediately tell the ASX once it becomes aware of any information a reasonable person would expect to have a material effect on its share price. A reasonable person would expect information to have a material effect on an entity's share price if the information would, or would be likely to, influence investors in dealing with that security.

There remain a number of untested issues concerning what liabilities will arise as a result of a breach, and the impact a data breach is likely to have on a listed company's share price. However, where a significant data breach has occurred, or the information is critical to the business operations it is very likely that market disclosure will be required.

ASIC is alive to the possibility that a cyber-attack might amount to the release of market-sensitive information and has cited research done by Freshfields Bruckhaus Deringer that found significant loss was suffered by global listed companies hit by cyber-attacks between January 2011 and April 2013 and that affected companies took an average of 24 days to recover to the pre-crisis valuation.

---

In the US, the SEC has issued a Disclosure Guidance document in 2011 that makes it clear material information regarding cyber security risks and cyber security incidents must be disclosed.\textsuperscript{11} It remains to be seen whether the ASX will implement a similar guideline.

Third party liability

At the present time, no litigation has been filed in Australia arising from data breaches. This is in some ways surprising given the growing awareness of the risks to organisations caused by data breaches and the catastrophic losses that can arise for companies that suffer intrusions. Possible reasons why Australian litigation has been slow include:

1. Australian law does not recognise a common law tort or right of privacy. This limits potential claims to more difficult actions under negligence, breach of contract, and misrepresentation; and
2. Australia is yet to implement a mandatory data notification regime. In both the United States and Canada the implementation of notification requirements resulted in a significant increase in litigation, as the laws increased consumer awareness when personal information had been exposed, and initiated regulatory activity.

Globally however the rate of data breach litigation is increasing and it will only be a matter of time before matters are litigated locally. For this reason the best guidance on how litigation risk is likely to develop in Australia is obtained by considering other jurisdictions where the litigation has become common place, particularly in the United States and Canada.

Case study of Home Depot litigation

One of the most high profile incidents demonstrating the extent of regulatory and legal risks for companies that suffer data breaches is the intrusion suffered by Home Depot that compromised the payment and email records stored in its system between April and September 2014.

The incident allegedly put at risk approximately 56 million unique payment card records stored by Home Depot. The information at risk includes customer names, addresses, account numbers, card expiration dates and card verification information used in connection with purchases made between April 2014 and September 2014, as well as 53 million email addresses. Press reports suggest the malware behind the Home Depot incident, which has been dubbed 'Mozart', was uniquely tailored to hide on Home Depot's system. It has been alleged the hackers subsequently on-sold the information to various third parties who made fraudulent transactions with credit and debit cards issued to Home Depot customers.

According to a Home Depot press release on 6 November 2014, the hackers used a vendor's user name and password to enter Home Depot's network and then acquired elevated rights that allowed them to deploy custom malware on self-checkout systems.

This cyber breach has generated at least 31 US consumer class actions, four Canadian consumer class actions, 22 US financial institution class actions, seven US regulatory inquiries, and a shareholder derivative action.
The US class actions were consolidated and in January 2015 the District Court for the Northern District of Georgia created separate tracks for the consumer and financial institution class actions.

**Consumer class actions**

The plaintiffs in the US and Canadian consumer class actions typically allege Home Depot relied on outdated security measures and failed to notify in a timely way customers whose private information may have been compromised. *Marko, et al. v. Home Depot USA Inc.*\(^{12}\) also asserts that Home Depot promised to safeguard its customer's data and permitted unauthorised access of its customers' personal information from April of 2014 to at least September 2.

The consumer plaintiffs assert causes of action for violations of state and federal consumer protection laws and rely on unfair business practices laws, state data breach statutes, negligence, unjust enrichment, bailment, breach of privacy, breach of fiduciary duty, and breach of contract. The complainants seek compensatory damages, equitable relief, restitution, attorneys' fees, statutory damages and punitive damages. The statutory damages sought include $100 to $1,000 per wilful violation of the *Fair Credit and Reporting Act (FCRA)* and $1,000 per violation of the *Stored Communication Act*.

In the 2014 to 2015 Financial Year, Home Depot recorded US $63,000,000 in expenses related to the data breach, which it partially offset with US $30,000,000 of expected insurance proceeds.

In March 2015 Home Depot paid US $19,500,000 to settle the class action litigation. Of this amount, US $13,000,000 was paid to customers for out-of-pocket losses, and US $6,500,000 was allocated to provide 18 months of cardholder credit monitoring and identity protection services.

**Financial institution actions**

The banks and credit unions bringing these actions assert that Home Depot's security failed to comply with Payment Card Industry Data Security Standards (*PCI DSS*) and caused banks to incur loss for card replacement and subsequent fraud. Most of the financial institution class action complaints only include causes of action based on negligence. The *American Bank of Commerce* alleged Home Depot fraudulently benefitted from its failure to comply with PCI DSS by shifting the risk of fraudulent charges to financial institutions. Consequently, this complaint asserts causes of action for violations of the *Racketeer Influenced and Corrupt Organizations Act* and breach of contract in addition to the usual negligence charges.

Whilst there is no available information on the likely amount that Home Depot will need to pay to settle these claims, in the recent *Target* data breach which compromised 40,000,000 customer records, it has been estimated *Target* paid over US $87,250,000 to settle the claims brought against it by financial institutions including the payment card networks.

**Regulatory actions**

Following the incident, Home Depot was subject to investigations by the US House and Senate, the New York State Attorney General and a multistate group of state Attorney Generals comprised of forty-

---
12 Case No. 3:14-cv-00981.
three states and the Manhattan District Attorney. There has also been repeated speculation that the Federal Trade Commission will launch its own investigation.\textsuperscript{13}

In its public filings with the SEC, Home Depot acknowledges that the risk of litigation claims and regulatory investigation is likely to impact its financial condition, financial results and cash flows in the future.

**Understanding the risk of litigation following data breaches**

In March 2014, a detailed study of data breach lawsuits was undertaken by Romanosky, S., D. Hoffman, and A. Acquisti\textsuperscript{14}, which identified key trends and found that:

1. of 1,772 US data breach observed in their study, 65 (3.7\%) had been litigated. It was however 6 times more likely for litigation to occur where individuals financial information had been compromised by the breach;
2. plaintiffs who litigated following a data breach would generally seek relief for actual loss from identity theft (e.g., financial or medical fraud), emotional distress, cost of preventing future losses (e.g., credit monitoring and identity theft insurance), and the increased risk of future harm;
3. defendants were typically large firms such as banks, medical/insurance entities, retailers, or other private businesses;
4. 52\% of data breach litigation settled prior to a final determination;
5. the vast majority of data breach lawsuits terminate before trial, either through dismissal (motion to dismiss or summary judgment) or by settlement. Only 2 of the 230 litigated claims observed resulted in a favourable trial finding for the plaintiff;
6. class certification is a significant impediment for plaintiffs, however of the cases that achieved class certification, 85 percent settled, whereas when the class was not certified, only 48 percent settled;
7. firms had a significantly greater risk of being sued where:
   a. individuals suffered financial harm following a data breach;
   b. the defendant firm was responsible for improperly disclosing data to outside parties;
   c. the information compromised related to health or credit card records or financial information which were generally subject to higher statutory protection or protected through contractual mechanisms; and
   d. a large number of records had been compromised by the breach. The mean number of records compromised in the observed breaches that had been litigated was around 5.3 million.
8. Firms had a reduced risk of litigation where:
   a. credit monitoring was provided to those affected by the breach;
   b. where there was no tangible evidence third parties had suffered financial loss from the breach; or
   c. breaches were due to lost/stolen hardware.


Claims by individuals for breaches: the overseas experience

A wide range of litigation has been commenced by individuals in the US who were affected by data breaches. Around 76% of these actions taking the form of class actions, under which collective redress is sought on behalf of multiple individuals who have sustained the same injuries from the breach.

By and large the majority of US claims by individuals affected by data breaches have relied on negligence however statutory claims, breach of implied contract and negligent misrepresentation have also been asserted. US plaintiffs have faced an uphill battle making out many of the elements required for a successful negligence claim.

**Duty of care**

There is US authority to the effect that organisations will owe a duty to individuals to take reasonable steps to protect their information. In *Bell v Michigan Council* 2005 25 MICH. APP. LEXIS 353 (Mich. C.A.) the Michigan Court of Appeals, with one judge dissenting, affirmed a $275,000 jury verdict against a union whose members suffered identity theft. In its reasoning the majority held that the "defendant did owe plaintiffs a duty to protect them from identity theft by providing safeguards to ensure the security of their most essential confidential and identifying information."

Further, in *In re: Sony Gaming Networks and Customer Data Security Breach Litigation* 2014 BL 15530, (S.D. Cal., No. 3:11-md-02258-AJB-MDD, partially dismissed Jan 21, 2014), at pp. 21-22. the Court found there was a duty imposed on commercial organisations to safeguard confidential information entrusted to them by their customers:

> Although neither party provided the Court with case law to support or reject the existence of a legal duty to safeguard a consumer's confidential information entrusted to a commercial entity, the Court finds the legal duty well supported by both common sense and California and Massachusetts law.

> "A basic principle of negligence law is that ordinarily everyone has a duty to refrain from affirmative acts that unreasonably expose others to a risk of harm."

Conversely however in the recent case of *Dittman v. UPMC* No. GD-14-003285, a Pennsylvanian trial court dismissed a data breach class action law suit finding that no common law cause of action existed against parties who fail to protect personal information. While this decision relied mainly on Pennsylvania's economic loss doctrine – which prevents plaintiffs from using the law of negligence to recover pure economic loss - the Court also cited public policy considerations in favour of not imposing a duty:

> The creation of a private cause of action could result within Pennsylvania alone of the filing each year of possibly hundreds of thousands of lawsuits by persons whose confidential information may be in the hands of third persons. Clearly, the judicial system is not equipped to handle this increased caseload of negligence actions. Courts will not adopt a proposed solution that will overwhelm Pennsylvania's judicial system.

The US Courts have also accepted claims may be possible under the negligent misstatement doctrine, for example in *In re TJX Companies Retail Security Breach Litigation*, 2007 BL 15530, (S.D. Cal., No. 3:11-md-02258-AJB-MDD, partially dismissed Jan 21, 2014), at pp. 21-22. The creation of a private cause of action could result within Pennsylvania alone of the filing each year of possibly hundreds of thousands of lawsuits by persons whose confidential information may be in the hands of third persons. Clearly, the judicial system is not equipped to handle this increased caseload of negligence actions. Courts will not adopt a proposed solution that will overwhelm Pennsylvania's judicial system.

The US Courts have also accepted claims may be possible under the negligent misstatement doctrine, for example in *In re TJX Companies Retail Security Breach Litigation*, 2007 BL 15530, (S.D. Cal., No. 3:11-md-02258-AJB-MDD, partially dismissed Jan 21, 2014), at pp. 21-22.

---

17 No. GD-14-003285.
misstatement would require plaintiffs to establish their justifiable reliance upon information or statements made by the defendant, and the defendant's failure to exercise reasonable care or competence in obtaining or communicating that information.

**Reasonable standard of care**

A further challenge in these cases is the limited guidance as to what constitutes a reasonable standard of care in protecting information. For example in *Guin v. Brazos Higher Education Service* the Court found that the defendant had not been unreasonable in allowing an employee to take data home on a laptop. Conversely however in *Bell v. Michigan Council*, the Court found that it was unreasonable for the defendant to allow an employee to take data home on a laptop.

**Causation**

To establish a right to recover damage, a Plaintiff must establish that the damage they have suffered was caused directly by the Defendant's conduct. US Courts have been reluctant to infer causation. In *Stollenwerk et al v. Tri-West Healthcare Alliance* plaintiffs sought to recover loss after they suffered identity fraud several weeks after hard drives were stolen from Tri-West's offices. The Court was unwilling in this case to infer causation and draw a link between the two events, saying that the mere fact the identity theft occurred after the drives were stolen was insufficient. As the same information had been provided to a number of different other organisations, Her Honour thought that it would be unreasonably speculative to infer causation.

Plaintiffs may need extraordinarily good evidence of causation in order to be successful. In *Bell* the plaintiffs were successfully able to prove causation using a notebook that had been found in the possession of the identity thief. The notebook contained their personal information and detailed all of the fraudulent purchases that had been made in their names.

**Proof of loss and damage**

A further challenge observed in these cases is that to succeed in a claim, plaintiffs must demonstrate they suffered 'actual damages' as a result of the breach. In some instances US courts have been unwilling to accept arguments that plaintiffs might suffer identity theft as a result of the defendants' negligence, taking the view that these arguments are too speculative.

The majority of the case law in the US has taken the view that a plaintiff does not suffer 'actual damages' until they suffer some identity theft. Importantly, the effect of this is that plaintiffs have no entitlement to recover monitoring or other mitigation costs they have incurred if they do not suffer some actual identity theft. Recently however the U.S. District Court for the Central District of California in *Corona v Sony Pictures Entertainment, Inc.* held that the plaintiffs had a 'cognizable injury' as it is termed under Californian law where the plaintiff is exposed to credit monitoring costs, identity theft protection and penalties.

---

19 Civ. No. 05-668, 2006 U.S. Dist. LEXIS 4846 (Dist. Minn.).
21 2005 U.S. Dist. LEXIS 41054 (Dist. Ariz.).
Pure economic loss

A further challenge for the Plaintiffs is that (generally speaking) the only exposures arising for individuals following a data breach is the potential that they sustained pure economic or financial loss, as opposed to property damage or physical harm. A number of US states have found that purely economic losses are unrecoverable in tort or any action asserting strict liability in the absence of personal injury or property damage.\(^{24}\)

As seen in *Corona* however there are certain exceptions, for example where a special relationship exists between the parties. In *Corona*, the plaintiffs were all either current or past employees of Sony. Following *J'aire Corp. v. Gregory*\(^{25}\) the Court decided that this employer/employee relationship was sufficient to establish a special relationship that provided an exception to the economic loss doctrine.

Class certification

Plaintiffs have experienced difficulty in satisfying the US Class Action Certification requirements,\(^{26}\) which is a necessary step to bring litigation on behalf of a group of Plaintiffs. Plaintiffs typically have the most difficulty demonstrating they have sufficient "questions of law or fact common to class members".

Claims by individuals in Australia

There is no direct authority in Australia on whether data breach claims by affected individuals will succeed. There are however a number of features of our laws which suggest the claims by individuals may be easier to establish in Australia.

A key aspect of data breach litigation is that generally claims by individuals seek remedy for pure economic loss, as a plaintiffs injury is financial and is not tied to some personal injury or property damage suffered by the plaintiff. Australian courts are more open to allowing recovery of pure economic loss where a duty of care is established and a defined class of plaintiffs is determinable.\(^{27}\)

In Australia there are no cases considering whether an organisation owes a duty of care to protect individuals' personal information, and a court will be required to consider whether a novel category of duty of care should be established. This will turn on whether a plaintiff can satisfy the salient features test\(^{28}\) which requires consideration of the following elements:\(^{29}\)

1. the foreseeability of loss,
2. whether a duty of care could expose a defendant to liability to an indeterminate class or in an indeterminate amount or for an indeterminate period;
3. an individual's vulnerability to risk; and
4. the defendant's knowledge of that risk and its magnitude.

In practice, were a large scale data breach to occur in Australia, a number of aspects of the salient features test are likely to be satisfied given:


\(^{26}\) Federal Rule of Civil Procedure 23. Rule 23(a) require that to obtain class certification the litigation must exhibit (1) numerosity, (2) commonality, (3) typicality and (4) adequacy. Rule 23(b) sets out further requirements, as discussed.

\(^{27}\) See Caltex Oil (Australia) Pty Ltd v Dredge "Willemstad" (1976) 136 CLR 529.


\(^{29}\) Woolcock Street Investment Pty Ltd v CDG Pty Ltd (2004) 216 CLR 515.
1. once information has been collected about individuals, they cannot take steps to protect themselves and are vulnerable if the organisation does not have proper systems in place system to protect this data;

2. companies will likely be found to have known of the reliance put on them by individuals and should foresee that damage or harm could result if the information was not protected given the wide publication of data breaches and the harm which they cause;

3. companies also exercise a high degree of control over the risk of harm which will often be a by-product of their own data breach security; and

4. whilst there may be a wide class of plaintiffs the class is unlikely to be indeterminate, as the class will be formed by the specific individuals who the organisation kept information about.

Plaintiffs will however face challenges where there is no action taken by a company to assume responsibility for individual's data, or if a company does not represent that it would hold information subject to security protections. Difficulties may also arise if a class of potential plaintiffs become too wide or indeterminate.

Cases by individuals in Australia are likely to be run as class actions, and Australia’s class action regime is generally considered to be friendlier for litigants than the US regime. The requirements plaintiffs must meet in order to commence and conduct a class action in Australia are set out in section 33C of the Federal Court of Australia Act 1976 (Cth) and generally require claims to arise out of the same or related circumstances and give rise to a substantial common issue of law or fact. These threshold requirements have been interpreted liberally by the Courts and accordingly are not difficult for plaintiffs to satisfy.

A difficulty Australian plaintiffs will face is establishing that where a data breach has occurred, the organisation failed to take reasonable steps to prevent the harm. The reasonable standards test is objective and turns on what steps a hypothetical objective person would have taken in the place of the defendant. Concepts of what is reasonable may be problematic in the world of data security given there are evolving debates concerning the most appropriate risk strategies, and what will be reasonable will vary based on the circumstances of each company, including the resources available to the company, its type of business and the specific information it holds.

Plaintiffs will also be challenged in establishing causation, and demonstrating a causal connection between a failure to protect data and their physical injury. The plaintiffs will have to prove on the balance of probabilities that their injury was caused by the alleged data breach, as opposed to any other intervening cause, and that it is appropriate to extend the scope of a defendant's duty. Causation is most likely to be satisfied where some actual fraud occurs closely following the data breach. Where however there is a longer timeframe involved, or there are intervening actions of third parties, a causation case will be more difficult to make out.

The implementation of Australia’s mandatory notification regime is likely to have a significant impact on litigation by plaintiffs, as data breach notifications will provide plaintiffs with the information they require to progress claims, and facilitate class actions. In the US higher rates of litigation were observed once data breach laws were implemented.
Actions by financial institutions: the overseas experience

Claims by financial institutions present a greater risk than claims brought by individuals due to the heightened loss financial institutions sustain in the aftermath of a breach, and also because these claims are not subject to the same weaknesses as underlying claims made by individuals.

Claims by financial institutions generally seek damages for:

1. costs incurred in notifying customers of an organisation's data breach and the potential for identity theft;
2. costs of cancelling and reissuing credit cards for customers potentially affected by the data breach;
3. costs of reimbursing customers for fraudulent transactions committed following the breach;
4. costs of monitoring customer accounts to detect and prevent fraudulent charges;
5. costs of resolving customer complaints resulting from the data breach; and
6. loss of interest, transaction fees, and other charges and fees arising as a consequence of the data breach.

The majority of claims are run as negligence actions on the basis that the breached organisation failed to exercise reasonable care in securing, storing and using personal information, and breached the statutory laws governing disclosure of consumer and credit information.

The claims by financial institutions represent a greater risk to companies both in quantum, and the risks of litigation succeeding. A significant reason for this is because financial institutions can point to tangible costs which they will incur in the course of cancelling and reissuing cards, and resolving client fraud. It has been estimated that following the Target data breach, it cost the financial institutions up to US $10 per card to issue replacement cards to customers affected by the breach and that over 15,300,000 cards were reissued following the incident.

Financial institutions are also able to use aggregated data to measure the increase in fraudulent activity that may arise concerning their customers after a data breach. In addition, financial institutions following the Home Depot breach have also alleged damages for lost interest and transaction fees due to reduced card usage resulting from the breach. These claims are however more speculative.

Finally, claims have also been brought by payment card networks such as Visa and MasterCard that require merchants who use their payment cards to comply with the Payment Card Industry Data Security Standard (PCI-DSS), which establishes information security standards for payment processes, systems, networks, software and applications. Merchants who fail to comply with PCI-DSS are subject to fines and reimbursement assessments from the payment card companies. Although the fines vary depending on the volume of payments processed by the merchant and the number of violations, companies that experience a data breach can be fined and subject to a reimbursement assessment of millions of dollars.

---

**Actions by financial institutions in Australia**

There has been no data breach litigation by financial institutions in Australia, and a significant issue the Australia courts will need to grapple with is whether an organisation's duty of care should extend to protecting financial institutions from the consequential fraud and losses, which are arguably a more remote by-product of a data breach than the damages sustained by individuals whose information is lost. As a class of Plaintiffs, financial institutions may be considered too indeterminate to satisfy the salient features test. Plaintiffs may however be able to point to some form of physical damage, taking into account the actual costs and physical steps involved in replacing credit cards.

It is arguable that there are public policy reasons for financial institutions to recover these losses given the Privacy Act imposes statutory duties to protect personal information, and where reasonable steps have not been taken the breach of these statutory duties will be a direct cause of the financial institution loss.

Claims by Payment Card Networks and PCI-DSS are also likely to represent a very significant risk for Australian companies given these companies can rely on contractual provisions with merchants that include indemnification for third party losses incurred by banks and credit card issuers.

**Indemnification litigation**

There is potential for entities that sustain a data breach to recover damages from third parties that are responsible for the intrusion. Each of these cases will turn on its own facts and the specific contractual and factual relationship between the parties. While there is limited reported judicial consideration in any jurisdiction, in the US cases this issue has been explored where an organisation claimed a credit card processing system sold to it did not comply with industry regulations and caused a data breach.\(^{33}\) These claims are likely to be more common, particularly as organisations become more exposed to third party claims and reliant on recovery of their own losses.

**Shareholder class actions: the US experience**

Shareholder class actions in the US are a new phenomenon, and there are relatively few cases. For the most part, the shareholder class actions resulting from data breaches have been derivative actions brought by shareholders on behalf of the entity against its directors and/or executives.

Whilst there have been securities class actions resulting from data breaches, these actions are inherently less likely because the US has periodic – rather than continuous - disclosure requirements.

**Wyndham case**

Between April 2008 and January 2010, attackers gained access to the Wyndham computer network on three separate occasions using a brute force attack to access an administrator's account and collect data.

The FTC brought an action against Wyndham (under s5(a) of the FTC Act\(^ {34}\)) for Wyndham's failure to maintain reasonable and appropriate data security measures for consumers' sensitive personal information.\(^ {35}\) The FTC alleged the breach was the result of a failure: \(^{36}\)

---


\(^{34}\) Section 5(a) of the FTC Act prohibits "unfair or deceptive acts or practices in or affecting commerce."

\(^{35}\) FTC v. Wyndham Worldwide Corporation, et al., Civil Action No. 13-1887 (ES).
1. Protect customer data through the use of firewalls;
2. Encrypt credit card information;
3. Use up to date software that can receive security updates;
4. Use default passwords that were not widely known;
5. Use complex passwords instead of easily guessed passwords;
6. Keep track of the computers connected to its network; and
7. Employ reasonable measures for detecting and preventing intrusions.

The FCT’s action resulted in a shareholder derivative action against Wyndham’s board of directors, president/CEO and general counsel alleging that, amongst other things, they had breached their fiduciary duties by failing to:
1. Implement adequate data security mechanisms and internal controls to protect consumers’ information; and
2. Disclose the breaches to shareholders in a timely manner.

The derivative action was however dismissed in October 2014 on procedural grounds that appear to be the main obstacle for US plaintiffs in bringing a derivative action. Before filing a derivative action, shareholders are required to send a letter of demand to the board requesting they commence an action against the entities responsible for the harm in issue. The Wyndham Board unanimously refused two letters of demand that had been sent by the shareholder plaintiffs. As the board had unanimously refused the two letters of demand, the Court in Wyndham dismissed the shareholders’ action because the board’s refusal to pursue the proposed lawsuit was an exercise of business judgement made in good faith.

**Target case**

Similar issues have plagued the shareholder derivative actions brought in response to the Target data breach in late 2013, where attackers gained access to the personal information of up to 70 million customers. Following the breach, shareholders commenced 4 derivative actions (which were later consolidated) against Target’s 12 directors, CFP and former CIO and Target itself. They alleged that the directors and officers caused injury to Target by failing to prevent the data breach and failing to cause Target to announce the breach as quickly as it should have. They are currently seeking unspecified damages and improvements to Target’s corporate governance and internal procedures, alleging breach of fiduciary duty, waste of corporate assets, gross mismanagement and abuse of control.

Since the suit was filed, there has been little movement because – as was the issue in Wyndham – US law requires shareholders to demand the board bring the suit. For obvious reasons, this procedural requirement is problematic. When directors’ decisions are protected by a business judgement rule, shareholder plaintiffs in derivative suits have little chance of convincing a board of directors to commence an action against themselves.

The shareholder plaintiffs in Target attempted to get around this procedural requirement by alleging that a demand on the board would be futile. All parties however agreed to a stay in the proceedings in June 2014 to allow time for a special litigation committee appointed by Target to investigate the breach and

---

determine whether and to what extent Target should pursue the litigation. Whilst the investigation was to be concluded by November 2015, it appears the report is yet to be handed down.

Whilst it is currently unclear what the outcome of this case will be, it is clear that the cost to Target in defending this litigation has been massive. In its last status report, the special litigation committee noted that it had to date hired independent counsel and experts, met 75 times, conducted just under 60 interviews and reviewed nearly 100,000 documents.

**Heartland case**

The *Heartland* case differs from the *Wyndham* and *Target* cases in that the plaintiffs brought a securities class action suit against Heartland, rather than a derivative suit.

Following a 2008 data breach in which attackers made off with 130 million credit and debit card numbers, shareholder plaintiffs filed a securities class action suit against Heartland and its CEO and CFO. The plaintiffs alleged that the defendants had falsely stated in Heartland's annual report that:

1. Heartland "place[d] significant emphasis on maintaining a high level of security"; and
2. maintained a network that "provide[d] multiple layers of security to isolate [its] database from unauthorized access."^{37}

Considering Heartland's commitment to data security (essentially the money it had spent on cyber security generally and the fact Heartland did take steps to bolster its security after an earlier breach), the Court found that the statements were not false and that Heartland likely did place a high emphasis on security but was overcome nonetheless.^{38}

**Summary**

The *Wyndham* and *Target* cases demonstrate that derivative suits confront procedural problems that are potentially too significant for derivative suits to provide a reliable remedy for shareholders in the event of a breach.

Similarly, provided entities are alive to the comments they are making in their annual reports, periodic disclosure shareholders are unlikely to be reliably successful in securities class actions. As in the *Heartland* case for example, plaintiffs are likely to have difficulty demonstrating the entity did not "place significant emphasis" on cyber security.

**Shareholder actions in Australia**

**Overview**

Shareholder class actions are potentially more likely to succeed in Australia.

The majority of the securities class actions in Australia assert either misleading or deceptive conduct or breach of continuous discourse obligations (sections 1041H and 674(2) of the Corporations Act 2001 (Cth) (CA) respectively). Damages are claimed typically under sections 1041I, 1317HA and 1325 of the CA.

---

^{37} *In re Heartland Payment Systems, Inc. Securities Litigation* Civ. No. 09-1043.
^{38} *In re Heartland Payment Systems, Inc. Securities Litigation* Civ. No. 09-1043.
ASX Listing Rule 3.1 requires an entity to immediately tell the ASX once it becomes aware of any information a reasonable person would expect to have a material effect on its share price. It is likely that information regarding a significant data breach would be material. There have been a number of articles arguing that data breaches do not affect share prices, however these articles take a long-term view. It is not relevant to the materiality consideration that 1, 3 or 5 years after the announcement a company's share price may have recovered. Evidence of a short-term price reduction will be sufficient to bring a class action.

Entities are required to disclose a breach when 'aware' of the information. Under ASX Guidance Note 8, an entity is not taken to be 'aware' of information until it has come into possession of sufficient information about the event or circumstance in order to be able to appreciate its market sensitivity. This creates a dilemma: directors want any disclosure they make to be as full and as complete as possible, however the obligation to disclose the breach may arise before this information is available to them. In normal circumstances, entities would be able to rely upon the third carve out (confidentially), however in the case of a data breach confidentiality is not satisfied.

In this event it is likely that the most appropriate course of action will be to call a trading halt to allow the company to gather more information so that when they do ultimately make disclosure, the information they give the market is more complete and meaningful. The David Jones case in 2012 shows the dangers of early and incomplete disclosure.

**Fraud on the market**

Fraud on the market can be relied upon by US plaintiffs in securities class actions to make certification and to prove causation. In *Basic v Levinson*, the US Supreme Court held that plaintiffs are entitled to a rebuttable presumption that the market was efficient and that they traded in reliance on the integrity of the market price. That is, they are entitled to the presumption that the market price will reflect any misrepresentations and therefore individual shareholders do not need to prove direct reliance on a misrepresentation.

Whilst the majority of recent securities class actions filed in Australia have pleaded indirect market-based causation arguments, there has been a lack of proper and full judicial consideration on the matter until recently. In the New South Wales Supreme Court case of *Re HIH Insurance Ltd (In Liq)* (HIH), the Judge found that notions of indirect causation were sufficient to make out causation.

---


Legal issues arising from response strategies

Privilege

In the event of a data breach, organisations often retain experts to investigate the breach, resulting in an assessment of what went wrong, what data was compromised, response strategies and potential weaknesses in internal systems. As the risk of legal and regulatory claims arising from data breaches grows, protecting and claiming privilege over these sensitive reports will be critical in protecting the company's interests.

There are currently no Australian authorities that consider privilege in the context of data breach investigations. Legal challenges have however been instituted by plaintiffs in two prominent US cases, namely Genesco, Inc. v. Visa U.S.A. Inc (Genesco) and In re: Target Corporation Customer Data Security Breach Litigation (Target). A short summary of each is set out below.

In Genesco, the plaintiff demanded documents produced by an independent forensic investigation conducted following a data breach. The court refused production and found privilege existed in communications between solicitors and technology experts, where those experts had been retained to assist the solicitor's investigations.

In Target, following a catastrophic breach the company claimed privilege over investigation and expert documents that were used to assist and educate Target's solicitors so they could provide legal advice and manage anticipated claims. Privilege over these documents was challenged on the basis that Target would have investigated the breach regardless of any legal risks in order to appease customers, ensure continued sales, discover vulnerabilities, and prevent future breaches. The District Court of Minnesota mostly upheld Target's privilege claim on the basis that expert investigations were necessary for Target's lawyers to prepare to defend the company in litigation that was reasonably anticipated to follow.

Under Australian common law, legal privilege has two distinct limbs: ‘advice privilege’ and ‘litigation privilege’. These limbs are narrower than the scope of privilege available in other jurisdictions such as the US and so while US law may serve as guidance for the Australian Court, it is not binding. The relevant test to establish privilege is that a document must have been created for the dominant purpose of obtaining legal advice, or for use in current or anticipated litigation (Dominant Purpose Test).

44 2013 U.S. Dist. LEXIS 101503.
45 MDL No. 14-2522 (PAM/JJK).
In addition to the common law, the right to claim privilege in Australia is also influenced by the Evidence Acts and the Court Procedure Rules adopted across the various jurisdictions. These statues can significantly affect privilege as under Queensland's Court Rules a statement or report of an expert cannot be privileged from disclosure in litigation. This contrasts with the law in New South Wales where expert reports will be privileged under common law if the Dominant Purpose test is satisfied and privilege has not been waived.

Before advice privilege or litigation privilege can exist, a client must retain a solicitor to act for them. Once a solicitor is retained, a privilege strategy should be implemented quickly as privilege issues turn on the circumstances existing at the time each individual document was produced. If a document was created before solicitors were retained, then privilege is less likely to exist.

In Australia, advice privilege is confined to communications between a lawyer and a client, or a communication made by a third party adviser to a lawyer for the "dominant purpose" of the client obtaining legal advice. Advice privilege has been narrowly construed and will not exist if a court considers a document would have been brought into existence for other commercial purposes, irrespective of the need for legal advice.

Litigation privilege protects documents brought into existence for the "dominant purpose" of anticipated use in legal proceedings. This is often found to have wider application than advice privilege.

The Dominant Purpose Test must be satisfied in either case and the test turns on the reasons why a document was created. This includes the intentions of the parties, the potential threat of litigation, the nature of any previous dealings between the parties, and whether a document was driven by internal or collateral motivators.

Whether documents created as part of an investigation after a data breach will be subject to privilege will depend on the reasons for their creation. What form an investigation will take, and what documentation and reports are necessary will ultimately rely on the specific risks to the business arising from the breach, and the purpose behind the investigation. This can create challenges in asserting privilege because during the investigation there will be competing priorities, demanding different reactions and responses as an organisation's management of a breach must:

1. assess the extent of damage to IT systems and its impact on the ongoing business;
2. consider the potential for liability under the Privacy Act 1988 and other relevant legislation and whether reasonable steps were taken to protect personal information;
3. direct response strategies and determine steps to mitigate damage;
4. remedy weaknesses in internal controls to prevent further intrusion;
5. consider the risk of future legal claims by third parties whose information has been compromised, or who will suffer consequential loss from the breach;
6. prepare for regulatory investigations that may be instituted by the Office of the Privacy Commissioner, the Australian and Securities and Investment Commission or other industry regulators;
7. consider liability under the Payment Card Industry (PCI) scheme, if applicable;
8. manage damage to the company's reputation and relationships with key stakeholders;
9. comply with the mandatory disclosure regime Australia will shortly adopt; and
10. consider potential insurance claims.
Some of these drivers will respond to the legal risks arising from the breach and these will support a right to privilege over documents generated by an investigation. Other motivators will have their origin in internal or commercial factors that will not support the ability to claim privilege. The Dominant Purpose Test is then more difficult to satisfy.

It is not possible to guarantee records will be privileged following an intrusion, however the following steps will improve the prospects of a privilege claim.

The starting point a court will often use when considering privilege is the nature of any instructions given to an investigating third party. To help satisfy the criteria of the Dominant Purpose Test an expert's instructions should:

1. be prepared and issued by the organisation's solicitors, and letters of instructions should be marked as privileged communications;
2. demonstrate that the organisation has considered its long term risks and the legal implications that may arise from the data breach, including liability to third parties;
3. identify that the organisation has retained solicitors, and include the solicitors as party to any expert retainer;
4. specify how the expert's work is tied to the organisation's legal obligations and exposures;
5. focus the expert's work on identifying the cause and extent of the breach and only as a subsidiary issue consider matters such as system improvement and any internal management issues; and
6. highlight that the expert's role is to work closely with and provide assistance to the organisations solicitors.

A privilege strategy should also be developed with solicitors and implemented consistently to manage both third parties and internal documents that are generated. As part of this strategy consideration should be given to the entire scope of documents that will be produced, and the potential for common interest privilege to be claimed, where documents will be relied by both insurers and their insureds.

A privilege strategy should also distinguish between the tasks that are undertaken for commercial and non-legal purposes as the documents created for these purposes are unlikely to satisfy the Dominant Purpose Test. In some instances parts of the investigation work may need to be isolated and kept separate so it will not weaken the right to assert privilege over other documents.

Finally, it is also necessary to manage the circulation of privileged documents and to avoid the document being misused or disclosed in a manner that could waive privilege. For example where parts of documents are copied or used in different contexts a right to privilege could be lost.

**Insurance**

In Australia there is a growing market for Cyber Insurance Policies which generally cover the costs of forensic investigations, cyber extortion, data restoration, regulatory costs, breach notification expenses, credit monitoring, business interruption and litigation risks. Internationally, insurance response has been a key resource to assist companies in managing a data breach and managing financial loss.

Assessing and resolving coverage issues is a complex area where specialist advice should be sought, however an issue for companies will be ensuring they have an adequate insurance program, and that sub limits and indemnity amounts are sufficient. The potential application of policy retroactive dates needs active review, particularly as breaches can go undetected for a long period of time.
Another issue for companies is the extent to which traditional policies may respond to a data breach. In *Landmark American Insurance Co v Gulf Coast Analytical Labs. Inc*\(^{46}\) a policyholder sought coverage under a property insurance policy after data on its hard drive storage system had become corrupted. The court found that the property policy would respond and held that electronic data has physical existence and can be observed, altered or damaged through physical interaction.

Similarly in the Australian case of *Switzerland Insurance Australia Ltd (formerly The Federation Insurance Ltd) v Dundean Distributors Pty Ltd*\(^{47}\) the court allowed recovery under a property insurance policy where as a result of a power outage, the operating and accounting software became corrupted and accounting information stored on the hard disk was lost. The court found there had been physical damage to the hard disk as there was physical alteration made to the computers as a result of the corrupting of the software because this caused change in the alignment of the magnetic particles on the hard disk of the computer which had the effect of rendering the system useless in a practical sense until the particles had been realigned.


\(^{47}\) [1998] VSC 244.