Cybersecurity risk and mobile payments

July 2015

Speed read

Continuing our series on mobile payments, this article discusses the enormity of cybersecurity risk, and what to do about it. Given that hackers were able to access 83 million household and small business accounts via JPMorgan Chase & Co, banks and other mobile participants are not immune from this threat.

While cybersecurity is now a fundamental issue for modern commerce in general, it is particularly important in the case of platforms like mobile payments.

And, as we noted in *Harvard Business Review: Cyber security is a bigger GC, board, CEO, and CFO issue*, these types of risks are routinely underestimated, or inadequately dealt with, by New Zealand companies.

In this article we refer to international payment best practice standards, including the Payment Card Industry's Data Security Standard (PCI DSS), a central feature of mobile payments.

Dealing with cybersecurity calls for a multi-disciplinary approach, and that involves the legal elements, which must be integrated with the broader solutions. There's a valuable methodology developed by the General Counsel in the UK's top companies, readily applicable here. They focus on building a "defensive shield" both to help prevent problems developing and also to be ready to deal with a cybersecurity breach. The approach includes:

- Understand the cybersecurity legal framework, both domestically and internationally.
- Ask a series of critical questions, internally and with external suppliers.
- Build a "defensive shield" against regulatory action and litigation.
- Apply best practice cyber security standards.

The Detail

The story so far

This follows our earlier articles:

- *How does Apple make money from Apple Pay?*
- *Introduction to NZ mobile payments regulation and law*

And this article will be followed by:

- *Mobile payments and the slippery slope of privacy loss...*
- *Retailers pay banks more over payWave/PayPass than over EFTPOS*
- *Mobile payments and competition law*

Why is cybersecurity important?

The increasing frequency of major hacks, which now include Sony, Target, and, infamously, the infidelity website Ashley Madison, illustrates the digital vulnerability of many companies, whether large or small.

Closer to home for the payments world is the 2014 hacking of JPMorgan Chase & Co when intruders got the names, addresses, phone numbers and email addresses of the holders of some 83 million households and small business accounts, making it one of the biggest data breaches in history. As Reuters reported, quoting a cybersecurity expert:[1]

> *"Tal Klein, vice president with the cybersecurity firm Adallom, said that the breach could undermine confidence in the security of banks and other companies that people assume are well protected from hackers.....*
>
> *"Until now the assumption has been that the companies that get breached are the ones that have poor security practices, but we know that JPMorgan had a good security program and that they invest heavily in this area," he said. "So what we are waking up to is that the fundamental nature of security is broken."*

Mobile payments, along with integration into other databases such as loyalty programmes, increase cybersecurity risk (but mobile payments might also be used to minimise the risk too, with the security features that can be used). The critical nature of the data transmitted in each mobile payment, and the fact that many consumers already have security concerns about the technology, mean omitting to implement a robust cybersecurity strategy is bet-the-bank stuff.

Key reasons to focus on a robust cybersecurity strategy include:

- Secure systems develop customer trust and improved brand reputation
- Improved efficiency of IT systems (and reduced operational costs)
- Better prepared to comply with other regulation
- A breach could result in data loss, reputational loss, fines, lawsuits, etc

In *Top 100 General Counsel position on cyber security law and practice* we reviewed the cybersecurity recommendations by the association of General Counsel from the UK's largest 100 companies, which included:

- Understand the cybersecurity legal framework, both domestically and internationally.
- Ask a series of critical questions, internally and with external suppliers.
- Build a "defensive shield" against regulatory action and litigation.
- Apply best practice cyber security standards.

Cybersecurity is multi-disciplinary and that summarises the role of the law and lawyers in that area. The concept of building a "defensive shield" is the biggest takeaway from that report.

The rest of this article deals with that last point as to cyber security standards.

PCI DSS

The Payment Card Industry's Data Security Standard (PCI DSS) is an internationally accepted set of policies regarding credit and debit card data security. First created in 2004 by Visa, Mastercard, American Express, and Discover to combat credit card fraud, it is now a widely recognised benchmark of payment security.

Most if not all NZ banks and payment providers, such as Paymark, require merchants to comply with PCI DSS when accepting payments, including mobile payments.

Full compliance with PCI DSS involves, among other steps, creating and regularly changing strong passwords, training employees as to cybersecurity procedures, implementing up-to-date firewalls and anti-viral protection, only using certified payment terminals and third party online payment software, and regularly monitoring security systems.

On 1 January 2015, PCI DSS v 3.0 came into effect, followed by a minor update – version 3.1 – in April 2015.[2]

In addition to specific technical updates (such as the elimination of SSL), the new standards exhibit three major themes: (1) establishing a culture of security; (2) making PCI compliance business as usual; and (3) greater guidance as to the shared responsibilities between merchants and service providers.

Merchants should not underestimate the extent of their responsibilities under the PCI DSS. Compliance is not only important as to a merchant's obligations and agreements with their bank and payment providers, but also to protect against potentially catastrophic data and reputational loss. The PCI DSS requires an active and engaged security strategy to ensure that the recommended technology, procedures and system monitoring is implemented and updated with the necessary frequency to effectively combat risk.

Cybersecurity involves ongoing vigilance; it's not a one-off event.

Validation of full compliance with the PCI DSS must be conducted annually by independent Qualified Security Assessors (QSAs).[3] However, smaller organisations (less than 1 million e-commerce transactions per annum) are eligible to validate their own compliance through a combination of annual self-assessment reporting and quarterly network vulnerability scans undertaken by an external scanner.

Specific PCI standards: mobile payments

PCI has released a swathe of highly specific standards, including the PA-DSS for software developers, and PCI Mobile Payment Acceptance Security Guidelines for both merchants and developers. These guidelines provide more detailed guidance as to preventing mobile device data from being compromised, and were updated to version 1.1 in July 2014.

For merchants, the guidelines offer valuable advice as to mobile payment best practices, including how to properly safeguard mobile payment terminals, and as well as practical checklists, such as never storing customer account data on a server which is connected to the internet.

Domestic self-regulation: Payments NZ

A further solution to combat the threat of cybersecurity is through domestically-relevant, industry-wide self-regulation. One such example is the recent formation of the UK Financial Data and Technology Association (FDATA), a trade body developing a new UK code of practice for financial data security.[4]

Payments NZ's recently released *Mobile Device Rules and Standards*, which we first referred to here, also contain guidelines and industry-wide standards to uphold the security of NZ's domestic payment system.

Recommendations to further maximise cybersecurity standards

The following recommendations are specifically aimed at achieving PCI DSS compliance, but are also applicable to the implementation of any best practice cybersecurity standard. This is in addition to the necessary legal focus, outlined above:

- **Review and apply security standards in their entirety.**
- **Standards are a benchmark only, and can be exceeded.**
- **Maintain diligence.** PCI's annual compliance report indicates that 80% of companies have failed a PCI DSS interim assessment, which means they failed to sustain the security controls they initially put in place.
- **Don't assume the company can outsource security obligations.** NZ merchants using 'Direct Post' payment technology, for example, were previously able to outsource responsibilities, but are now directly responsible for payment security under the latest PCI standards.
- **Be aware of variations and updates within standards.** For example, some aspects of the new PCI DSS v 3.0 permitted an interim grace period from 1 January 2015 until 30 June 2015, at which point they became a mandatory requirement to combat increasingly sophisticated cyber threats.
- **Utilise supporting material.** PCI releases supplementary guidelines as to (a) undertaking a prioritised approach towards initial compliance; (b) maintaining ongoing compliance; and (c) specific advice for small to medium sized businesses.

Other articles

We've also outlined cybersecurity risk issues in other articles including:

- *What Foot and Mouth can teach us about cyber security.* This article helpfully illustrates that complying with best practice industry standards will generally reduce the legal risk.
- *The Internet of Things - ramping up privacy and security considerations.* In this article we review a US Federal Trade Commission report regarding security concerns towards the Internet of Things. The Internet of Things is at the heart of mobile payments too.

1. Reuters "JPMorgan hack exposed data of 83 million, among biggest breaches in history" (2 October 2014) (http://www.reuters.com/article/2014/10/03/us-jpmorgan-cybersecurity-idUSKCN0HR23T20141003)

2. See PCI Documents Library for access to all PCI Standards: https://www.pcisecuritystandards.org/security_standards/documents.php

3. Approved QSAs in NZ can be identified here: https://www.pcisecuritystandards.org/approved_companies_providers/qualified_security_assessors.php

4. FDATA (http://fdata.org.uk/)

Wigley+Company
PO Box 10842
Level6/23 Waring Taylor Street, Wellington
T +64(4) 472 3023 E info@wigleylaw.com
and in Auckland
T +64(9) 307 5957
www.wigleylaw.com