# AUSTRALIA'S CREDIT CARD SECURITY PROBLEM

*Australia has a credit card security problem – Customer credit card data is not being kept safe and it could bite business hard in the form of reputational damage and fines if it's not addressed soon*

IP Payments

*making cash flow*

In the first study of its kind in Australia, part one of the 'State of Business Banking' report has found that over-three quarters of senior financial decision-makers admit to not knowing about the essential standards for keeping credit card data safe – namely PCI compliance. Not only this, but nearly one in 25 businesses in Australia admitted to suffering a breach themselves. If you haven't come across PCI compliance before, you may wish to read on.

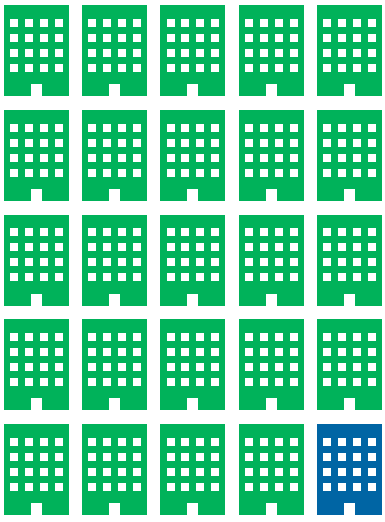
TO HELP COMBAT credit card fraud, customers need to be confident in the handling of their confidential credit card data, and that the companies that hold this information are compliant. This white paper looks at why compliance is important and provides some simple steps that can be taken towards becoming compliant effectively.

PCI compliance[1] applies to every organisation worldwide that transacts with customer credit card information. The Payment Card Industry Data Security Standard (PCI DSS), "PCI", is an information security standard for all organisations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards.

Validation of compliance is performed annually by an external Qualified Security Assessor (QSA) for organisations handling large volumes of transactions, or by Self-Assessment Questionnaire (SAQ) for companies handling smaller volumes. The standard, defined by the Payment Card Industry Security Standards Council (PCI SSC)[2], was created to increase controls around cardholder data and to reduce credit card fraud.

## WHY IS PCI IMPORTANT?

As criminals become more sophisticated in their approach, there have been a number of very high profile breaches of customer credit card data over the last 12 months, both globally and also in Australia. As a result, organisations are finding it more challenging to keep their data secure so that they don't become victim to high profile and often very negative public exposure.



**1 IN 25**

BUSINESSES ADMITTED TO SUFFERING A **BREACH**

In 2011, Sony was the victim of multiple breaches of confidential customer data worldwide. Hackers were able to access the payment details of over 100 million customers who had registered on the PlayStation®3 network and various Sony websites.

Hackers used a common method of attack, SQL

injection. Had Sony undergone a PCI audit and remediation program, hackers would have been unsuccessful in their attempts with that particular technique.

The impact to Sony[3] was significant. First there was a drop in share price, then there was the reputational damage to consider, and finally the physical cost, which some analysts in the US have predicted at around US$1.5 billion. Not only is there a cost to Sony, but the credit card lenders have suffered too, which some analysts predicted at around US$300 million.

In late 2011, IP Payments[4], an innovator in corporate payments and PCI compliance solutions sought to understand just how well Australian businesses understood these essential regulations.

## THE STORY IN AUSTRALIA

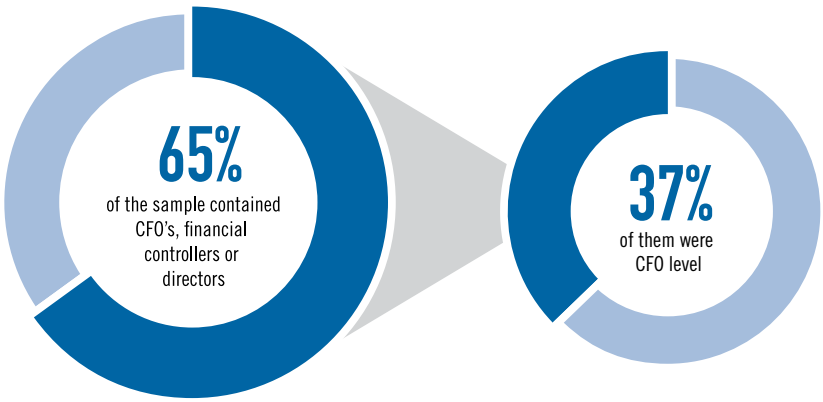
While there have been very few 'official' recorded instances of businesses suffering from a breach of customer financial data, our survey of Australia's most senior financial executives in large businesses suggests otherwise.

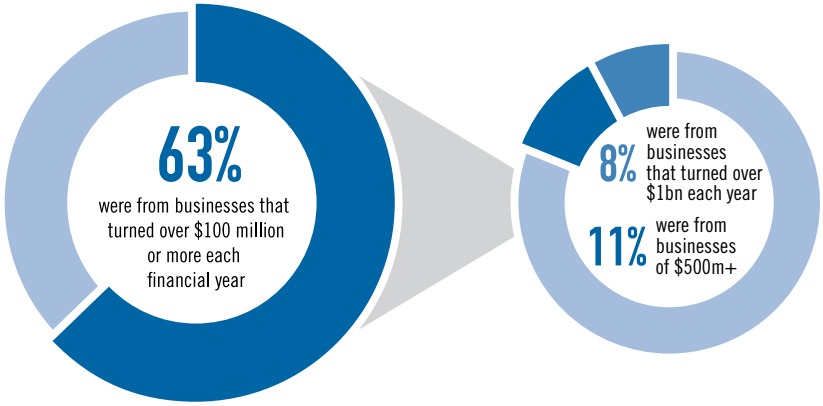
The survey, conducted by AMR, questioned 150 respondents across large organisations in Australia. To qualify for the survey, respondents had to be responsible for their overall business banking relationship and work in a business that turned over $30 million or more each financial year.

Our research uncovered that 1 in 25 businesses admitted to suffering a breach, and when asked if they knew of any business that had suffered a breach, nearly 1 in 8 (13 per cent) said that they did. Although there have been few recorded instances of breaches in Australia, that does not mean to say that they have not happened. Many of these breaches do not hit the headlines of media, so the public typically never find out about them.

> "Many of these breaches do not hit the headlines of media, so the public typically never find out about them"

Naturally, it is very hard to get organisations to admit to this exposure, particularly when there is so much at stake in terms of financial penalties and reputational damage. Indeed, respondents to the PwC Global Economic Crime Survey 2011[5] survey ranked reputational damage as their biggest fear from cybercrime. The temptation to 'shut down the doors' in this instance is very strong. It can hit the business hard, and the thing that hurts the most is just how unquantifiable brand damage really is – the longer term effects can be felt for years as trust and confidence can take years to rebuild.




Although it can be a bitter pill for businesses to swallow, admitting to the breach as early as possible will benefit the organisation in the long run as historical breaches have shown. Following on from this, showing how the matter was dealt with is going to leave companies far better off than if it is left to chance with non-disclosure.



IP Payments
making cash flow

## CONFUSION AND CONTRADICTION

The problem in Australian organisations runs deeper than suffering from a breach.

It appears that the majority of Australian businesses are in darkness as to what PCI regulations actually entail. The standard should have been adopted by all organisations with payment card data by 1 January 2011. However, the survey identified that over three-quarters (77 per cent) had not heard of PCI compliance, clearly showing that it's unlikely that Australian organisations are actually aware of the deadline.

The confusion reported in the survey reigns even deeper. While only 23 per cent of respondents said that they had heard of PCI compliance, 42 per cent said that they knew their business was PCI compliant, and 44 per cent said that they knew what the regulations entailed. The results suggest a clear confusion – how can a higher proportion of people in the survey know that they are compliant and understand the regulations if they haven't actually heard of the regulations before?

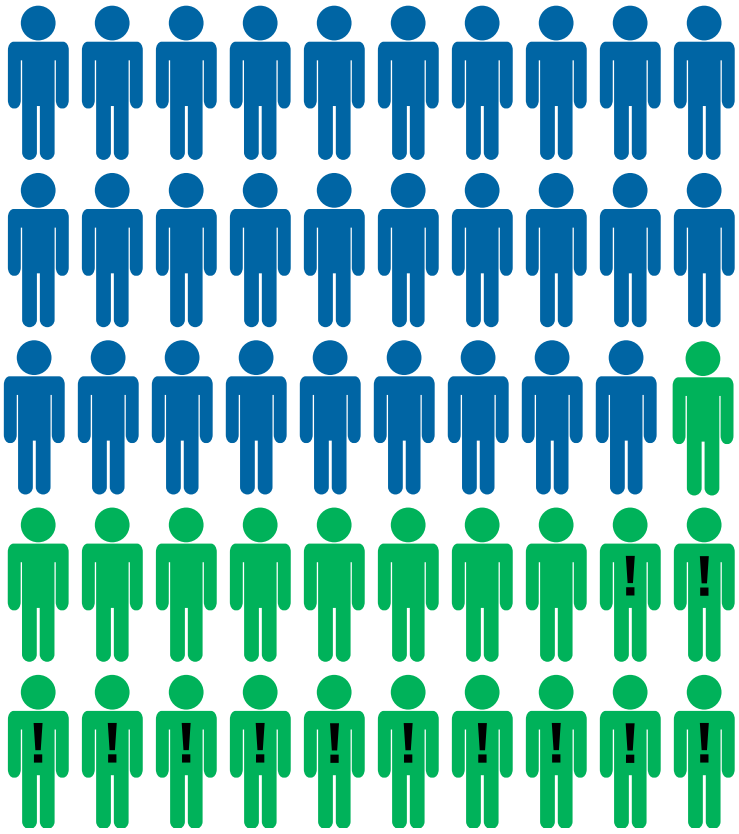
73 per cent also said that their customer data was as secure as it could be, despite 77 per cent having not heard of PCI compliance – the recognised standard for ensuring customer data is safe.

While companies might think that their data is secure, we would advise those in charge of their data security to take a close look at their current set-up and seek advice and understanding around the regulations. The results above show that there is a clear confusion, and one of IP Payments' goals is to help companies understand the requirements better so that they can ensure their own compliance.

## WHY SHOULD I BE COMPLIANT?

While compliance is mandatory for all organisations that accept credit card payments to be compliant with the PCI standards, the business benefits of achieving PCI compliance should be very obvious too:

- **Customer confidence:** compliance with the PCI DSS means that company systems are secured to a known standard, and customers can trust you with their confidential payment card information. The wider benefits of this means that your customers have confidence in doing business with you, are more likely to be repeat customers, and hopefully recommend you to others. This has been



ALTHOUGH

**42%**

OF BUSINESSES STATED THAT THEY WERE PCI COMPLIANT,

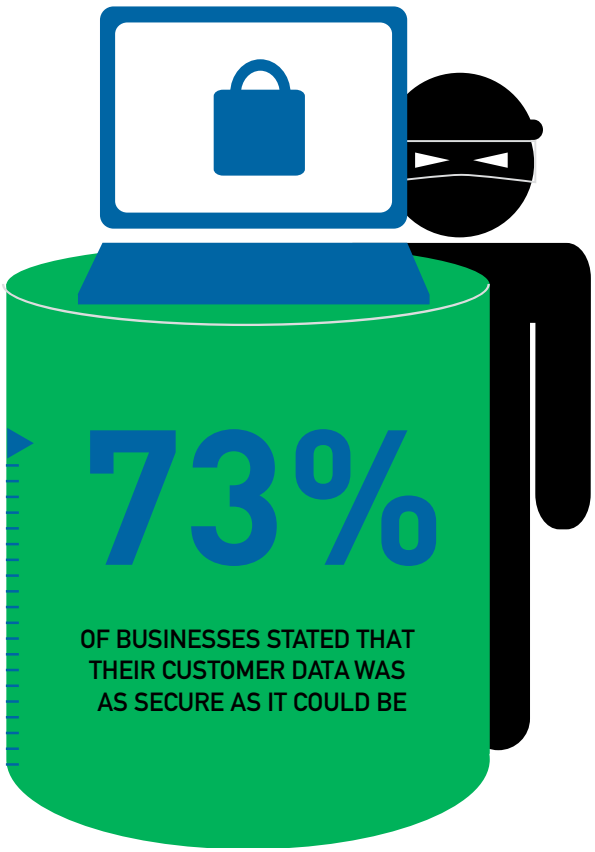
**ONLY 23%**

HAD ACTUALLY HEARD OF IT!

*How can a higher proportion of people in the survey know that they are compliant and understand the regulations if they haven't actually heard of the regulations before?*

proven in numerous surveys over the last few years, but according to the Unisys Security Index™ [6] in late 2011, at least 8 in 10 people in Australia, Hong Kong, and New Zealand would stop dealing with an organisation, such as close their account, if they found out that the privacy of their personal information had been compromised. Of the 12 countries surveyed in the global research study, Australians are the most likely to say they would take such action.

- **Security breaches will become increasingly sophisticated:** compliance is an ongoing process, not a one-time event and some simple steps can help to eliminate the vast majority of breaches that occur. Compliance helps prevent security breaches and theft of payment card data, not just today but in the future. In the past data theft was the result of the loss of physical objects, but as more data is stored in digital files hackers have become increasingly sophisticated in how they gain access to those files. Forensic investigators from security company, Verizon have found many instances where attackers have maintained access to a victim's infrastructure for months, and have slowly leeched credit cards and data out, sometimes by installing malware. The important thing to note though is that with some simple and effective security practices, most threats are avoidable. The recent Verizon 'Data Breach report'[7] survey highlighted that 96 per cent of threats are preventable.




## HOW DO I BECOME PCI COMPLIANT?

The standard[8] includes 12 requirements[9] for any business that stores, processes or transmits payment cardholder data. These requirements specify the framework for a secure payments environment.

IP Payments has over eight years' experience in the PCI compliance market and was one of the first PCI compliance solution providers to receive the PCI DSS level 1 certification. IP Payments has undergone some of the most thorough safeguards in the industry to ensure it exceeds the standard.

> "Compliance helps prevent security breaches and theft of payment card data, not just today but in the future"

IP Payments counts some of the biggest companies in Australia as its customers, befitting its status as the vendor with the most PCI compliance experience in the market. Based on these experiences, IP Payments recommends three steps towards PCI compliance: Assess, Remediate and Report.

### Step 1 – Assess

The purpose of assessing is to identify all technology and process vulnerabilities that pose risks to the security of cardholder data that is transmitted, processed or stored by your business.

First of all, look at how cardholder data flows from the beginning to the end of the transaction processes. Do not forget to include PCs and laptops with access to critical systems, storage mechanisms for paper receipts and so on.

Additionally, your liability for PCI compliance extends to third parties involved with your process flow, so you must also confirm that your partners are compliant too. Comprehensive

assessment is a vital part of understanding what elements may be vulnerable to security exploits and where to direct remediation.

There are tools to assist organisations validate their PCI DSS compliance. The free Self-Assessment Questionnaires (SAQ)[10] include a series of yes-or-no questions about your security posture and practices, and is a validation tool for merchants and service providers who are not required to do on-site assessments for PCI DSS compliance.

The PCI SSC also provides programs for two kinds of independent experts to help with your PCI assessment: Qualified Security Assessor (QSA) and Approved Scanning Vendor (ASV):

- QSAs have trained personnel and processes to assess and prove PCI DSS compliance
- ASVs provide commercial software tools to perform vulnerability scans for your systems

### Step 2 – Remediate

Remediation is the process of fixing vulnerabilities that may exists after you have conducted the initial assessment. These could include technical flaws in software code or unsafe practices in how your organisation processes or stores cardholder data. There is a five-step process that you can follow to help identify and remediate any vulnerabilities:

1. Scan your network with software tools that analyse infrastructure and spot known vulnerabilities;
2. Review vulnerabilities found in on-site assessment (if applicable) or through the Self-Assessment Questionnaire process;
3. Risk assess and rank the vulnerabilities to help prioritise the order of remediation;
4. Apply patches, fixes, workarounds, and changes to unsafe processes and workflow; and
5. Re-scan to verify that remediation actually occurred.

### Step 3 – Report

PCI compliance is an ongoing process that requires updating and monitoring, as such regular reports are required, however the PCI SSC is not responsible for PCI compliance. Reports are submitted to the acquiring bank and global payment brands that you do business with.

To begin with, all merchants and processors must perform a quarterly scan report, which must be completed by a PCI SSC Approved Scanning Vendor (ASV). An ASV is an organisation that validates adherence to certain PCI SSC requirements by performing vulnerability scans of Internet facing environments of merchants and service providers. PCI SSC has approved more than 130 ASVs.

"While there appears to be confusion as to whether an organisation is actually compliant and what the regulations actually entail, the good news is that you're not alone"

Businesses with large transaction flows must do an annual on-site assessment completed by a PCI SSC-approved QSA and submit the findings to each acquirer. Businesses with small transaction flows are required to submit an annual attestation within the Self-Assessment Questionnaire.

## WHAT SHOULD I DO NEXT?

For IP Payments, the survey results paint a very real insight into our experiences over the last eight years when dealing with PCI compliance in Australia. We understand that there is confusion and that clarity is required. We have worked with many companies to help them understand the myriad of regulations that PCI entails, as we appreciate that it can at times appear bewildering as to what each company should adhere to.

While there appears to be confusion as to whether an organisation is actually compliant and what the regulations actually entail, the good news is that you're not alone and there are companies, such as IP Payments that can assist in this matter. Reading this paper and following the above three steps is an extremely good start towards setting yourself on the path to PCI compliance.

*About the author: Mark Lewis is a director at IP Payments.*

[1] https://www.PCIsecuritystandards.org

[2] https://www.PCIsecuritystandards.org/merchants/index.php

[3] http://www.reuters.com/article/2011/04/29/us-sony-creditcards-cost-idUSTRE73S0FL20110429

[4] www.ippayments.com

[5] http://www.pwc.com/gx/en/economic-crime-survey/download-economic-crime-people-culture-controls.jhtml

[6] http://www.unisyssecurityindex.com

[7] http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012-press_en_xg.pdf

[8] https://www.PCIsecuritystandards.org/security_standards/index.php

[9] https://www.PCIsecuritystandards.org/merchants/index.php

[10] https://www.PCIsecuritystandards.org/security_standards/documents.php?category=saqs

**Mark Lewis is Technical Director at IP Payments.**

IP Payments has emerged as a leader in secure revenue management solutions and has helped clients improve cash flow and comply with secure payment standards since 2004. We provide organisations with the corporate payments technology that sits at the heart of their business and ensure their compliance with PCI data security standards. We are a partner of 3,500 enterprises around the globe, including various ASX 50 and Fortune 500 organisations in the Asia Pacific region. For four straight years, Deloitte has identified IP Payments as one of the 500 fastest-growing ICT companies in Asia and had our online statement, invoice and payments solution recognised as the 'Most Innovative Financial Application' in the Asia Pacific region. For more information, please visit www.ippayments.com

IP Payments
*making cash flow*