PCI Compliance:

How to ensure customer cardholder data is handled with care

Choosing a safe payment process for your business

Contents

Executive Summary

Increasing the bottom line is crucial for success in business, and continuous advances in technology mean there are constantly new options available for businesses seeking ways to increase their efficiency. As technology develops and Australians move towards digital payment technologies, personal cardholder data is susceptible to hacking, phishing and fraud.

In the finance department, payment methods such as direct debit, BPAY and eCommerce can enable businesses to take control of their cash flow. Payment technologies can reduce cash handling, allow businesses to manage payments online and provide access to reporting 24/7. These advanced payment technologies provide a platform for businesses to reduce administrative costs whilst increasing customer satisfaction and retention, but such technology also carries risks.

Consumers are aware of these risks and a recent study published by the Office of Australian Information Commissioner found that Australian's are becoming increasingly concerned with privacy risks. According to the report, 33% of Australians were concerned with the way their personal data was used. Businesses that process card payments of any kind need to be mindful of the security measures required to protect cardholder data, not only for compliance reasons but also to ensure consumer satisfaction and trust.

In an attempt to improve security measures, five major global Card payment brands, including Visa and MasterCard, founded the Payment Card Industry (PCI) Security Standards Council in 2006 and subsequently introduced the international Data Security Standard (DSS).

Businesses that use third party payment providers have the advantage of being able to outsource their data security to help meet their obligations. To remain compliant, it is important to understand the requirements of PCI DSS. Additionally, when using a payment provider, it is important to ensure the provider is PCI DSS compliant.

Failure to comply with PCI guidelines can cause damage to your business reputation, financial liability, or even cancellation of a merchant facility. Yet compliance breaches continue to occur. A study conducted by the Verizon RISK Team reported 855 incidents and 174 million compromised records suggesting a need for businesses to be better educated in preventing breaches and improving compliance.

This paper has been developed by Ezidebit, Australia's first non-bank PCI DSS Level 1 company, to provide a useful resource for businesses and to outline the security obligations for businesses handling cardholder data.

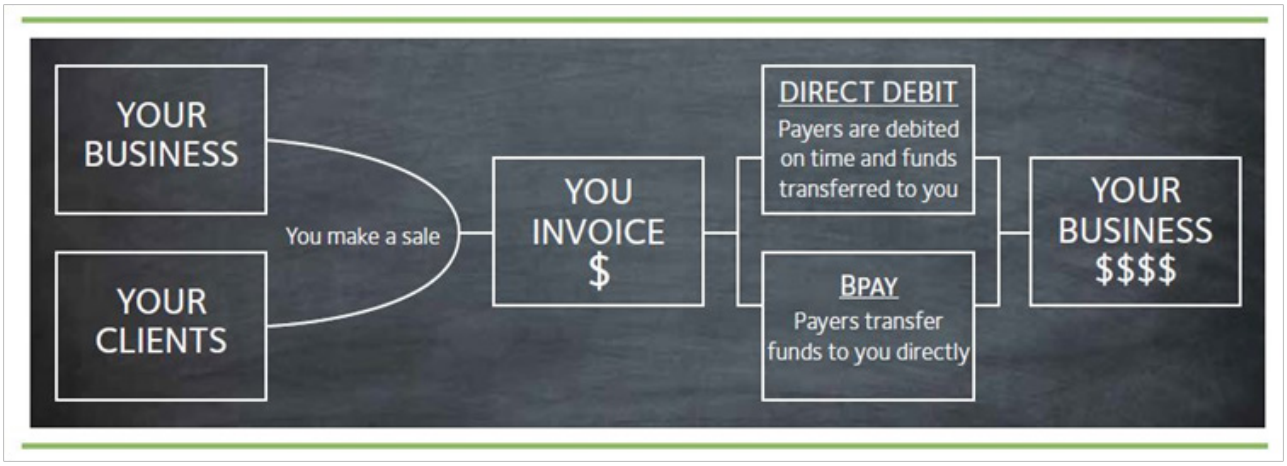
PCI compliance and accreditation

The PCI DSS Security Standards Council was established in 2006 and manages the PCI security standards, including the PCI DSS. The PCI DSS was founded by five global Card payment brands (American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc.) to establish a framework for secure payment card processing and data handling. These brands, together with the Council's Strategic Members, contribute to the ongoing work of the organisation. Penalties (fines) for non-compliance of the PCI DSS are enforced by the individual payment brands and not by the council.

Who PCI compliance applies to

PCI compliance applies to all businesses that accept, transmit, or store cardholder data. If your business enrols a third-party processor you still also need to be PCI compliant, however you can outsource many of your compliance costs and risks to the third party.

The data handling process



Not being PCI compliant is risky

ATM tampering, spyware, key logger malware, stolen credentials, and hacking are some of the many ways that breaches in the financial services industries can occur. Attackers are often financially motivated and the list of merchants who have had a credit card data security breach continues to grow.

In Australia, payments fraud data released by the Australian Payments Clearing Association revealed 1,373,025 fraud transactions on Australian-issued cards for the 2013 financial year.

Ultimately, businesses that breach compliance expose their business to damaging (and potentially irreversible) consequences.

The consequences of a breach or non-compliance:

Monetary costs	Fines such as payment card issuer and government fines for non-compliance can range from $5,000 to $500,000. Additional economic costs can be widespead and include potential increases in transaction fees with sponsor banks, lawsuits, insurance claims, and cancelled accounts.
Time costs	A compliance breach can result in increased audit requirements and cost of staff time during security recovery. Written notification must be supplied to all individuals whose information may have been compromised when a data breach occurs.
Brand costs	A breach in cardholder data can occur even where a company is 100% PCI compliant and can result in loss of reputation and loss of customer, supplier and partner trust and loyalty.

> “ In the US, 80% of small businesses who experience a data breach go bankrupt or experience severe financial difficulties within two years. ”
>
> *US Privacy Rights Clearing House*

A costly example

US retailer Target demonstrates the costliness of non-compliance

A data breach can potentially effect tens of thousands of records and the 2013 US Target data breach is a frightening example of the immense costs that can result.

Target first reported the major data breach in mid-December 2013 and statistics reflect the massive impact the breach had on its bottom line. Data from consulting group Kantar Retail reveals that Target experienced a drop of more than 46 percent in fourth-quarter profit.

In January 2014, 33% of US households reported shopping at Target or SuperTarget, a drop of 22% in penetration compared to January 2013.

Analysts estimate the costs to Target could run into the billions. More than 90 lawsuits have been filed against Target by customers and banks for negligence and compensatory damages according to 'Business Week'.

Data Breach costs in Australia

Data breach costs are also high in Australia. The Australian Competition and Consumer Commission's (ACCC) annual 'Targeting scams' report outlines the massive costs associated with data breaches and scams. In the past three years, the dollar value of scam losses reported to the ACCC has continued to rise:

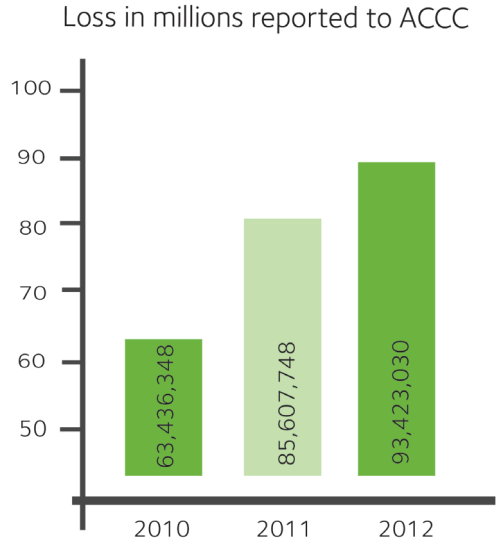
- Australians reported $93,423,030 in financial losses to the ACCC in 2012
- Australians reported $85,607,748 in financial losses to the ACCC in 2011
- Australians reported $63,436,348 in financial losses to the ACCC in 2010

What's more, the figures only reflect financial losses reported to the ACCC. Many losses go unreported or are reported to other agencies and as a result the actual figures may be far greater.

In the online world, the growing amount of purchases via mobile phones, and other changes in the payments industries due to continuous changes in technology, highlights the need for businesses to stay ahead with their security and compliance requirements.

In 2012, the Australian Competition & Consumer Commission reported a total loss of $4,038,479 due to online shopping scams.

The costs associated with being compliant may seem daunting, however the costs associated with breaching compliance are far greater.



Ongoing steps for PCI Compliance

3 ongoing steps the PCI DSS suggest for meeting security best practices:

Step 1

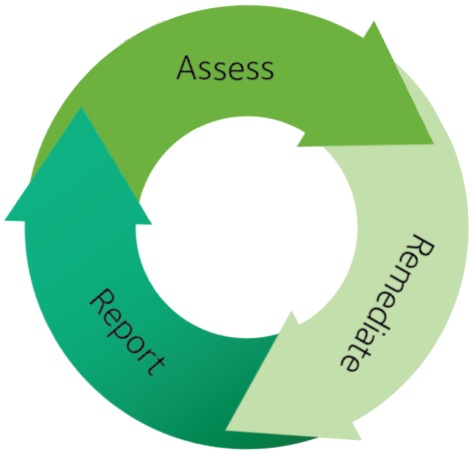
Assess:
The first step is to assess cardholder data, IT assets, and business processes for payment card processing for any security weaknesses.

Step 2

Remediate:
The second step involves addressing any weaknesses and ensuring cardholder data is not stored unless necessary.

Step 3

Report:
Following remediation, the third step involves compiling reports to record remediation. Compliance reports are then submitted to the business' sponsor bank and participating cardholders.



Each card brand has its own compliance program. Information for Visa, MasterCard and AMEX is available online at the following sites:

American Express: www.americanexpress.com/datasecurity
MasterCard: http://www.mastercard.com/sdp
Visa Inc: http://www.visa.com/cisp

Choosing a safe payment process for your business

When choosing a safe payment process for your business it is important to choose a compliant service provider. Service providers are organisations that process, store, or transmit cardholder data on behalf of another entity. Businesses seeking a service provider for payment solutions should choose one that is PCI compliant.

Qualified Security Assessors (QSAs) report PCI DSS compliant Service Providers to major credit card companies such as VISA and MasterCard. The lists of compliant Services Providers as of the date indicated are available on the MasterCard and VISA websites.

Visa and Mastercard websites:
http://www.visa.com/splisting/
http://www.mastercard.com/us/company/en/docs/SP_Post_List.pdf

12 PCI Data Security Standards Key Requirements

Overview of PCI DSS Requirements

Build and maintain a secure network 1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplier defaults for system passwords and other security parameters	**Implement strong access control measures** 3. Restrict access to cardholder data by business need-to-know 4. Assign a unique ID to each person with computer access 5. Restrict physical access to cardholder data
Protect cardholder data 6. Protect stored cardholder data 7. Encrypt transmission cardholder data across open, public networks	**Regularly monitor and test networks** 8. Track and monitor all access to network resources and cardholder data 9. Regularly test security systems and processes
Maintain vulnerability management program 10. Use and regularly update antivirus software 11. Develop and maintain secure systems and applications	**Maintain an information security policy** 12. Maintain a policy that addresses information security

PCI DSS Compliance Levels

In addition to the 12 requirements outlined previously, there are four PCI compliance levels with individual requirements. The required PCI compliant level is determined by the accumulated Visa transaction volume of credit, debit and prepaid transactions over a 12-month period from a merchant (payment provider) Doing Business As (DBA).

The four PCI DSS compliance levels as defined by Visa are:

Level 1	Any business processing more than 6 million Visa transactions annually or any other business that Visa deems should meet the Level 1 requirements
Level 2	Any business processing 1,000,000 to 6,000,000 Visa transactions annually
Level 3	Businesses processing 20,000 to 1,000,000 Visa e-commerce transactions per year
Level 4	Any business processing less than 20,000 Visa e-commerce transactions per year, and all other businesses processing up to 1,000,000 Visa transactions per year

How Compliance is Achieved

The complete definitions of the individual compliance levels and requirements as determined by Visa are available online.

Businesses that are not required to have a Qualified Security Assessor assess their business procedures onsite can complete a PCI DSS Self-Assessment Questionnaire (SAQ) which they may be required to share with their sponsor bank.

Download the PCI DSS SAQ at: https://www.pcisecuritystandards.org/merchants/self_assessment_form.php.

Each version of the PCI DSS SAQ caters for a different business scenario. Businesses can consult their sponsor bank for further details regarding their particular PCI DSS requirements.

Level 1	✓ Annual onsite assessment by a Qualified Security Assessor (QSA) or an Internal Audit if signed by Officer of the company. ✓ A quarterly network scan completed by an Approved Scanning Vendor (ASV).
Level 2	✓ Annual completion of PCI DSS Self-Assessment Questionnaire (SAQ). ✓ A quarterly network scan completed by an ASV.
Level 3	✓ Annual completion of PCI DSS Self-Assessment Questionnaire (SAQ). ✓ A quarterly network scan completed by an ASV.
Level 4	✓ Annual completion of PCI DSS Self-Assessment Questionnaire (SAQ). ✓ A quarterly network scan completed by an ASV.

Costs of Becoming Compliant

The fees associated with being PCI DSS Compliant will vary from business to business. Fees depend on a number of factors such as the business' existing credit/debit card processes and the number of transactions processed annually. For example, businesses that require an on-site audit (PCI DSS Compliance Level 1) will generally pay higher fees than businesses completing the Self-Assessment Questionnaire (SAQ) and a quarterly scan (PCI Compliance Levels 2, 3 and 4).

A list of the PCI DSS Programs Fee Schedule is available on the PCI Security Standards Council's website.

https://www.pcisecuritystandards.org/

The costs of becoming PCI Level 1 compliant can be broken down into 4 main categories:

Infrastructure: A range of network, system and application design and implementation changes are required to meet the PCI DSS standard. Big ticket costs include Network Firewall to segregate card holder networks, security systems like Intrusion Detection Systems, File Integrity Monitoring, Variability Scanners and Centralised Logging and Web Application Firewall. These systems have the potential of running into the hundreds of thousands of dollars just to purchase before implementation.	**Compliance:** To obtain compliance, an organisation is required to engage the professional services of a QSA (Qualified Security Assessor) to conduct the audit, generally costing tens of thousands of dollars annually. The QSA will conduct an onsite audit and follow a process of gathering evidence of your card holder environments and processes against the PCI DSS Standard. A qualified penetration tester is also required to conduct internal and external penetration tests every year as a minimum.
Process: PCI DSS requires a mature and comprehensive set of company policies and procedures. The ability to prove the policies are both comprehensive and enforced.	**People:** The hours involved can vary depending on the size of the organisation. The life cycle of full compliance certification can take from 6 months to 3 years of effort. Majority of the hours are spent on technical design and implementations, and on processing documentation and development.

Ezidebit, Australia's 1st PCI DSS Level 1 compliant direct debit company

Ezidebit was the first non-bank payment service provider in Australia and New Zealand to hold PCI DSS Level 1 compliance. This level of compliance is PCI's most comprehensive security standard and represents a gold standard in information security. Once achieved, maintaining level 1 compliance requires rigorous external audits, ongoing quarterly network penetration testing and regular site inspections by a qualified security assessor.

Every year on the anniversary of the Level 1 payment service provider's compliance, a ROC (Record of Compliance) is forwarded for assessment by the Qualified Security Assessor. Ezidebit is committed to security and compliance to ensure bank account and credit card information is protected 24/7.

Ezidebit is a trusted payment technology company that has formed strong partnerships and integrations with over 20,000 Australian and New Zealand businesses.

Ezidebit's Compliance and Accreditation

- ✓ Level 1 PCI Compliance
- ✓ Australian Financial Services Licence
- ✓ Commercial Agent Licence
- ✓ Associate Member of APCA
- ✓ Card Scheme Approved Merchant Aggregator

Further information about Ezidebit is available by visiting www.ezidebit.com.au or telephoning 1300 763 256.

About the Ezidebit Compliance Officer

Tony Crudgington has an all-encompassing background in Financial Services, spanning 30 years. In appointments with various corporate Financial Institutions he was responsible for managing and developing (both strategic and technical) electronic payment systems, management of a number of Sales and Operational Units that developed and supported the provision of all cheque and electronic and foreign currency payment related systems. Appointed to various regulatory bodies, Tony has been part of major reform in the Australian payments industry.

If you have any questions about PCI Compliance you can contact Tony at tony.crudgington@ezidebit.com.au.