



## A guide to implement the Payment Card Industry Data Security Standard (PCI DSS)

Visa and MasterCard have developed the Payment Card Industry Data Security Standard (PCI DSS) to manage the risk of external and internal data compromises. This is a set of industry-wide requirements and processes supported by every major international payment card system.

The PCI DSS has 6 major milestones that focus on using secure systems and protecting cardholder data.

These include removing sensitive data, protecting networks, securing payment card applications, monitoring and controlling access to systems, protecting stored cardholder data and finalising processes to support maintenance of PCI DSS.

If you accept Visa, MasterCard or any charge card payments, you must comply with the PCI DSS requirements.

	DATA ELEMENT	STORAGE PERMITTED	PROTECTION REQUIRED	PCI DSS REQUIRED
<b>CARDHOLDER DATA</b>	Primary Account Number	YES	YES	YES
	Cardholder Name*	YES	YES*	NO
	Service Code*	YES	YES*	NO
<b>SENSITIVE AUTHENTICATION DATA</b>	Expiration Date	YES	YES*	NO
	Full Magnetic Stripe	NO	N/A	N/A
	CVC2/CVV2/CID	NO	N/A	N/A
	PIN/PIN Block	NO	N/A	N/A

\*These data elements must be protected if stored in conjunction with the PAN.

### The Benefits for Your Business

By following the industry-wide requirements of PCI DSS, organisations can:

- Protect their customers' personal data
- Boost customer confidence through a higher level of data security
- Lower their exposure to financial losses and remediation costs
- Maintain customer trust and safeguard the reputation of their brand
- Provide a complete "health check" for any business that stores or transmits customer information

## Don't Put Your Customers or Your Business at Risk

Protecting your customers' account information from the growing threat posed by high-tech criminals is one of the biggest challenges facing businesses today. As the technology used by merchants and their partners has evolved, card fraud has become more sophisticated. Any business that processes, stores or transmits cardholder account data is a potential target.

***If you don't need it, don't store it.***

There have been many instances around the world of hackers accessing computer systems, stealing cardholder data and using this data to commit fraud.

It is important for merchants and businesses alike to understand what measures need to be taken every day to ensure the security of highly sensitive personal financial information.

## When Things Go Wrong

The credit card accounts of 120,000 Australians were exposed to fraud following a major security breach at a large US processor in 2005. The breach was detected by card fraud detection systems.

A reputable shoe retailer was forced to notify its customers after thieves accessed their database last year and stole information on 1.4 million credit cards and the names of those accounts.

In another incident, a problem with the point-of-sale software at a US designer brand name clothing store compromised the credit card data of as many as 180,000 of their customers.

A US data broker reported A\$15 million in losses following the exposure of 145,000 customer accounts. Factoring in the costs of system and process modifications, research firm Gartner estimated the cost at about A\$118 per exposed account.

By minimising the risk of data compromise, implementation of PCI DSS assists businesses to protect against potential financial liabilities, investigative costs and the risk of invasive media attention.

## The Milestone Approach

The benefits of producing a road map, or 'prioritized approach' allows merchants or organisations to prioritize the risks associated with failing to comply with the PCI DSS.

PCI DSS MILESTONE APPROACH	
<b>MILESTONE ONE</b> <b>Remove sensitive authentication data and limit data retention</b>	Without sensitive data and other cardholder data storage, the effects and the costs of a compromise are greatly reduced.  <b>If you don't need it, don't store it</b>
<b>MILESTONE TWO</b> <b>Protect the perimeter, internal, and wireless networks</b>	Targets a key area that represents the point of access for most compromises: vulnerabilities in networks or at wireless access points.
<b>MILESTONE THREE</b> <b>Secure payment card applications</b>	Targets controls for applications, application processes and application servers. Vulnerabilities are a key access point used to compromise systems and obtain access to cardholder data.
<b>MILESTONE FOUR</b> <b>Monitor and control access to your systems</b>	Controls detect the who, what, when and how about who is accessing your network
<b>MILESTONE FIVE</b> <b>Protect stored cardholder data</b>	Targets deployment of controls for protecting stored cardholder data. Applies only to organizations that have analysed their business processes and determined it is essential to store Primary Account Numbers.
<b>MILESTONE SIX</b> <b>Finalize all the policies, procedures, and processes to support maintenance of PCI DSS Compliance</b>	Focus on confirming that all PCI DSS controls put in place throughout Milestone One through Six are codified and are repeatable activities that promote and support maintenance of ongoing PCI DSS compliance.

## PCI DSS and Your Business

The way PCI DSS relates to your business, and the way in which it should be implemented, will depend on:

- The size and nature of your business
- The configuration of your card acceptance systems and processes
- The service providers you work with and their respective roles

High risk merchant considerations:

- **Batch Processor Merchant** – do I save the card number, expiry date and CVV2 together?
- **Merchant Hosted** – Does my site capture cardholder data before sending through to the payment gateway?
- **Third Party Processors** – Does my business rely on a third party web host to send through card details to my system? Are these third party processors PCI DSS compliant?
- **Merchants with a Web Presence** – Does my business take card details via a website/online presence, and then process them through other means (ie. EFTPOS terminal?) Where are these card details stored?

## How Do I Get Started?

MasterCard and Visa have created a set of tools and resources to make it as straightforward as possible for you to implement the PCI DSS.

Visa's program is called **Account Information Security (AIS)**  
– for details on the program go to [www.visa-asia.com/secured](http://www.visa-asia.com/secured)

MasterCard's program is called **Site Data Protection (SDP)**  
– for details on the program go to [www.mastercard.com/us/sdp/index.html](http://www.mastercard.com/us/sdp/index.html)

Alternatively, the PCI Standards Council also has created a site that provides a comprehensive look and action into the PCI standards. For further details go to <https://www.pcisecuritystandards.org/>

## Frequently Asked Questions

### How do I know if I meet the PCI DSS Requirements?

To check whether your organisation meets the PCI DSS requirements, you complete the following validation tasks (depending on the average monthly volumes you process):

- Self-Assessment Questionnaire
- Vulnerability scan
- Onsite Review

### Do I have to complete all the validation tasks?

MasterCard and Visa have defined four merchant levels to determine requirements. These are:

	Merchant Categories	Validation Tasks
<b>Level 1</b>	- Any Merchant having greater than 6,000,000 total combined transactions annually. - Any Merchant that has suffered a hack or an attack that resulted in a Card data compromise.	- An annual onsite assessment conducted Qualified Security Assessor (QSA) (Must be completed before Dec '10) - Quarterly network scans – conducted by an Approved Scanning Vendor (ASV)
<b>Level 2</b>	- Any Merchant with greater than 1,000,000 but less than or equal to 6,000,000 transactions annually.	- An annual self-assessment - Quarterly network scans conducted by an ASV - Effective 31 December 2010, an annual onsite assessment by approved QSA
<b>Level 3</b>	- Any Merchant with greater than 20,000 total ecommerce Transactions annually but less than or equal to one million total ecommerce transactions annually.	- An annual self-assessment - Quarterly network scans conducted by an ASV
<b>Level 4</b>	Any merchant not deemed to be Level 1, 2 or 3 Merchant is deemed to be a	- An annual self-assessment - Quarterly network scans conducted by an ASV

Level 4 Merchant.

All Level 4 merchants Acquirers will be required by April '10 to provide VISA with a risk based compliance program for their Level 4 merchants. We will be required to report on their compliance status twice a year.

### **What is the Self-Assessment Questionnaire?**

The Self-Assessment Questionnaire is a free, confidential tool that can be used to gauge your level of compliance with PCI DSS. It is an online tool made up of a series of questions relating to your business processes.

Once it has been completed, you will have made a good assessment of your risk level. If the assessment indicates that remediation work is needed, you will need to undertake this work in order to comply with PCI DSS. You can complete the process internally or work with a Qualified Security Assessor to manage it on your behalf.

### **What is a vulnerability scan?**

A vulnerability scan ensures that your systems are protected from external threats such as unauthorised access, hacking or malicious viruses. The scanning tools test all of your network equipment, hosts and applications for known vulnerabilities.

Scans are intended to be non-intrusive, and are conducted by an authorised network security scanning vendor.

Regular quarterly scans are necessary to ensure that your systems and applications continue to afford adequate levels of protection.

### **What acknowledgement of validation to PCI DSS will be received?**

Bendigo and Adelaide Bank Ltd will inform MasterCard and Visa when your organisation has met the PCI requirements.

### **What if I choose not to be involved in the program?**

You will cover Bendigo and Adelaide Bank Ltd. against all losses, expenses and damages the Bank may suffer as a result of MasterCard & Visa imposing fees, fines or penalties as a result of your failure to observe your obligations under the PCI DSS. Should a compromise occur and your organisation has not taken the appropriate steps to ensure that account information was protected; all costs to enable a forensic analysis to investigate the compromise will be passed directly onto your organisation.

Bendigo and Adelaide Bank Ltd. remains the right to terminate your merchant facility at any time if you are found to be in breach of your agreement.

