PAYMENT CARD INDUSTRY DATA SECURITY STANDARDS

THE PAYMENT CARD INDUSTRY DATA SECURITY STANDARD 'PCI DSS'

Visa and MasterCard have developed the Payment Card Industry Data Security Standard or 'PCI DSS' as a means of managing 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 through the PCI Security Standards Council or 'PCI Council'.

The PCI DSS has 12 basic requirements that focus on using secure systems. The standards include installing a firewall, changing default passwords, protecting stored data, using antivirus software and encrypting transmissions of cardholder data across public networks.

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 system and processes.
- The service providers you work with and their respective roles.

THE PCI DSS REQUIREMENTS

By following the PCI DSS requirements you can assess if your business protects cardholder data, has a secure network, maintains a security policy, maintains strong access control measures, regularly monitors and tests networks, utilises a third party and if so, if they are also meeting the PCI DSS requirements. The 12 PCI DSS requirements are as follows:

Build and maintain a secure network

1. Install and maintain a firewall configuration to protect cardholder data.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.

Protect cardholder data

3. Protect stored cardholder data.
4. Encrypt transmission of cardholder data across open public networks.

Maintain a vulnerability management program

5. Use and regularly update anti-virus software or programs.
6. Develop and maintain secure systems and applications.

Implement strong access control measures

7. Restrict access to cardholder data by business need-to-know.
8. Assign a unique ID to each person with computer access.
9. Restrict physical access to cardholder data.

Regularly monitor and test networks

10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.

Maintain an information security policy

12. Maintain a policy that addresses information security for employees and contractors.

Further information can be obtained from **www.pcisecuritystandards.org**

THE BENEFITS TO YOUR BUSINESS

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

- Protect customer data.
- Provide a complete 'health check' for any business that stores or transmits customer information.
- Lower exposure to financial losses and remediation costs.
- Maintain customer trust and safeguard the reputation of their brand.

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

HOW DO I GET STARTED?

The PCI Help Desk (1300 736 216) will be able to provide advice on the validation process to merchants who require it. The service will be answered by Vectra Corporation.

Visa and MasterCard have created a set of tools and resources to make PCI DSS implementation simple and straightforward.

Visa's program is called the **Account Information Security Program 'AIS'** – for details visit **http://www.visa-asia.com/ap/au/merchants/riskmgmt/ais.shtml** or email **vpssais@visa.com**

MasterCard's program is called the **Site Data Protection Program 'SDP'** – for details visit **http://www.mastercard.com/us/sdp** or email **sdp@mastercard.com**

FREQUENTLY ASKED QUESTIONS

Who needs to be compliant?
All entities that store, process and/or transmit cardholder data, such as merchants, service providers (e.g. payment gateways, SPSP, processors), must comply with the PCI DSS. The requirements apply to all acceptance channels including retail (brick-and-mortar), mail and telephone order 'MOTO,' and e-commerce. The obligation to comply may also arise under your Merchant Agreement.

How do I know if I meet the PCI DSS requirements?
To check that you have met the PCI DSS requirements, you will need to complete one or more of the following validation tasks (depending on the annual volumes you process). These standards include:

- The Self-Assessment Questionnaire 'SAQ'
- Vulnerab ility Scan
- On-site Review.

Do I have to complete all the validation tasks?

Visa and MasterCard have defined four merchant levels to determine the requirements. These are summarised in the table below:

Level	Visa/MasterCard	Validation Requirements
1	• Merchants processing over 6 million transactions annually (all channels), or global merchants identified as Level 1 by any card scheme	• Annual on-site assessment by QSA[1] • Quarterly network scans by ASV • Attestation of compliance
2	• Merchants processing 1 million to 6 million transactions annually (all channels)	• Annual SAQ[2] • Quarterly network scans by ASV • Attestation of compliance
3	• Merchants processing 20,000 to 1 million e-commerce transactions annually	• Annual SAQ • Quarterly network scans by ASV
4	• Merchants processing less than 20,000 e-commerce transactions annually, and all other merchants processing up to 1 million transactions annually	• Annual SAQ • Quarterly network scans by ASV

1 As at 30/06/12, Level 1 merchants conducting annual onsite assessments using an internal auditor must ensure that primary internal auditor staff engaged in validating compliance with the PCI DSS attend PCI SSC ISA Training and pass the associated accreditation program annually in order to continue to use internal auditors.

2 As at 30/06/12, Level 2 merchants conducting an annual self-assessment questionnaire must ensure that staff engaged in the self-assessment attend PCI SSC ISA Training and pass the associated accreditation program annually in order to continue the option of self-assessment for compliance validation.

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 Approved Scanning Vendor (ASV).

Regular quarterly scans are necessary to ensure that your systems and applications continue to afford adequate levels of protection. For a list of ASVs that provide vulnerability scanning, please visit **www.pcissc.org**

What is the Self-Assessment Questionnaire?

The SAQ is a free, confidential tool that can be used to gauge your level of compliance with the PCI DSS. It is an online tool made up of a series of 'yes' and 'no' questions. Once it has been completed, you will have made a good assessment of your risk level. If the assessment indicates that remedial work is needed, you will need to undertake this work in order to comply with the PCI DSS. You can complete the process internally or work with a QSA to manage it on your behalf.

Once completed, the SAQ will provide you with an assessment of where potential risks may lie. The questionnaire will also point out if any remedial action is required. If this occurs, you must make sure that you act quickly to ensure compliance with the PCI DSS standards.

The appropriate SAQ can be downloaded from the PCI Council website and can be completed manually and submitted to the bank. Alternatively a number of Scan vendors support acquiring online completion of the SAQ on their websites.
You can visit the PCI Council website at:
www.pcisecuritystandards.org/

What do I do once I acknowledge my validation to PCI DSS compliance?

All information relating to PCI DSS certification should be stored in a safe location on your merchant premises and your certificate of compliance must be emailed to **pci@nab.com.au**

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

Merchants must adhere to PCI DSS requirements, failure to do so may give rise to a breach of the Merchant Agreement and/or lead to your merchant facilities being suspended or terminated.

For more information call

13 13 12

8am – 8pm AEST, Monday to Friday
9am – 6pm AEST, Saturday and Sunday
or visit us at **nab.com.au**

Hearing impaired customers
with telephone typewriters
can contact us on **1300 363 647**

The registered address of the issuer:
National Australia Bank Limited
Level 1
800 Bourke Street
Docklands VIC 3008