Payment Card Industry Data Security Standards

The payment card industry data security standard

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. PCI DSS is a set of industry-wide requirements and processes, supported by every major international payment card scheme through the PCI Security Standards Council or 'PCI Council'. In order to accept payments via cards issued by the international payment card schemes it is important to understand and comply with these standards. They also form part of the NAB Merchant Agreement.

Why is PCI DSS important for my business?

PCI DSS is essential for businesses of all sizes to help prevent card payment a breaches and maintain customer trust. Fraudsters use increasingly sophisticated techniques to exploit weaknesses and gain access to sensitive information and card payment data.

In addition to financial losses, a data breach may lead to long-term implications such as severely harm your business's reputation, cause customer harm, bring about lawsuits and incur financial penalties.

The standards include:

- Build and Maintain a Secure Network and Systems
- Protect Account Data
- Maintain a Vulnerability Management Program
- Implement Strong Access Control Measures
- Regularly Monitor and Test Networks
- Maintain an Information Security Policy

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

The PCI DSS requires you to:

- assess if your business protects cardholder data
- ensure it has a secure network
- maintain a security policy
- maintain strong access control measures
- regularly monitor and test networks
- if youutilise a third part, ensure they are also meeting the PCI DSS requirements.

The 12 PCI DSS requirements are as follows:

Build and Maintain a Secure Network and Systems

1. Install and maintain network security controls.
2. Apply secure configurations to all system components.

Protect Account Data

3. Protect stored account data.
4. Protect cardholder data with strong cryptography during transmission over open, public networks.

Maintain a Vulnerability Management Program

5. Protect all systems and networks from malicious software.
6. Develop and maintain secure systems and software.

Implement Strong Access Control Measures

7. Restrict access to system components and cardholder data by business need to know.
8. Identify users and authenticate access to system components.
9. Restrict physical access to cardholder data.

Regularly Monitor and Test Networks

10. Log and monitor all access to system components and cardholder data.
11. Test security of systems and networks regularly.

Maintain an Information Security Policy

12. Support information security with organisational policies and programs.

Further information can be obtained from **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's 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?

NAB Merchant PCI Help Desk will be able to provide advice on the validation process to merchants who require it. Please contact PCI@nab.com.au for introduction to the PCI DSS requirements.

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 **visa.com.au/support/small-business/security-compliance.html** or email **vpssais@visa.com**

MasterCard's program is called the **Site Data Protection Program 'SDP**' – for details visit **mastercard.com.au/en-au/merchants/safety-security/security-recommendations/site-data-protection-PCI.html** or email **sdp@mastercard.com**

Frequently asked questions

Who needs to be compliant?

All entities that store, process, redirect and/or transmit cardholder data, such as merchants, or 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 is included in 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 tasks include:

- The Self-Assessment Questionnaire 'SAQ'
- Vulnerability 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 Qualified Security Assessor (QSA)[1] • Quarterly vulnerability scans by Approved Scanning Vendor (ASV) • Attestation of compliance
2	• Merchants processing 1 million to 6 million transactions annually (all channels)	• Annual Self-Assessment Questionnaire (SAQ)[2] • Quarterly vulnerability scans by Approved Scanning Vendor (ASV) • Attestation of compliance
3	• Merchants processing 20,000 to 1 million e-commerce transactions annually	• Annual SAQ • Quarterly vulnerability 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	• You should complete an annual SAQ and quarterly vulnerability scans by a PCI-approved scanning vendor.

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 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 **listings.pcisecuritystandards.org/assessors_and_solutions/approved_scanning_vendors**

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: **pcisecuritystandards.org/document_library/**

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.

What do I do if I suspect a data breach has happened?

If you suspect or have confirmation of a data breach, you must contact us immediately. You can contact us by:

- Calling your Relationship Manager and Emailing our Merchant Risk PCI Team on pci@nab.com.au
- We may require you to engage a certified PCI Forensic Investigator (PFI) to conduct a forensic investigation to determine when the data breach occurred, how it happened, and whether any card payment information was at risk. You must avoid attempting to change or remove evidence that may impact the ability to conduct the forensic investigation.

1. 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 Payment Card Industry Security Standards Council Internal Security Assessor (PCI SSC ISA) Training and pass the associated accreditation program annually in order to continue to use internal auditors.
2. 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 or engage a QSA for a On-site assessment or a QSA assisted SAQ.

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
395 Bourke Street
Melbourne VIC 3000