

Westpac Merchant

A guide to meeting
the new Payment
Card Industry
Security Standards

Contents

Introduction	01
What is PCIDSS?	02
Why does it concern you?	02
What benefits will you receive from PCIDSS?	03
What does PCIDSS investigate?	03
What software/hardware is included in the PCIDSS review?	04
What should you do in the event of a breach?	05
How do you get PCIDSS certified?	05
What is your PCIDSS Level?	06
Level 1	06
Level 2 and 3	06
Level 4	06
Other times when evidence of compliance may be required	07
PCIDSS Self Assessment Questionnaire	08
Port Scan	09
Who does the scanning	09
What happens if your business fails the tests?	10
PCIDSS On-Site Review (audit)	11
What penalties may apply to my business for failure to meet PCIDSS requirements?	12
Checklist for PCIDSS compliance	14
What should you do now?	15
Westpac support	15
PCIDSS information available online	15

Introduction

- Merchants that store, process, transmit or have access to credit card details – or use a service provider to do so – have a responsibility to ensure that customers' payment details remain secure.
- Currently, all systems processing information in the cardholder data environment must operate cardholder account information security programmes, such as MasterCard's Site Data protection (SDP) and Visa's Account Information Security (AIS). The growth of e-commerce has seen a proliferation in electronic crime – such as identity theft and hacking – which means any storage device containing card data is increasingly vulnerable to compromise, especially those in systems that offer public internet access.
- In response to this threat, the Payment Card Industry (PCI) has developed a new set of security requirements that govern credit card transactions and protect cardholder data. These are known as the Payment Card Industry Data Security Standards (PCIDSS) and all merchants will soon be required to implement them.
- Westpac has compiled this guide – Complying with PCIDSS – to introduce the new standards, outline the changes that are to take place, and explain how merchants can comply. Please read this document carefully and act on the information it contains. Failure to comply may result in fines, or suspension and even closure of your credit card transaction facility.

Important note:

PCIDSS defines practices for protecting account and transaction information. None of Westpac or the Card Schemes, however, makes any warranty or claim that any of these standards, or the information set out in this brochure, will prevent security breaches or losses, and each disclaims any responsibility or liability for any security breaches or losses incurred, whether the PCIDSS or this brochure has been implemented completely or not.

References within this guide to non-Westpac websites are provided for your convenience and Westpac accepts no responsibility for the availability or content therein.

What is PCIDSS?

PCIDSS is a set of standards implemented by MasterCard and Visa to support their existing cardholder account information security programmes.

They are designed to create a single, industry-wide approach to protecting sensitive data for all card brands – primarily e-commerce credit card transactions but also non-e-commerce ones as well.

The aim of PCIDSS is to help manage the risk to merchants of external/internal data breaches or hacker access by establishing the security processes and controls that must be implemented in order to meet the scheme's requirements for protecting cardholder data.

Further information on PCIDSS can be found online at:

www.visa-asia.com/secured

sdp.mastercardintl.com

www.pcisecuritystandards.org

Why does it concern you?

PCIDSS compliance is required of **all** merchants and service providers that store, process, transmit or have access to cardholder data – or have systems that offer public internet access to the company – and extends to **all** payment channels: point of sale, internet, phone, or mail.

Failure to comply may result in fines, or suspension and even closure of your credit card transaction facility.

What benefits will you receive from PCIDSS?

- Ensuring the security of cardholder data by complying with PCIDSS can lessen the likelihood of a data breach within your business;
- Your business may experience continued patronage due to confidence in the secure storage of vital customer information;
- By completing the PCIDSS programme, your company will avoid any penalties for non-compliance with PCIDSS, and is less likely to have penalties imposed in the event of a data breach.

What does PCIDSS investigate?

The PCIDSS programme will examine and assess how your business:

- built its secure network;
- maintains a secure network;
- protects cardholder data;
- maintains a vulnerability management programme;
- implements strong access control measures;
- regularly monitors and tests networks; and
- maintains a security policy.

If your business utilises a third party to store, process, transmit, or which has access to, credit card details, it will also be examined and assessed on the factors listed above.

What software/hardware is included in the PCIDSS review?

PCIDSS applies to all 'system components'. These are defined as any network component, server, or application included in, or connected to, the cardholder data environment.

Network components include, but are not limited to:

- firewalls;
- switches;
- routers;
- wireless access points;
- network appliances; and
- other security appliances.

Servers include, but are not limited to:

- web;
- database;
- authentication;
- DNS (domain name servers);
- mail;
- proxy;
- FTP (file transfer protocol); and
- NTP (network transfer protocol).

Applications include:

- purchased (off-the-shelf);
- customised; and
- internal and external (web) applications.

What should you do in the event of a breach?

Immediately notify Westpac via your Relationship Manager, or through our PCIDSS Support area (PCIDSS_Support@westpac.co.nz) that you suspect a breach has occurred. In the interim, also undertake the following measures:

- Isolate the problem, such as unplugging the affected system from the network;
- Do not install software or make changes;
- Tighten network security controls;
- Alert your acquiring bank;
- Notify relevant authorities;
- Calculate the gross potential exposure; and
- Document every move.

It is a requirement of PCIDSS that Westpac investigate any breaches. Your business, and any third party involved in assisting your business with processing transactions, will be required to provide assistance and access to Westpac during the investigation. There are serious consequences for failing to cooperate (see *What Penalties may apply to my business for failure to meet PCIDSS requirements*).

Important note: All merchants that have suffered a hack or an attack that results in an account compromise could be required to meet the compliance criteria of a Level 1 merchant.

How do you get PCIDSS certified?

The new standards specify activities and procedures that businesses must follow to prove that a system is compliant with PCIDSS, to the satisfaction of both Westpac and the card companies. These include the completion of the following validation tools:

- Self Assessment Questionnaire(s);
- Port Scans to detect system vulnerabilities; and
- Full onsite reviews (for large merchants only).

On successful certification with PCIDSS, your business will be registered as being compliant. You will also need to maintain ongoing compliance by completing the appropriate PCIDSS activities on a regular basis.

What is your PCIDSS level?

Based on the number of credit card transactions processed by the business annually, the Card Schemes classify merchants into three levels – the letter accompanying this guide will indicate whether your company is Level 1, 2, 3 or 4.

PCIDSS Level	Number of card transactions that your Businesses turns over (Annual Visa/MasterCard/BankCard)
Level 1	More than 6,000,000 (six million) card transactions per annum
Level 2	More than 1 million but less than 6 million transactions of any type per annum
Level 3	More than 20,000 e-commerce, but less than 1 million e-commerce transactions per annum
Level 4	All other merchants

Your company's PCIDSS level will govern the certification requirements you will need to meet to become compliant, as follows:

Level 1

As these merchants are accepting extremely large volumes of card payment details, a data breach at this level could involve thousands of cardholders. Accordingly, these merchants must complete an:

- Annual Self Assessment Questionnaire;
- Quarterly port scan;
- Annual on-site reviews from a Card Scheme-accredited audit company.

Levels 2 and 3

Merchants at this level are processing moderately large volumes of credit card payments and are required to complete an:

- Annual Self Assessment Questionnaire;
- Quarterly port scan.

Level 4

These merchants are required to complete an:

- Annual Self-Assessment Questionnaire;
- Quarterly port scan.

Other times when evidence of compliance may be required.

Normally, you will be expected to certify for PCIDSS at regular intervals depending on your level. However, there are also a number of exceptional circumstances where you may be asked to carry out an immediate certification of your system to confirm its ongoing compliance with PCIDSS, as follows:

1. Your business installs/upgrades software or hardware that stores, processes, transmits or has access to credit card payment details, or has access to the internet;
2. Your Visa, MasterCard and Bankcard volumes exceed the PCIDSS Level assigned when you applied - in other words, your business moves to a different level;
(Westpac will monitor your transactions, advise you of any change in your level, and explain any additional compliance activities you will need to undertake)
3. You've experienced a data breach, in which case, you may be required to rectify any weaknesses in your system and undertake immediate re-certification for PCIDSS;
4. A Card Scheme requests that you undertake compliance for any reason.

PCIDSS Self Assessment Questionnaire

The Self Assessment Questionnaires consist of yes/no questions that aim to identify:

- weaknesses in day-to-day operations;
- vulnerabilities in software and hardware; and
- other potential areas of non-compliance.

The results are designed to show businesses what they need to correct and improve upon in order to provide a secure card acceptance environment.

The questionnaire covers a number of operational and technical areas. We recommended that, where these areas are supported and managed separately within your business, the appropriate responsible parties are actively involved.

Please complete the Self Assessment Questionnaire and send it to Westpac for review. Copies can be downloaded from:

www.pcisecuritystandards.org

Port Scan

If required, your business will need to have all ports that can access the internet scanned to comply with PCIDSS quarterly. The scans are aimed at identifying vulnerabilities and mis-configurations of websites or IT infrastructures that contain externally facing IP addresses, including:

- IP addresses;
- filtering devices, such as firewalls and routers;
- WEB servers;
- application servers;
- Domain Name servers;
- wireless access points; and
- and load balancers.

Scans are mandatory not only for merchants offering web-based transactions, but also for those with systems connecting to the public internet, including email and web browsing.

Who does the scanning?

Port scans can be completed by engaging a certified, third party scanning agent. You should then advise Westpac of the results.

Port scans follow a defined set of procedures and must be conducted correctly to ensure compliance with PCIDSS. Further information on the scanning process and a list of certified agents is available from the PCI Council website:

www.pcisecuritystandards.org

What happens if your business fails the tests?

Self-Assessment Questionnaire

At the end of the process, if the Self-Assessment Questionnaire identifies vulnerabilities in your system, you will be required to rectify these in order to ensure your system is fully PCIDSS compliant. If areas of non-compliance do exist, they will need to be rectified and reported to Westpac in terms of the level of risk they present.

Port Scan Results

Should the port scan results uncover any high-risk issues, you will need to rectify these and pass a further scan in order to be considered compliant. If it is not possible to rectify the areas of non-compliance immediately, you will be required to provide a plan of corrective action to Westpac.

Failure to rectify the areas of non-compliance in a timeframe acceptable to Westpac may result in suspension or closure of your facility until the issues are resolved.

Westpac will review the results of your Self-assessment Questionnaires and port scans from time to time and may contact you for further information or to discuss your results.

PCIDSS On-Site Review (audit)

Businesses that are required to conduct an annual On-site Review must engage an independent Visa-certified Qualified Security Assessor (QSA) to perform this function. Westpac must be advised of your proposed QSA. The timing for the On-site Review must be approved by Westpac.

A list of QSAs in New Zealand can be obtained from:

www.pcisecuritystandards.org

As a way of reducing costs, you may wish to include the requirements of the PCIDSS On-site Review into your normal annual audit. As it's likely to become a recurring cost, it would also be advisable to plan and budget for it as part of your annual expenditure.

If any areas are deemed non-compliant you will need to address these, and provide a plan of action to Westpac on how you plan to achieve PCIDSS compliance. You should email us at our dedicated PCIDSS support address:

PCIDSS_Support@westpac.co.nz

Failure to become fully compliant in a timeframe acceptable to Westpac may result in suspension or closure of your facility until the issues are resolved.

What penalties may apply to my business for failure to meet PCIDSS requirements?

As part of an ongoing PCIDSS monitoring programme Westpac is required to report the PCIDSS levels of merchants to MasterCard and Visa, and confirm their compliance status on a regular basis.

Where merchants have failed to meet the PCIDSS requirements, the Card Schemes may, at their discretion, impose fines for non-compliance.

These can be avoided by ensuring your business complies with the PCIDSS requirements.

There are also a range of costs your business may be liable for, which may result from any data breach at your business.

These include:

- Costs for monitoring and/or replacement of cards compromised in the data breach;
- Costs for failure to report and rectify the breach in a timely and effective fashion;
- Forensic costs to determine the cause and impacts of the breach; and
- Costs for corrective action to address the cause of the data breach.

These penalties and costs will be imposed on Westpac, but would be passed on to your business under the contractual arrangements with Westpac. Although compliance with PCIDSS will not automatically protect you against these penalties and costs, there is a much greater possibility of a full or partial waiver if you ARE compliant.

The table below summarises the fines your business could potentially face, from both MasterCard and Visa, as a result of non-compliance or a data breach.

Fee/Penalty	MasterCard	Visa
Non-compliance	<ul style="list-style-type: none"> ▪ Level 1 merchants – up to \$US25,000 ▪ Level 2 and 3 Merchants – up to \$US5,000 	No penalties at this stage
Data breach	<p>\$US100,000 per violation, with a maximum aggregate assessment of \$US500,000 for additional or continuing violations during any 12-month period.</p> <p>And any investigative and related costs incurred by MasterCard.</p>	25% of overall fraud capped at \$US400,000 per violation, where VISA fraud is in excess of \$1 m.
Failure to investigate/report exposure	Up to \$US25,000 each day of non-compliance	
Per card fees for a data breach	The card issuers may have a right to claim for compromised or potentially compromised cards: \$US25 for each card re-issued; and \$US5 for each card monitored (but not reissued).	Each card issuer may claim \$US5 per card re-issued for more than 1,000. Capped at \$US100,000 per incident.

*subject to change

Checklist for PCIDSS compliance

For your business to have the greatest chance of meeting the PCIDSS requirements, these basic guidelines should at all times be followed.

General handling

- Do not store sensitive cardholder information;
- Never store the magnetic strip information after obtaining an authorisation;
- Never store the Card Validation Code: the three digit code printed on the signature panel of credit and charge cards;
- Store only the customer's account information that is necessary for your business, such as name, address or email address, and only with their knowledge and approval;
- Store all data containing cardholder information (for example, authorisation logs, transaction reports and transaction receipts) in a secure place that allows access to authorised personnel only;
- Encrypt card account numbers in databases or only use part of the account number (for example, print the first six or last few digits of the account number on receipts).

Destroy cardholder information after use:

- Securely destroy all media containing transaction data with cardholder information that is no longer needed for business, legal and/or regulatory reasons.

Use only secure payment solutions through Westpac or accredited third parties:

- Use only Westpac accredited Gateway providers, or Westpac accredited payment solutions for processing credit and charge card transactions over the internet;
- Westpac's solutions and our accredited Gateway providers are required to meet the PCIDSS standards. While this does not guarantee your business will be exempt from liability in the event of a data breach, if you use other Gateway providers or solutions not accredited by Westpac, any violation by your Gateway provider may cause unnecessary financial exposure and inconvenience to your business.

If you absolutely *must* store the card payment details, then:

- Ensure the system where the card payment details are stored is not directly accessible through the internet;
- Ensure you keep your operating and security system software patches and updates current;
- Ensure you have adequate protection, such as firewalls, intrusion detection systems, etc;
- Ensure you obtain a dynamic virus checker, for example Trend PC cillan, McAfee or Norton, and enable live updates every time you are online;
- Ensure you comply with PCIDSS at all times.

Westpac support

If you require further assistance, please send an email to PCIDSS_Support@westpac.co.nz or call the Westpac PCIDSS Support Line on 0800 888 066 .

PCIDSS information available online

PCI Council www.pcisecuritystandards.orgfnf

Notes

Westpac New Zealand Limited
10-08