Your guide to the Payment Card Industry Data Security Standard (PCI DSS).

Merchant Business Solutions.

June 2020.

Contents.

Introduction.

At Westpac we are committed to providing our merchants with every assistance in protecting their business from the growing threat of an Account Data Compromise (ADC). Criminals are using increasingly sophisticated techniques to obtain customer account information, therefore it is critical that merchants implement rigorous controls to minimise the risk of being the subject of an ADC.

The Payment Card Industry Data Security Standards (PCI DSS) is a set of comprehensive requirements for enhancing payment account data security and forms industry best practice for any entity that stores, processes and/or transmits cardholder data. As a merchant it is important that you understand these standards and implement controls to your business environment to avoid potential financial penalties, investigative costs and negative media attention associated with an ADC. It is also important that you ensure that any third party entity which stores, processes and/or transmits cardholder account data on your behalf is compliant to the PCI DSS.

The PCI DSS was developed by the Payment Card Industry Security Standards Council (PCI SSC) and has been formalised into the Mastercard® Site Data Protection (SDP) and Visa Account Information Security (AIS) programs. It is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organisations proactively protect customer account data.

The PCI DSS consists of 6 core principles which are accompanied by 12 requirements. The PCI DSS applies to all merchants, however the scope of your assessment changes depending on what solution you use and how you operate your business. These requirements can be viewed on the following page.

What are the 12 key requirements of PCI DSS?

The 12 key requirements are listed in the following table.

PCI data security standard	
Build and maintain a secure network and systems	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. Protect all systems against malware 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. Identify and authenticate access to system components 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

Protect your business.

Compliance to the PCI DSS greatly reduces the possibility of being the subject of an ADC and in turn protects your business reputation and ensures you retain customer confidence in your brand.

What is an Account Data Compromise (ADC)?

An ADC is when a person or group gain unauthorised access to cardholder data that is held within your business environment in either electronic or physical form. It can be identified in a number of ways however it is usually detected as a common point of purchase before cards are used fraudulently elsewhere.

Once a potential ADC has been reported a PCI forensic investigator must come on-site to determine the source of the compromise and quantify the amount of cardholder data that has been stolen.

What are the potential impacts of an ADC?

If you become the subject of an ADC you risk financial penalties, the suspension or termination of your merchant facility, damage to your brand and reputation and having to undertake additional ongoing audit tasks.

There have been, and continue to be, many examples of ADC events worldwide and they have been experienced by all types of business small and large. It is important to recognise that criminals do not target any particular type of business, if there is an identified weakness and they can exploit it, they will.

Once a potential ADC has been identified a PCI forensic investigator may be required to come on-site to determine the source of the compromise and quantify the amount of cardholder data that has been stolen.

Your business may be required to change your payment solution to move all processing of cardholder data to an entirely outsourced PCI DSS validated third-party service provider.

Where do I start?

The PCI DSS can be found on the PCI SSC website **pcisecuritystandards.org**

It is recommended that you perform a gap analysis by completing the relevant Self Assessment Questionnaire (SAQ) and, when applicable, engage an Approved Scanning Vendor (ASV) to perform a vulnerability scan. Both the SAQs and a list of ASVs can be found on the PCI SSC website. More information about SAQs can also be found on page 9 of this brochure.

What are my compliance requirements?

Being compliant to the PCI DSS forms part of your merchant agreement, however your validation requirements differ depending on the number of transactions you process annually and the merchant solution you use. The use of compliant third party entities also forms part of your merchant agreement.

How do I determine my validation requirements?

As Mastercard and Visa have different transaction levels which regulate the requirements, we have simplified the process by setting parameters for you based on existing merchant information. You may notice that our validation requirements may differ slightly from those of Mastercard or Visa which you may view online, or in other material from the Card Schemes.

Westpac will review your transaction count annually and should we require you to validate compliance as a Level 1, 2 or 3 merchant we will advise you accordingly.

At all times, the Westpac PCI DSS Levels will take precedence over Mastercard and Visa levels for our merchants. We reserve the right to reclassify your level at any time for any reason.

Westpac PCI Levels:

PCI DSS Level	Number of Visa or Mastercard transactions processed by the business annually	Validation requirements
Level 1	More than 6,000,000 transactions per annum	1. Annual on-site assessment completed by a QSA 2. Quarterly Vulnerability Scan performed by an ASV
Level 2	More than 1,000,000 transactions but less than 6,000,000 transactions per annum	
Level 3	More than 20,000 e-commerce transactions but less than 1,000,000 total transactions per annum	1. Annual SAQ 2. Quarterly Vulnerability Scan performed by an ASV
Level 4	All other merchants	Recommended SAQ and Vulnerability Scans (if applicable)

What is the Self-Assessment Questionnaire (SAQ)?

The SAQ is a validation tool intended to assist merchants that are not required to undergo an on-site security assessment, in self-evaluating their compliance with the PCI DSS.

There are a variety of different SAQs which cater for different merchant environments, for example stand-alone terminal solutions and fully outsourced eCommerce solutions. You should complete the SAQ which is most appropriate to your business and if in doubt you should complete SAQ D.

The SAQs can be viewed and downloaded from the PCI SSC website.

The different SAQs are outlined in the table below.

SAQ	Description
A	Card-not-present merchants (e-commerce or mail/telephone order) that have fully outsourced all cardholder data functions to PCI DSS compliant third-party service providers, with no electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises. Not applicable to face-to-face channels.
A-EP	E-commerce merchants who outsource all payment processing to PCI DSS validated third parties, and who have a website(s) that doesn't directly receive cardholder data but that can impact the security of the payment transaction. No electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises. Applicable only to e-commerce channels.
B	Merchants using only: • Imprint machines with no electronic cardholder data storage; and/or • Standalone, dial-out terminals with no electronic cardholder data storage. Not applicable to e-commerce channels.

B-IP	Merchants using only standalone, PTS-approved payment terminals with an IP connection to the payment processor, with no electronic cardholder data storage. Not applicable to e-commerce channels.
C-VT	Merchants who manually enter a single transaction at a time via a keyboard into an Internet-based virtual terminal solution that is provided and hosted by a PCI DSS validated third-party service provider. No electronic cardholder data storage. Not applicable to e-commerce channels.
C	Merchants with payment application systems connected to the Internet, no electronic cardholder data storage. Not applicable to e-commerce channels.
P2PE-HW	Merchants using only hardware payment terminals that are included in and managed via a validated, PCI SSC-listed P2PE solution, with no electronic cardholder data storage. Not applicable to e-commerce channels.
D	SAQ D for Merchants: All merchants not included in descriptions for the above SAQ types. SAQ D for Service Providers: All service providers defined by a payment card brand as eligible to complete a SAQ.

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 will test all of your network equipment, hosts and applications for known vulnerabilities. Scans are intended to be nonintrusive, and must be conducted by an Approved Scanning Vendor (ASV). A vulnerability scan would not ordinarily be required for a merchant using a stand-alone terminal.

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

A current list of Approved Scanning Vendors (ASV) can be located on the PCI SSC website.

What is an on-site assessment?

If you are required to complete an on-site assessment you will need to employ the services of a Qualified Security Assessor (QSA). A QSA is accredited by the PCI SSC annually to validate merchant compliance to the PCI DSS.

If your business requires an annual on-site assessment you may wish to include the PCI DSS review requirements within your normal annual audit to reduce costs. As this is likely to become a recurring cost, we would recommend that you budget for the review as part of your annual expenditure.

A list of Qualified Security Assessors (QSA) can be viewed on the PCI SSC website.

You must advise us of your proposed QSA, and the timing for the on-site assessment, remediation plan and validation of compliance.

What should I do if I'm 'non-compliant'?

Once you have completed the SAQ you may discover that there are some deficiencies in your business environment that don't meet the PCI DSS. If this is the case it is imperative that you develop a plan which outlines actions for each non-compliant element along with estimated timeframes for the completion of each task. If you are a 'non-compliant' Level 1, 2 or 3 merchant you are required to submit your remediation plan within the Prioritised Approach Tool every quarter. By demonstrating progress towards compliance you give yourself the best possible chance of avoiding 'non-compliance' penalties.

The Prioritised Approach Tool.

The Prioritised Approach Tool was developed by the PCI SSC to assist 'non-compliant' merchants in prioritising their remediation work. It has divided the PCI DSS requirements into six milestones which indentify which requirements need the most attention.

The Prioritised Approach Tool can be found on the PCI SSC website.

What are the requirements for Payment Applications?

If you implement any 'off the shelf' software applications you must ensure that they are compliant to the Payment Application Data Security Standards (PA DSS). The PA DSS was developed by the PCI SSC to ensure that software vendors and others who develop payment applications that store, process and/or transmits cardholder data allow the environment in which it is implemented to be compliant to the PCI DSS.

A list of compliant Payment Applications can be found on the PCI SSC website.

Any payment application which is developed in house or heavily customised will be encapsulated in the scope of either the merchant's or the service provider's PCI DSS requirements and does not need to be compliant to the PA DSS.

What should I do in the event of an Account Data Compromise?

Immediately notify Westpac via your Relationship Manager, or through our Merchant Risk Team (pci@westpac.com.au) that you suspect that an ADC event has occurred. Within the first 24 hours take action to prevent further loss of data by conducting a thorough investigation of the suspected or confirmed loss or theft of cardholder data and transaction information.

To preserve evidence and facilitate the investigation:

- Do not access or alter compromised systems (i.e. do not log on at all to the machine and change passwords, do not log on as ROOT);
- Do not turn off the compromised associated hardware machines. Instead, isolate compromised systems from the network (i.e. unplug cable);
- Preserve logs and electronic evidence;
- Keep a record of all actions taken;
- If using a wireless network, change the SSID on the AP and other machines that may be using this connection with the exception of any systems believed to be compromised; and
- Be on 'high' alert and monitor all systems with cardholder data and transaction information.

It is a requirement of the Card Schemes that a PCI Forensic Investigator (PFI) investigate any breaches affecting our merchants. We will request that you, and any third party involved in assisting your business with processing transactions, provide assistance and access to us for the term of the investigation. There are serious consequences for failing to co-operate in the investigation of any security breaches.

What penalties may apply to my business for failure to meet the PCI DSS requirements?

- If your business is assessed by the Card Schemes as being 'non-compliant' to the PCI DSS you are liable to financial penalties. 'Non-compliance' is assessed at the discretion of the respective Card Schemes and start at USD $25,000 for Level 1 and 2 Merchants and USD $10,000 for Level 3 Merchants for the first quarter. Fines have the potential to double every subsequent quarter that you remain 'non-compliant'.
- In the event that your business experiences an ADC event you may be liable for financial penalties which may be in the hundreds of thousands of dollars. A number of factors are considered by the Card Schemes in the assessment of financial penalties including, but not limited to, the number of compromised accounts, the presence of sensitive authentication data, the number of accounts which need to be monitored by the issuer and the Merchant's level of compliance to the PCI DSS.

This page has been left blank intentionally.

We're here to help.

If you have any questions in relation to PCI DSS please contact us via email at pci@westpac.com.au

Additional Information.

Westpac: **westpac.com.au/business-banking/merchant-services/preventing-fraud**

Visa: **visa.com**

Mastercard: **mastercard.com/us/sdp/index.html**

PCI SSC: **pcisecuritystandards.org**