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

Effective date: 08 December 2023

We're here to help

PCI Security Standards Council:
pcisecuritystandards.org

Westpac:
westpac.com.au/merchantsupport

Visa:
visa.com.au

Mastercard:
mastercard.com.au

If you have any questions, please email us at:

pci@westpac.com.au

Accessibility support.

At any time, you can inform us how you would prefer to be contacted. If you are deaf and/or find it hard hearing or speaking with people who use a phone, you can reach us through the National Relay Service (NRS). To use the NRS you can register by visiting **accesshub.gov.au/about-the-nrs**

Visit **westpac.com.au/web-accessibility** for further information on our accessible products and services for people with disability.

In short

As a business, you need to safeguard your customer's sensitive payment information.

Your data security systems need to meet the Payment Card Industry Data Security Standards (PCI DSS) guidelines. This is even if you outsource your data security to a third-party service provider.

You could face penalties and fines if you don't have adequate data security systems in place.

It's essential to notify us in case any customer payment data is compromised.

You can find more information in this guide and on the PCI DSS website pcisecuritystandards.org

Protecting your payment data and your business

When it comes to running a business, most business owners understand the importance of maintaining the safety and security of a customer's sensitive payment information.

Unfortunately, criminals are using increasingly sophisticated techniques to get customer account information. That's why your business must maintain strict controls to reduce such risks so that customers can trust you with their payment card information.

We're committed to helping you understand how to protect your business from such threats – often referred to as an Account Data Compromise (ADC).

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's generally detected at a common point of purchase before cards are used fraudulently elsewhere. Both small and large businesses worldwide have fallen victim to such data breaches.

What are the potential impacts of an ADC?

If your business faces an ADC, you may risk fines and penalties, the suspension or termination of your merchant facility, and damage to your brand and reputation.

Once a potential ADC has been identified, a PCI forensic investigator may come on-site to determine the source of the compromise and analyse the amount of cardholder data that's been stolen. You may need to change your payment solution and move all processing of cardholder data to an entirely outsourced PCI DSS validated third-party service provider.

What is PCI DSS?

The Payment Card Industry Data Security Standards (PCI DSS) were created and are maintained by the Payment Card Industry Data Security Standards Council. The Council was founded in 2006 by American Express®, Discover, JCB International, Mastercard® and Visa®, to help reduce costly consumer and bank data breaches. It's a set of comprehensive requirements for improving payment account data security and is intended to help organisations proactively protect customer account data. These global security standards form industry best practice for businesses that store, process and/or transmit cardholder data.

Why is PCI DSS important for my business?

When it comes to payment card data, criminals don't target any particular type of business. And no matter what the size of your business, if they find a weakness and can exploit it, they will. That's why it's critical to have PCI DSS controls in place.

Besides the financial impacts of any breach, the resulting reputational damage could be hard to recover from and may impact your business long term. That's why it's vital that you understand these prescribed standards and implement the necessary controls in your business. You must make sure any third-party provider that stores, processes, and/or transmits cardholder account data on your behalf is compliant with these requirements.

We understand that PCI DSS compliance could be overwhelming for business owners. This guide breaks down all the main steps to safeguard both your business and your customers.

What are the 12 key requirements of PCI DSS?

The PCI DSS consists of 6 core principles which are accompanied by 12 requirements. The PCI DSS applies to all merchants, however the type of controls you'll require will change depending on what payment solution you use and how you operate your business. Meeting these requirements reduces the possibility of experiencing an ADC.

You'll find the 12 key requirements in the following table.

PCI data security standard.

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

Where do I start?

Visit the PCI DSS website pcisecuritystandards.org for more information.

On this website, we recommend that you complete:

- the relevant Self-Assessment Questionnaire (SAQ)
- and, when applicable, engage an Approved Scanning Vendor (ASV) to perform a vulnerability scan. You can find more information about SAQs further ahead in this guide.

What are my compliance requirements?

Meeting the PCI DSS requirements and using compliant third-party providers, all forms part of your merchant agreement. But your validation requirements differ depending on the number of transactions you process annually and the merchant solution you use.

How do I determine my validation requirements?

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

We'll review your transaction count annually, and if we require you to validate compliance as a Level 1, 2, or 3 merchant, we'll let you know.

At all times, the Westpac PCI DSS Levels will take priority over Mastercard and Visa levels for our merchants. We may also reclassify your level at any time – such as when your business grows and changes.

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 eCommerce 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 created to help merchants who aren't required to undergo an on-site security assessment to self-evaluate their compliance with the PCI DSS. The Self-Assessment Questionnaire includes a series of yes-or-no questions for each applicable PCI Data Security Standard requirement.

There are different SAQs that cater to different merchant environments, such as standalone terminal solutions compared with fully outsourced eCommerce solutions. Complete the SAQ which is most appropriate to your business. If you're unsure, complete the SAQ D (which is the complete set of PCI DSS requirements for merchants) or contact us for guidance.

The SAQs can be viewed and downloaded from pcisecuritystandards.org

We've shown the different SAQs in the table below.

SAQ	Description
A	Card-not-present merchants (eCommerce or Mail Order/Telephone-Order) that completely outsource all account data functions to PCI DSS validated and compliant third parties. No electronic storage, processing, or transmission of account data on their systems or premises. Not applicable to face-to-face channels. Not applicable to service providers.
A-EP	eCommerce merchants that partially outsource payment processing to PCI DSS validated and compliant third parties, and with a website(s) that does not itself receive account data but which does affect the security of the payment transaction and/or the integrity of the page that accepts the customer's account data. No electronic storage, processing, or transmission of account data on the merchant's systems or premises. Applicable only to eCommerce channels. Not applicable to service providers.
B	Merchants using only: • Imprint machines with no electronic account data storage; and/or • Standalone, dial-out terminals with no electronic account data storage. Not applicable to eCommerce channels. Not applicable to service providers.

SAQ	Description
B-IP	Merchants using only standalone, PCI-listed approved PIN Transaction Security (PTS) point-of-interaction (POI) devices with an IP connection to the payment processor. No electronic account data storage. Not applicable to eCommerce channels. Not applicable to service providers.
C-VT	Merchants that manually enter payment account data a single transaction at a time via a keyboard into a PCI DSS validated and compliant third-party virtual payment terminal solution, with an isolated computing device and a securely connected web browser. No electronic account data storage. Not applicable to eCommerce channels. Not applicable to service providers.
C	Merchants with payment application systems connected to the Internet, no electronic account data storage. Not applicable to eCommerce channels. Not applicable to service providers.
P2PE-HW	Merchants using only a validated, PCI-listed Point-to-Point Encryption (P2PE) solution. No access to clear-text account data and no electronic account data storage. Not applicable to eCommerce channels. Not applicable to service providers.

SAQ	Description
SPoC*	Merchants using a commercial off-the-shelf mobile device (for example, a phone or tablet) with a secure card reader included on PCI SSC's list of validated SPoC Solutions. No access to clear-text account data and no electronic account data storage. Not applicable to unattended card-present, Mail Order/Telephone Order (MOTO), or eCommerce channels. Not applicable to service providers.
D	SAQ D for Merchants: All merchants not included in descriptions for the above SAQ types. Not applicable to service providers. SAQ D for Service Providers: All service providers defined by a payment brand as eligible to complete a SAQ.

*New SAQ for PCI DSS v4.0.

What is a Vulnerability Scan?

A vulnerability scan makes sure your systems are protected from external threats like unauthorised access, hacking or malicious viruses. The scanning tools will test all your network equipment, hosts, and applications for known vulnerabilities. Scans are intended to be non-intrusive and must be conducted by an Approved Scanning Vendor (ASV). Generally, a vulnerability scan wouldn't be required for a merchant using a standalone terminal.

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

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

What is an on-site assessment?

If you're required to complete an on-site assessment, you'll need to hire a Qualified Security Assessor (QSA). A QSA is accredited by the PCI SSC annually to validate merchant compliance to the PCI DSS. A list of Qualified Security Assessors (QSA) can be viewed on the PCI SSC website.

Important things to keep in mind:

- 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'd recommend that you budget for the review as part of your annual expenditure.
- You must inform 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've completed the SAQ, you may discover that there are some deficiencies in your business environment that don't meet the PCI DSS. It's critical 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're 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' fines.

The Prioritised Approach Tool

The PCI SSC developed the Prioritised Approach Tool to assist 'non-compliant' merchants plan their remediation work. The tool has organised the PCI DSS requirements into six main milestones, which let you know which requirements need the most attention.

You can find the Prioritised Approach Tool on the PCI SSC website.

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

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

To protect evidence and support the investigation:

- Don't access or alter compromised systems (for instance, don't log in to the machine to change passwords, don't log on to the account that by default has access to all commands and files on an operating system, known as ROOT);
- Don't turn off the compromised associated hardware machines. Instead, isolate compromised systems from the network (e.g. unplug the cable);
- Preserve logs and electronic evidence;
- Keep a record of all actions taken;
- If using a wireless network, change the Service Set Identifier (SSD) on the Access Point (AP) and other machines that may be using this connection except for any systems believed to be compromised; and be on 'high' alert and monitor all cardholder data and transaction information systems.

Important things to keep in mind:

- The Card Schemes require that a PCI Forensic Investigator investigate any breaches affecting our merchants.
- We'll request that you, and any third party involved in helping your business with processing transactions, give us the assistance and access we require for the term of the investigation. There are serious consequences for failing to co-operate in the investigation.

What penalties may apply to my business if it doesn't meet the PCI DSS requirements?

If your business experiences an ADC event and the Card Schemes assess your business as 'non-compliant' to the PCI DSS, you may receive fines and penalties. 'Non-compliance' is evaluated at the discretion of the respective Card Schemes and starts 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'.

The Card Schemes consider many factors in assessing financial penalties, some of which include the number of compromised accounts, the presence of sensitive authentication data, the number of accounts that need to be monitored by the issuer and the Merchant's level of compliance with the PCI DSS.

Besides the fines, there are also other potential expenses that could affect your business, such as fraud losses and legal costs.

Westpac acknowledges the traditional owners as the custodians of this land, recognising their connection to land, waters and community. We pay our respects to Australia's First Peoples, and to their Elders, past and present.