



Payment Card Industry Data Security Standards.

Your guide to protecting
cardholder data

SUNCORP BANK
Business



Helping you manage the risk.

Credit Card fraud and data compromises are an increasingly serious problem, costing Australian consumers and businesses millions of dollars each year. Criminals use more and more sophisticated methods in an attempt to obtain cardholder information, making it critical for merchants to safeguard their customers' payment card data.

In response, MasterCard and Visa have together developed the Payment Card Industry Data Security Standard (PCI DSS), an industry-wide standard of data security aiming to manage the risk of both external and internal data compromises. PCI DSS is supported by all major international payment card systems through the PCI Security Standards Council.

All organisations that store, process and transmit cardholder data, such as merchants, must comply with PCI DSS. Failure to do so will give rise to a breach of your Merchant Agreement and potentially lead to your merchant facilities being suspended or terminated.

Understanding your PCI DSS requirements.

Suncorp Bank has engaged Vectra Corporation, a PCI DSS specialist, to assist you in this process. You can contact the Vectra PCI Helpdesk on 1800 558 522.

PCI DSS comprises 12 basic requirements that aim to ensure merchants utilise secure systems, such as restricting access to cardholder data, using a firewall and antivirus software, and encrypting cardholder data transmission. By adhering to the PCI DSS requirements, your business can protect cardholder data more effectively. These requirements are:

Build and maintain a secure network	<ol style="list-style-type: none">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	<ol style="list-style-type: none">3. Protect stored cardholder data.4. Encrypt transmission of cardholder data across open public networks.
Maintain a vulnerability management program	<ol style="list-style-type: none">5. Use and regularly update anti-virus software or programs.6. Develop and maintain secure systems and applications.
Implement strong access control measures	<ol style="list-style-type: none">7. Restrict access to cardholder data by business need-to-know.8. Assign unique ID to each person with computer access.9. Restrict physical access to cardholder data.
Regularly monitor and test networks	<ol style="list-style-type: none">10. Track and monitor all access to network resources and cardholder data.11. Regularly test security systems and processes.
Maintain an information security policy	<ol style="list-style-type: none">12. Maintain a policy that addresses information security for employees and contractors.

Protect your customers and your business.

Protecting your customers' cardholder data and personal information from criminal fraud is an important responsibility of your business. Payment card fraud is becoming more sophisticated, and any business that processes, stores or transmits cardholder account data is a potential target.

As a merchant, you will need to understand what measures your business needs to take to ensure the security of your customers' sensitive personal financial information.

The steps you need to take to become PCI DSS compliant are dependent on:

- The size and nature of your business
- The configuration of your card acceptance system and processes
- How you process your transactions
- The service providers you work with and their respective roles

You will need to complete this compliance every 12 months. Suncorp Bank will send you a reminder notice when your compliance is due for renewal.

How to ensure your business is PCI DSS compliant.

To ensure that you have met your PCI DSS obligations, you will need to complete one or more of the following validation tasks, depending on the nature of your business. These validation tasks include:

- The Self-Assessment Questionnaire (SAQ)
- Vulnerability scan

You will be guided by the SAQ as to which validation tasks your business is required to complete.



Your guide to validation tasks.

The Self-Assessment Questionnaire

The SAQ is a free online tool you can use to determine your compliance with the PCI DSS. It's a series of 'yes' or 'no' questions that will give you a good assessment of your risk level.

You can complete online the appropriate SAQ from the Vectra Portal at <http://suncorp.vectrapci.com.au>

Once you have successfully completed your SAQ, and if your business and systems are compliant, you will be provided with the option to print out your Confirmation of Compliance which is valid for 12 months.

If your SAQ reveals areas which can be improved, you will need to put together a remediation plan to address these issues. Vectra Corporation can provide advice on how to meet your business's specific PCI DSS requirements.

Vulnerability Scan

A vulnerability scan ensures that your internet facing systems are protected as much as possible from external threats such as unauthorised access, hacking or malicious viruses. It's a scanning tool that tests all your network equipment, hosts and applications for known vulnerabilities. Scans are intended to be non-intrusive and are conducted by our security services partner Vectra Corporation.

You will need to conduct regular quarterly scans, to ensure that your systems and applications are still securely configured to provide satisfactory levels of protection. Contact Vectra Corporation for more information.

How PCI DSS compliance can benefit your business.

Compliance means your credit card systems are secure, so your customers will know they can purchase from you with confidence. With a reputation for protecting and valuing your customers' personal data, your brand will be enhanced and potentially benefit from repeat sales. You'll also be lowering your business's exposure to potential financial losses and remediation costs.

To find out more about the
PCI Security Standards Council,
visit www.pcisecuritystandards.org

For more information, contact the
Vectra PCI Helpdesk on 1800 558 522.

And if you have any questions or concerns,
call Suncorp Bank on 13 11 75.

