

PCI DSS Information sheet

(PAYMENT CARD INDUSTRY DATA SECURITY STANDARD)



The payment card industry has introduced data security standards (PCI DSS) to ensure that all cardholder data is always stored, processed and transmitted securely. This applies to all businesses and organisations involved in the processing, storing and/or transmitting of cardholder data. PCI DSS has been developed by the major credit card companies, including MasterCard and VISA, proactively to protect cardholder payment data, and covers security

management, policies, procedures, network architecture, software design and other critical protective measures. These standards have been developed due to the rising incidence of stolen cardholder account data, which has become a major concern for all participants in the payment card industry. As a result of these thefts, merchants and financial institutions suffer fraud losses and incur unanticipated operational expenses, inconveniencing

consumers significantly. To protect your business, your cardholders and the integrity of the payment system you are required to become PCI DSS compliant.

For more information, visit www.nedlink.co.za or call the Nedbank merchant helpdesk on **0860 114 966**

Level	Criteria	Compliance requirements	Merchant action
Level 1 merchants	All merchants with an annual total of more than 6 million MasterCard/Visa transactions.	Annual onsite audit. Quarterly network vulnerability scan.	Contact qualified security assessor (QSA) to perform onsite audit.*
	Merchant organisations (service establishments) processing over 2,5 million American Express transactions annually.		Contact Approved Scanning Vendor (ASV) to perform network scans.*
	All merchants who experience an account data compromise (ADC).		
Level 2 merchants	All merchants with an annual total of more than one million but less than 6 million MasterCard/Visa transactions.	Annual self-assessment questionnaire (SAQ). Quarterly network vulnerability scan Site audit.	Contact QSA to perform onsite audit.*
	Merchant organisations (service establishments) processing between 50 000 and 2,5 million American Express transactions annually.		Contact ASV to perform network scans.*
			Register on Nedbank PCI Management system to complete SAQ.
Level 3 merchants	All merchants with an annual total of MasterCard/Visa e-commerce transactions greater than 20 000 but less than one million transactions.	Annual SAQ. Quarterly network vulnerability scan.	Contact ASV to perform network scans.*
	All merchant organisations (service establishments) processing under 50 000 American Express transactions annually.		Register on Nedbank PCI Management system to complete SAQ.
Level 4 merchants	All other MasterCard/Visa merchants not included in levels 1, 2 and 3.	Annual SAQ. Network vulnerability scan at least quarterly.	Contact ASV to perform network scans.*
			Register on Nedbank PCI Management system to complete SAQ.

* Nedbank can provide a list of approved QSAs and ASVs, that it recommends.

Goals	PCI DSS merchant requirements
Build and maintain a secure network	Install and maintain a firewall configuration to protect cardholder data. Do not use vendor-supplied defaults for system passwords and other security parameters.
Protect cardholder data	Protect stored cardholder data. Encrypt transmission of cardholder data across open public networks.
Maintain a vulnerability management program	Use and regularly update antivirus software. Develop and maintain secure systems and applications.
Implement strong access control measures	Restrict access to cardholder data by business need-to-know. Assign a unique ID to each person with computer access. Restrict physical access to cardholder data.
Regularly monitor and test networks	Track and monitor all access to network resources and cardholder data. Regularly test security systems and processes.
Maintain an information security policy	Maintain a policy that addresses information security.

What is the definition of 'merchant'?

For the purposes of the PCI DSS a merchant is defined as any entity that accepts payment cards bearing the logos of any of the five members of the PCI SSC (American Express, JCB, MasterCard or Visa) as payment for goods and/or services. Note that a merchant that accepts payment cards as payment for goods and/or services can also be a service provider, if the services sold result in storing, processing or transmitting cardholder data on behalf of other merchants or service providers. For example, an ISP is a merchant that accepts payment cards for monthly billing, but also a service provider if it hosts merchants as clients.

What are the penalties for non-compliance?

The payment brands may, at their discretion, fine an acquiring bank \$5 000 to \$100 000 per month for PCI compliance violations. The banks will most likely pass this fine on until it eventually reaches the merchant. Furthermore, the banks will also most likely either terminate your relationship or increase transaction fees. Penalties are not openly discussed nor widely publicised, but they can be catastrophic to a small business.

It is important to be familiar with your merchant account agreement, which should outline your exposure.

MAKE THINGS HAPPEN

NEDBANK

A Member of the  OLD MUTUAL Group



Frequently Asked Questions

What are the deadlines for complying with the PCI DSS?

Compliance is mandated by the payment card brands and not by the PCI. However, for most merchants the deadlines for validating compliance with the PCI DSS have already passed.

You should check with your acquirer and/or bank to check if any specific deadlines apply to you, based on merchant transaction volume (level) as determined by the card payment brands. All entities that transmit, process or store payment card data must be compliant with the PCI DSS.

I'm a small merchant who has a limited payment card transaction volume. Do I need to be compliant with the PCI DSS? If so, what is the deadline?

All merchants, whether small or large, need to be PCI DSS-compliant. The payment brands have collectively adopted PCI DSS as the requirement for organisations that process, store or transmit payment cardholder data. The PCI SSC is responsible for managing the security standards while each individual payment brand is responsible for managing and enforcing compliance with these standards. For questions regarding compliance validation requirements and deadlines, as well as compliance reporting requirements, we recommend that you contact your acquirer. For more information regarding the PCI security standards and supporting documentation, including 'Navigating the PCI DSS' as well as targeted SAQs to assist small and medium merchants, please visit the PCI SSC website at www.pcisecuritystandards.org.

Is the SAQ all I need to complete to validate compliance with the PCI DSS?

In accordance with the compliance programmes of payment brands those merchants and service providers who are permitted by the payment brands to self-evaluate their compliance with the PCI DSS may need to complete the following steps:

- Complete the SAQ according to the instructions in the Self-assessment Questionnaire Instructions and Guidelines.
- Complete a clean vulnerability scan with a PCI SSC-approved scanning vendor, and obtain evidence of a passing scan from the scanning vendor.
- Complete the relevant 'Attestation of compliance' in its entirety (located in the SAQ).
- Submit the SAQ, evidence of a passing scan and the 'Attestation of compliance', along with any other requested documentation, to your acquirer.

As a merchant, what SAQ form should I complete?

For each SAQ form the merchant can find a subsection entitled 'Eligibility to complete SAQ' in the attestation section, www.pcisecuritystandards.org/saq/index.shtml. If the merchant is able to answer 'yes' to each question on the attestation form, that particular form would be applicable in terms of

validating compliance with the PCI DSS. We also recommend that the merchant contacts his/her acquirer to ensure that he/she completes the correct SAQ form. Nedbank's Merchant Management System will provide the relevant SAQ applicable to the merchants logging onto the system; therefore the merchant will complete the SAQ form provided.

If you only accept credit cards over the phone, does the PCI DSS still apply to you?

Yes. All businesses that store, process or transmit payment cardholder data must be PCI DSS-compliant.

If your business has multiple locations, is each location required to validate PCI DSS compliance?

If your business locations process under the same tax ID, then typically you are only required to validate once annually for all locations. Quarterly passing network scans must also be undertaken by a PCI SSC-approved scanning vendor, if applicable.

How does the PCI DSS apply to individual PCs or workstations?

All system components in the network are considered part of the cardholder data environment, unless adequate network segmentation is in place that isolates systems that store, process or transmit cardholder data from those that do not. Without proper network segmentation, the entire network is in scope for the PCI DSS and all PCI DSS requirements apply. QSAs can advise their clients on how to implement network segmentation to reduce the PCI DSS scope. Where there are many PCs or workstations in an environment and all PCs do not need access to the cardholder data environment (CDE), the network segmentation should provide access to the CDE for all PCs that need access, and should prohibit access for all other PCs. With such segmentation in place, the PCI DSS requirements are relevant and should be applied to only that smaller PC population. Regarding the applicability of each PCI DSS requirement to an individual PC, the QSA should also consider features that are part of the PC's basic functionality (for example, logging or file integrity monitoring) or are part of existing network controls, and determine whether these features meet the intent of the PCI DSS requirements to protect cardholder data stored, processed or transmitted by these PCs.

How can issuers be PCI DSS-compliant if they store sensitive authentication data?

With regard to issuers or companies that support issuing services such as third-party processors (TPPs), and other issuing-type processors, it is recognised that such entities may have a legitimate need to retain sensitive authentication data such as the card verification code or value (CVV2, CVC2, CID or CAV2 data) or PIN. While the topic of issuing entities is not specifically addressed in the PCI DSS, the PCI SSC recognises that in certain instances storage of this data is necessary for entities performing, facilitating or supporting issuing

functions. It is allowable for companies that perform, facilitate, or support issuing services to store sensitive authentication data, if they have a legitimate business need to store such data. It should be noted that all other PCI DSS requirements apply to issuers, and the only exception for issuers and issuer processors is that sensitive authentication data may be retained if there is a legitimate reason to do so. A legitimate reason is one that is necessary for the performance of the function being provided for the issuer and not one of convenience. At their discretion, payment card brands may require issuers to validate PCI DSS compliance.

Are debit card transactions within the scope of the the PCI?

Cards falling within the scope of the PCI DSS include any debit, credit and prepaid cards branded with one of the five card association/brand logos that participate in the PCI SSC, namely American Express, Discover, JCB, MasterCard and Visa International.

What constitutes a service provider?

Any company that stores, processes or transmits cardholder data on behalf of another entity is defined as a service provider in the PCI guidelines.

What constitutes a payment application as it relates to PCI compliance?

The term payment application has a very broad meaning in the PCI DSS. A payment application is anything that stores, processes or transmits card data electronically. This means that anything from a point-of-sale system (eg Verifone swipe terminals and ALOHA terminals) in a restaurant to a website e-commerce shopping cart (eg CreLoaded and osCommerce) are all classified as payment applications. Therefore any software that has been designed to process credit card data is considered a payment application.

Can the full credit card number be printed on the consumer's copy of the receipt?

PCI DSS requirement 3.3 states: 'Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed.' While the requirement does not prohibit printing of the full card number or expiry date on receipts (either the merchant copy or the consumer copy), the PCI DSS does not override any other laws that legislate what can be printed on receipts [such as the U.S. Fair and Accurate Credit Transactions Act (FACTA) or any other applicable laws]. See the italicised note under PCI DSS requirement 3.3 'Note: This requirement does not apply to employees and other parties with a specific need to see the full PAN, nor does the requirement supersede stricter requirements in place for displays of cardholder data (for example, for point of sale (POS) receipts).' Any paper receipts stored by merchants must adhere to the PCI DSS, especially requirement 9 regarding physical security. (Source: PCI SSC.)



Do I need vulnerability scanning to validate compliance?

If you electronically store cardholder data post authorisation or if your processing systems have any internet connectivity, a quarterly scan by a PCI SSC-approved scanning vendor is required.

What is a network security scan?

A network security scan involves an automated tool that checks a merchant's or service provider's systems for vulnerabilities. The tool will conduct a non-intrusive scan to remotely review networks and web applications based on the external-facing internet protocol (IP) addresses provided by the merchant or service provider. The scan will identify vulnerabilities in operating systems, services and devices that could be used by hackers to target the merchant's or service provider's private network. As provided by an ASV, the tool will not require the merchant or service provider to install any software and no denial-of-service attacks will be performed.

Note: *Typically only merchants with an external-facing IP address are required to have passing quarterly scans to validate PCI compliance. This is usually merchants completing the SAQ C or D version.*

How often do I have to scan?

Every 90 days/once per quarter you are required to submit a passing scan. Merchants and service providers should submit compliance documentation (successful scan reports) according to the timetable determined by their acquirer. Scans must be conducted by a PCI SSC-approved scanning vendor.

What if a merchant refuses to cooperate?

The PCI DSS is not, in itself, a law. The standard was created by the major card brands such as Visa, MasterCard, Discover, American Express and JCB. At their acquirers'/service providers' discretion, merchants that do not comply with the PCI DSS may be subject to fines, card replacement costs, costly forensic audits, brand damage, etc, should a breach event occur.

For a little upfront effort and cost to comply with the PCI DSS you greatly help reduce your risk from facing these extremely unpleasant and costly consequences.

What should I do if I'm compromised?

We recommend that you follow the procedures outlined in Visa's 'What to Do If Compromised Visa Fraud Control and Investigations Procedures' document; link below. http://usa.visa.com/download/merchants/cisp_what_to_do_if_compromised.pdf.

Where can I find the PCI DSS?

The PCI DSS can be found on www.nedlink.co.za