Merchant Guide to PCI DSS

0800 085 3867
www.cardpayaa.com

ingenico

Card Pay AA

Contents

What is PCI DSS and why was it introduced?

PCI DSS stands for the Payment Card Industry Data Security Standard. This standard is managed by the Payment Card Industry Security Standards Council. PCI DSS is a set of minimum security requirements to help handle payment information securely. It was developed by the major payment card brands (MasterCard, Visa, Amex, Discover & JCB) in 2004. Any business accepting cards for payment of goods or services must be compliant with PCI DSS. Card Pay like most Acquirers, have outsourced their PCI DSS programme to a specialist company – Sysnet. They operate the customer portal, communications, and attestation on our behalf. The Card Pay PCI programme is called **Simple PCI DSS**.

Note: Card Pay are one of the few Acquirers who do not charge customers fees for PCI.

Who needs to become PCI DSS compliant?

If you accept payments by Credit or Debit card you are affected. Any business that stores, processes or transmits any cardholder data must take responsibility for PCI and achieve compliance.

Card Pay Simple PCI DSS - 3 step approach

Merchants logon to the Simple PCI DSS portal and answer some questions

The questions focus around how your business is set up to handle credit and debit card payments. Using dynamic profiling, you are only asked questions relevant to your business in order to figure out your security risk level.

Merchants are assisted in understanding how to protect their business

To help businesses understand and identify areas of your business that might be at risk, you will are brought through the security assessment that matches your business type, including any scanning if needed.

Merchants will finally be asked to confirm and validate their compliance

You will be asked to confirm and validate all of your responses and any tasks you were required to undertake. This is referred to as your Attestation of Compliance (AoC).

What does the Card Pay Simple PCI DSS include?

1. Dedicated online portal (https://simplepcidss.eu/services/login/login)
2. Dedicated program helpdesk with telephone and online chat support
3. Security & compliance advice and assistance

How does a business become compliant?

To report your PCI DSS compliance, businesses need to identify and complete the appropriate Self-Assessment Questionnaire (SAQ) for your business type. You also must ensure security controls are in place at all times to maintain your compliance. Securing your business requires the following steps:

- Analysis of business practice and processes
- Research of appropriate security solutions
- Implementing and maintaining security solutions.

Core to this is protecting your customers payment card data. Customers trust businesses to keep their information safe and you should repay that trust with, at the very least, compliance with PCI DSS.

There are 4 different levels to determine PCI validation requirements

These levels are prescribed by the card schemes. See the table below to understand the different levels and the compliance requirements within each.

Level	Criteria	Validation requirement
1	Any merchant processing in excess of 6 Million MasterCard OR Visa transactions a year, regardless of acceptance channel. Any merchant that has lost data due to a security breech or hacking with the last 12 months.	Annual Report on Compliance (ROC) (by either a Qualified Security Assessor, or qualified internal security resource) Compliant quarterly network scan by Approved Scan Vendor (ASV) Attestation of Compliance Form
2	Any merchant processing between 1 and 6 Million MasterCard OR Visa transactions a year, regardless of acceptance channel	Annual Report on Compliance (ROC) (by either a Qualified Security Assessor, or qualified internal security resource) Compliant quarterly network scan by Approved Scan Vendor (ASV) Attestation of Compliance Form
3	Any e-commerce merchant processing between 20,000 and 1 Million MasterCard OR Visa transactions a year	Annual Self-Assessment Questionnaire (SAQ) Compliant quarterly network scan by ASV Attestation of Compliance Form
4	Merchants processing fewer than 20,000 Visa or MasterCard eCommerce transactions annually and all other merchants processing up to one million Visa or MasterCard transactions annually. Merchants currently in scope of deadlines are those who process fewer than 1 million Visa eCommerce transactions per year	Level 4 merchants register compliance through our Simple PCI DSS merchant portal https://simplepcidss.eu/services/login/login

There are 12 broad requirements to complying with PCI DSS

Build and maintain a secure computer network

1. Install and maintain a security protection programme (known as a firewall configuration) to protect the card data you may hold
2. Do not use computer passwords that have been provided by external suppliers or businesses. Ensure you issue your own unique passwords and security measures

Protect cardholder data

3. Protect stored data but do not store card and transaction data unnecessarily. Such as:
    - The full card number, The contents of any information within the magnetic strip, The card security code (CVV2), The PIN if you operate an ATM machine.
4. If you are sending out card data or sensitive information by email you must always ensure that you encrypt it. If you are using the postage system, you should ensure it is at least by registered post which requires signed receipt upon delivery.

Maintain an IT vulnerability management program

5. Use and regularly update anti-virus software
6. Develop and maintain secure computer systems and applications

Implement robust control measures / Control access to card data

7. Only access card data when there is a business requirement
8. Assign a unique ID to each member of your staff who has computer access
9. Restrict physical access to the storage area where the cardholder data is kept.

Regularly monitor and test your computer networks

10. Regularly check to see who accesses your computers and cardholder data that you hold.
11. Regularly test your security systems and processes.

Make information security a priority

12. Create and maintain your own security policy to ensure you remain compliant with PCI DSS guidance.

Common objections businesses have about PCI

1

"Why do I have to do this, isn't my terminal secure?"

Having a PCI validated POS solution helps with the annual PCI DSS assessment, however, it does not guarantee PCI DSS compliance. Every business has a responsibility to ensure that the relevant policies, procedures and controls are in place (& practiced) to minimise exposure and reduce the likelihood of a breach.

2

"How often do I have to comply with PCI DSS?"

Annually. This is to ensure businesses are maintaining compliance with the standard, and to identify if anything new has come into scope for the assessment as a result of growth and/or expansion. For example: The introduction of an eCommerce site or the addition of a new premises will affect the risk factors.

3

"I outsource all my cardholder data functions via a third party service provider, do I still need to do this?"

Outsourcing cardholder data functions to a third-party service provider does not exclude a business from PCI DSS compliance. It may reduce the scope and effort involved in the annual assessment, providing the third party is PCI DSS compliant.

4

"What happens if I don't comply with the PCI DSS?"

Not being compliant with the PCI DSS can leave a business at risk of a data breach and related costs. These can be quite substantial and can include: card scheme fines and card replacement costs. Other factors include: reputational damage and loss of customer confidence not to mention businesses being vulnerable to lawsuits and audits.

EVO Payments International GmbH, Branch UK, trading as Card Pay from the AA is licensed by the Federal Financial Supervisory Authority BaFin (Bundesanstalt fur Finanzdienstleistungsaufsicht) in Germany and is regulated by the Financial Conduct Authority (No. 656608).