

MERCHANT GUIDE TO THE PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS)

**The mandatory guide for storing, processing
or transmitting cardholder information.**

CONTENTS

- What is PCI DSS?
- Who needs to become compliant?
- What do I need to do?
- Why has PCI DSS been introduced?
- What are the requirements?
- Getting started
 - Online businesses
- Support for compliance
- Who to contact for more help?
- The benefits to your business

- Appendices
 - A summary of track data
 - Penalties
 - Glossary of terms

What is PCI DSS?

PCI DSS – Payment Card Industry Data Security Standard is a compliance requirement, which aims to ensure that all cardholder information is always stored, processed and transmitted securely.

Who needs to become compliant?

If your business stores, processes or transmits any cardholder data, you must be compliant now. Depending on your level of card processing you should have carried out requirements detailed in this guide.

What do I need to do?

Businesses are divided into four levels depending on the volume and type of transaction you process. See the table below to find out which level your business is, and what you need to do to comply. If you do not undertake this compliance, you could be fined (see appendix 2).

Level	Criteria	Compliance requirement
Level 1	Any merchant processing in excess of 6 million MasterCard OR Visa transactions a year. Any merchant that has lost data due to a security breach, compromise or a “hack”	Annual on-site audit Quarterly vulnerability scan
Level 2	Any merchant processing between 1 and 6 million MasterCard OR Visa transactions a year	Annual Self Assessment Questionnaire Quarterly vulnerability scan
Level 3	Any e-commerce merchant processing between 20,000 and 1 million MasterCard OR Visa transactions a year	Annual Self Assessment Questionnaire Quarterly vulnerability scan
Level 4	Any merchant not level 1, 2 or 3	Annual Self Assessment Questionnaire Vulnerability scan at least annually

Annual on-site audit

A Qualified Security Assessor (QSA) conducts an onsite audit or review of your systems that store, process or transmit cardholder data

Annual Self Assessment Questionnaire

The PCI Self-Assessment Questionnaire (SAQ) is an important validation tool that is primarily used by smaller merchants and service providers to demonstrate compliance to the PCI DSS. <https://www.pcisecuritystandards.org/index.htm> for an example.

Vulnerability scans:

A way to detect weaknesses in computer systems and networks by deliberately trying to compromise data held remotely.

If you are in levels 1-3, we will already be working with you to help you become compliant. Please remember though, your business could grow to move into a higher level, so please retain this guide for future reference.

If your business is currently at level 4, please read through the guide in order to understand what steps you need to take to ensure your business complies with these regulations and what is necessary to protect your customers' card data. From time to time we may ask some level 4 merchants to submit their compliance plans and certifications.

Why has PCI DSS been introduced?

MasterCard and Visa have become increasingly concerned with the level of security protecting businesses' account and transaction information. They needed to ensure that the level of protection a merchant employs is sufficient to deter hackers and criminals. Cardholder data is a tempting target for fraudsters with a series of recent high-profile security breaches worldwide, highlighting the problem.

In January 2005, MasterCard and Visa combined their individual security standards for cardholder data to create a joint program, which is also endorsed by American Express, JCB and Diners (collectively known as the Card Schemes).

PCI DSS requires everyone who stores, processes or transmits card data to comply with 12 requirements, covering both IT security and operational practices.

What are the twelve requirements of 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 all stored data but do not store card and transaction data unnecessarily. This applies to:
 - The full card number
 - The contents of any information within the magnetic strip. Data stored within the magnetic strip is known as track data. For more details on this type of data, please refer to Appendix 1,
 - The card security code on the signature strip (CVV2)
 - The PIN (Personal Identification Number), if you operate an ATM machine.
- 4 If you are sending out card data or sensitive information by email or on disc through the post, you must always ensure that you encrypt it (electronically secure it so it cannot be hacked or read by anyone other than the authorised person) before you send it. If you are using the postal system, you should ensure it is sent at least by recorded delivery which requires signed receipt upon delivery and preferably by a method that can be tracked.

Maintain a vulnerability management programme / Minimise IT vulnerability

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

Implement strong access control measures

- 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.

Getting started with PCI DSS

There are a few simple steps you can take now to begin making sure that your business is compliant:

Read and understand the information on the PCI Security Standards Council website at <https://www.pcisecuritystandards.org/>

Contact an **Approved Scan Vendor** (ASV) to discuss your requirements within the programme. They will be able to answer your questions and provide helpful guidance on how to proceed. Make arrangements with your chosen **ASV** to complete a scheduled vulnerability scans on an ongoing basis as required.

Contact a **Qualified Security Assessor** (QSA) to see if your current system stores, processes or transmits cardholder data. If it does, your business will need to comply with PCI DSS.

Assess your current level of security employed and your processes used by completing a **Self-Assessment Questionnaire (SAQ)** and undertake an initial Vulnerability Scan.

The results will enable you to identify the work that you will need to do to become compliant; this will form your remediation plan.

Once the remediation work has been completed, complete the **SAQ** again.

You do not need to notify us of your progress towards compliance. However from time to time we may contact you to check your PCI DSS standards.

Do you have an online business?

If you use a Payment Service Provider (PSP) to store, process or transmit cardholder data on your behalf, then your PSP is responsible for complying with the PCI DSS. However you still need to complete a self assessment questionnaire (SAQ) to ensure your business is compliant.

If you use a computer programme that enables you to capture the card details on your systems, then your business will need to comply with the PCI DSS standard.

If you have any doubt about what is required for your business, please contact your PSP who will be able to advise you of this and your level of responsibility.

What support is available to help my business comply?

The PCI Security Council has a register of approved third party Qualified Security Assessors (QSAs) that can provide technical advice on the PCI guidelines and confirm that you have achieved PCI DSS compliance.

Full details of the requirements and QSAs can be found on the following web sites:

<https://www.pcisecuritystandards.org>

<https://sdp.mastercard.com/us/sdp/index.html>

<http://www.visaeurope.com/aboutvisa/security/ais/>

MasterCard also has a series of Webinars; internet based training sessions, which can be accessed at <http://www.iian.ibeam.com/events/mast001/24008/>

Who do I contact for additional guidance?

For a full list of independent Approved Scan Vendors visit:

https://www.pcisecuritystandards.org/pdfs/as_report.html

And a full list of independent Qualified Security Assessors (QSA) authorised to conduct the annual on-site audit, by visiting: https://www.pcisecuritystandards.org/resources/qualified_security_assessors.htm

In summary PCI DSS is:

- **Mandatory:**
All merchants who store, process or transmit cardholder data must comply with the standard.
- **Audited:**
Depending on your PCI DSS compliance level you will need to either engage a Qualified Security Assessor (QSA) or complete a Self Assessment Questionnaire, in both instances all merchants need to engage with an Approved Scan Vendor (ASV).
- **Time-limited:**
You must be compliant in accordance with your level within the PCI DSS compliance deadline.
Level 1-3 Merchants have already been notified of their deadlines but Level 4 Merchants have no current deadline.

The benefits to your business of implementing PCI DSS

By following the requirements of the PCI DSS and ensuring compliance, your business can:

- Identify any risks in the way you store or transmit customer data
- Provide a clear path of action and remediation to address any data security risks
- Ensure that your service providers do not put your business at data security risk
- Demonstrate to your customers that you are serious about their data security
- Maintain customer trust, and safeguard the reputation of your brand

Also, by minimising the risk of data compromise, it could:

- Protect against potential financial liabilities (including the full cost of any fraud perpetrated on compromised card accounts)
- Protect against the risk of investigative and legal costs
- Protect against the risk of invasive media attention

Every business which stores or transmits cardholder account data is a potential target.
PCI DSS compliance minimises the data security risk to your business.

Appendix 1: A guide to track data

Visa has instructed us to highlight to our merchants the regulations about 'track data'.

Track data is the information that is held on the magnetic strip and the chip of a credit or debit card. The detail includes the Primary Account Number across the card, expiry data, the security code on the signature strip and service code (used to control your card machine responses).

It can also be called full track, track, track 1, track2, and magnetic stripe data.

Can track data be stored?

Some track data can be stored but it must not be stored in full even if it is protected. If you accept card payments by Mail Order or Telephone Order you may have some of the details written down. Therefore you must have the necessary arrangements to ensure that these written details are securely protected or destroyed once they have been processed.

What track data can be stored in my business?

This table is an extract from the Security Standards Council PCI DSS requirements document and highlights what can and cannot be stored.

	Data Type	Storage Permitted?	Protection Required?
Cardholder Data	Primary Account Number (PAN)	YES	YES
	Cardholder Name	YES	YES
	Expiry Date	YES	YES
	Service Code	YES	YES
Sensitive Authentication Data	Full Magnetic Stripe	NO	N/A
	3 or 4 digit Security Code (CVC2/CVV2/CID)	NO	N/A
	PIN / PIN Block	NO	N/A

PLEASE NOTE:

Sensitive authentication data must not be stored subsequent to authorisation (even if encrypted).

As a minimum the Primary Account Number should be unreadable anywhere it is stored (including data on portable digital media, backup media, in logs, and data received from or stored by wireless networks) You should use some method to protect any data kept, see <https://www.pcisecuritystandards.org/index.htm>) for advice.

How will I know if track data has been stored in my systems?

Some merchants may not be aware that they are storing track data, because it can be done automatically by application software. If you have bought software that stores, processes or transmits card information, you should speak to your supplier to ask where track data may be stored.

Appendix 2: Penalties for PCI DSS Non Compliance – Level 1-3 merchants only

MasterCard and Visa can charge penalties (which are expressed in US Dollars or euro respectively) for non compliance with the PCI DSS regulations. The fines would be in Sterling equivalents based on the relevant exchange rates

Visa expects level 1, 2 or 3 merchants to demonstrate that they are actively engaged in the programme to become compliant. To do this, you need to undertake as a minimum, the following activities:

- Scoped the systems that store, process or handle cardholder data
- Carried out a GAP analysis of these systems against PCI DSS requirements
- Contracted with a QSA or agreed with acquirer to conduct an internal audit
- Contact with Authorised Scanning Vendor (ASV) to conduct a quarterly vulnerability scan
- Contacted a remediation plan to correct issues identified from the GAP analysis.

Further penalties will be applied if you suffer an actual data compromise and are found to be non compliant with PCI DSS.

Penalties for Merchant Data Compromise

The size of the penalty depends on a number of factors including:

- The number of accounts compromised
- Whether the compromised merchant/agent had validated compliance
- Whether the forensic investigation determines there is no evidence of track 2 storage
- Whether the compromise is reported in a timely manner and satisfactorily co-operates with Visa's requirements
- The extent of non compliance with PCI DSS found during the forensic investigation
- Penalties will be waived if the merchant/agent was found to be fully compliant with the PCI DSS at the time of the investigation

Appendix 3: PCI DSS Glossary

ASV – Approved Scan Vendor – a provider approved by the PCI Security Standard Council to carry out a vulnerability scan of your systems. A list is available from <https://www.pcisecuritystandards.org/index.htm>

ATM – Automated Teller Machine is a machine that a cardholder can obtain cash against their card account using their PIN.

Cardholder – Customer to whom a card is issued or individual authorised to use the card

Cardholder data – Information contained in the magnetic strip on back of a card, in the chip, or the information visible on the cards eg:

- account number
- cardholders' name
- expiry date
- security number on signature strip – Card Validation Code

Card Schemes

- Visa
- MasterCard
- American Express
- Diners
- JCB – Japan Credit Bureau

These independent organisations have set up systems for issuing and accepting card payments worldwide, some using local financial institutions as agents.

Card Validation Value or Code (CVV, CVC) – The code on the signature strip, normally 3 digits printed to the right of the card number. For American Express the code is 4 digit unembossed number printed above the card number on the face of all payment cards. The code is uniquely associated with each individual piece of plastic and ties the card account number to the plastic

Compromise – Intrusion into computer systems where unauthorised disclosure, modification or destruction of cardholder data is suspected.

Default passwords – Password set by manufacturer that is freely available. All passwords should be reset and changed often to prevent compromise.

Encryption – A way of converting information into an unintelligible format that allows storage or transmission without compromise.

Firewall – Hardware, software, or both that protects data on one network or computer from intruders from other networks. Typically, an enterprise with an intranet that permits workers access to the wider internet must have a firewall to prevent outsiders from accessing internal private data resources.

Forensic Investigation – Investigation carried out under scientific procedures with or without police involvement. This can involve removal of computer equipment and data storage from your premises.

Magnetic Stripe Data (Track Data) – Data encoded in the magnetic stripe used for authorisation during transactions when the card is presented. If chip and PIN is used to read the card then an equivalent is used by the terminal to authorise and this should not be kept either.

Merchant – Any business that takes card payments for goods and services

Network – A network exists if two or more computers are connected.

PAN – Primary Account Number is the card number that normally runs across the card. It identifies the organisation that issued the card, the Card Scheme and the card.

Password – A mixture of characters that can be used to authenticate a user allowing them access to a system, computer or network.

Payment Service Provider (PSP) – offers merchants online services for accepting electronic payments by a variety of payment methods including cards.

PIN – Personal Identification Number used in Chip and PIN and cash machines to validate the cardholder. This should never be stored or kept during transactions or given or asked of the cardholder.

PIN block – When a card holder enters their PIN, the information is first encoded into a plain text 'PIN block', derived from the PIN length, the PIN digits, and a portion of the PAN (primary account number). The plain text 'PIN block' is then encrypted using a standard algorithm and it is this that is used to verify the card.

QSA – Qualified Security Assessor – The PCI Security Standards Council maintains a list of all persons qualified to assess your systems and processes. For a list see https://www.pcisecuritystandards.org/resources/qualified_security_assessors.htm

SAQ – Self Assessment Questionnaire is a validation tool intended to assist merchants and service providers in self-evaluating their compliance with the Payment Card Industry Data Security Standard (PCI DSS).

Service Code – Messages contained within a card's magnetic strip or Chip that tells a terminal the process to follow when processing a transaction. i.e. a code within a card to instruct the terminal to ask for PIN authorisation.

Track Data – Information about the card and cardholder that is kept in the magnetic strip or Chip

Transaction Data – Information that identifies the purchases a cardholder makes with their card.

Vulnerability Scan – A way to detect weaknesses in computer systems and networks by deliberately trying to compromise data held remotely.

The Royal Bank of Scotland plc, Registered in Scotland No. 90312.
Registered Office: 36 St Andrew Square, Edinburgh EH2 2YB.

