Worldpay’s guide to the Payment Card Industry Data Security Standard (PCI DSS)

What is PCI DSS? | The 12 Requirements | Becoming compliant with SaferPayments | Understanding the jargon

SaferPayments

Be smart. Be compliant. Be protected.

Become compliant
Get started

As a business taking card payments, you’re probably aware of PCI DSS, but do you really know what it is, what it means for your business and how it can benefit your business? So let’s start with the basics.
Being PCI DSS compliant not only gives you peace of mind, but also helps protect your business and customers.

"The Payment Card Industry Data Security Standard (PCI DSS) is a set of standards designed to keep credit and debit card payment data safe and secure. It was created by the five major international card schemes - American Express, JCB, MasterCard, Visa and Discover - to combat the problem of card data theft.

PCI DSS compliance is the minimum level of card data security for any business that accepts credit and debit cards, regardless of size and any organisation which stores, processes and/or sends card data. The 12 requirements of PCI DSS are designed to keep an organisation safe from most types of attack."
Most small and medium size enterprises tend to require PCI DSS level 4 compliance. The different standards are governed by the number of card transactions a business takes on an annual basis.

What is Level 4 compliance?
Less than 20,000 online transactions per year, per card scheme and any business processing up to 1 million in-store or telephone transactions per scheme.
Be smart. Be compliant. Be protected.

• What is PCI DSS?

• What’s your PCI DSS compliance level?

• **Why is it important to become compliant?**

• What are the benefits of becoming PCI DSS compliant?

PCI DSS compliance is mandatory for all businesses accepting card payments. It helps keep your customers’ card information safe and your business secure. That’s why it’s a good idea to become compliant so you can trade reassured that if something does go wrong your business is protected.
Be smart. Be compliant. Be protected.

- What is PCI DSS?
- What’s your PCI DSS compliance level?
- Why is it important to become compliant?
- What are the benefits of becoming PCI DSS compliant?

Peace of mind
You’re protecting your business and customers’ card information

Prevent additional fees
Save money by avoiding the monthly non-compliance fee

Avoid fines
Your business is safeguarded against Card Scheme fines of up to £35,000/€43,000†
The 12 requirements of PCI DSS

The 12 requirements can be grouped into the 6 categories below:

- Build and Maintain a Secure Network
- Protect card holder data
- Maintain a vulnerability management program
- Implement strong access control measures
- Regularly monitor and test networks
- Maintain an information security policy
The 12 requirements of PCI DSS

The 12 requirements can be grouped into the 6 categories below:

• **Build and Maintain a Secure Network**

• Protect card holder data

• Maintain a vulnerability management program

• Implement strong access control measures

• Regularly monitor and test networks

• Maintain an information security policy

---

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.

---

If you choose to process, store or transmit cardholder data via the internet you’ll need to demonstrate that your firewalls and routers are securely configured and independently tested.

A firewall is a fundamental part of network security. A correctly configured firewall will comply with this requirement and you’ll need to verify this through the Security Assessment Questionnaire.

An important part of securing your network, is to make sure all accounts and settings are changed from default and configured to a secure standard.
The 12 requirements of PCI DSS

The 12 requirements can be grouped into the 6 categories below:

- Build and Maintain a Secure Network
- **Protect card holder data**
- Maintain a vulnerability management program
- Implement strong access control measures
- Regularly monitor and test networks
- Maintain an information security policy

3. Protect stored cardholder data.
4. Encrypt transmission of cardholder data across open, public networks.

It's important to protect any cardholder data in a physical or online format. All stored data must be encrypted and sensitive data is never disclosed or stored after authorisation (e.g. PIN numbers and the full card details on the magnetic strip).

You’ll also need to make sure your business is not using public networks to transfer data.

If you are storing, transmitting or processing cardholder data across open public networks (including the internet), you need to ensure you are using the strongest form of encryption to protect it.
The 12 requirements of PCI DSS

The 12 requirements can be grouped into the 6 categories below:

- Build and Maintain a Secure Network
- Protect card holder data
- **Maintain a vulnerability management program**
- Implement strong access control measures
- Regularly monitor and test networks
- Maintain an information security policy

5. Use and regularly update your antivirus software.

6. Develop and maintain secure systems and applications.

Keep your customer’s data and your business’ computer system safe by installing antivirus software.

You’ll need to regularly update this to ensure you’re protected from all online threats. Scans will need to run regularly and software kept up to date and you’ll need to remain vigilant against programs or applications that could cause a threat or vulnerability in the future through testing and maintenance.
The 12 requirements of PCI DSS

The 12 requirements can be grouped into the 6 categories below:

- Build and Maintain a Secure Network
- Protect card holder data
- Maintain a vulnerability management program
- **Implement strong access control measures**
- Regularly monitor and test networks
- Maintain an information security policy

7. Restrict access to cardholder data by business need-to-know.
8. Assign a unique ID to each person with computer access.
9. Restrict physical access to cardholder data.

Make sure you're controlling who can access your customers' card details. You should only allow access to employees who need to know this information.

You can do this by assigning unique IDs with different access permissions to each employee on your computer system.

Make sure to keep any physical records locked away with the keys provided to those who need it. Physical media needs to be monitored and destroyed when no longer needed.
The 12 requirements of PCI DSS

The 12 requirements can be grouped into the 6 categories below:

- Build and Maintain a Secure Network
- Protect card holder data
- Maintain a vulnerability management program
- Implement strong access control measures
- Regularly monitor and test networks
- Maintain an information security policy

10. Track and monitor all access to network resources and cardholder data.

11. Regularly test security systems and processes.

Regularly check your network for vulnerabilities by running internal and external vulnerability scans. You'll also need to track and monitor who is accessing your network and cardholder information so you can identify and act on any unusual activity.
The 12 requirements of PCI DSS

The 12 requirements can be grouped into the 6 categories below:

- Build and Maintain a Secure Network
- Protect card holder data
- Maintain a vulnerability management program
- Implement strong access control measures
- Regularly monitor and test networks
- Maintain an information security policy

12. Maintain a policy that addresses information security.

To make sure your business keeps all cardholder details safe, you need to create and maintain an information security policy. You are required to set a security policy that lets all employees know what is expected of them and that they must follow.
Becoming compliant with SaferPayments

• How can SaferPayments help?

• What are the benefits of SaferPayments?

• How to get started?
Becoming compliant with SaferPayments

• How can SaferPayments help?

• What are the benefits of SaferPayments?

• How to get started?

We know that when you’re running a business, you don’t always have a lot of time on your hands. But along with completing your annual tax return, your building and contents insurance, your PCI DSS compliance is also a necessity. So it should be as quick and simple for you as possible.

Worldpay’s SaferPayments programme is designed to do just that. It makes confirming compliance with the Payment Card Industry Data Security Standard (PCI DSS) quicker and easier and can take as little as 30 minutes to confirm or renew your compliance with the PCI DSS.
Becoming compliant with SaferPayments

- How can SaferPayments help?
- What are the benefits of SaferPayments?
- How to get started?

Saving you valuable time
Becoming certified takes as little as 30 minutes

Online SaferPayments portal
Use our online SaferPayments portal on your computer or smartphone

Dedicated telephone support
Telephone, email and chat support 7 days a week

Vulnerability scanning
Quarterly PCI DSS vulnerability scanning (if required)
Every time you accept card payments, you need to make sure that you are protecting your business and your customer’s card data. We’re all consumers, so we’d be concerned if every time we made a purchase by card, there was a risk your card information could be exposed to potential data theft.

Becoming PCI DSS compliant with Worldpay’s SaferPayments programme minimises that risk and in the unlikely event that something were to happen, your business would be protected and data compromise assessments would be reduced.

Becoming compliant with SaferPayments

• How can SaferPayments help?
• What are the benefits of SaferPayments?
• How to get started?
Get started.
Becoming compliant with SaferPayments

1. Log on to SaferPayments
2. Follow the simple steps to confirm your compliance or if already compliant with another QSA upload your certificate
3. Protect your business

Become compliant
Understanding the jargon

- PCI DSS
- Vulnerability Scan
- Qualified Security Assessor (QSA)
- Attestation
- Self-assessment questionnaires (SAQs)
- Information Security Policy
- Vulnerability Management Program
- Approved Scanning Vendors (ASV)
Understanding the jargon

- PCI DSS
- Vulnerability Scan
- Qualified Security Assessor (QSA)
- Attestation
- Self-assessment questionnaires (SAQs)
- Information Security Policy
- Vulnerability Management Program
- Approved Scanning Vendors (ASV)

The Payment Card Industry Data Security Standard is a set of 12 mandatory requirements for any business accepting card payments. All businesses must become PCI DSS compliant each year to help reduce data compromises and process payments securely.
If you qualify for certain Self-Assessment Questionnaires (SAQs) or you electronically store cardholder data after authorising payments, you will need to complete a Vulnerability Scan. This is an automated tool which scans your systems for vulnerabilities, particularly on your networks and web applications on the external-facing internet protocol (IP) addresses.

You’ll need to do this every 90 days or once per quarter and it must be conducted by a PCI SSC Approved Scanning Vendor (ASV) such as the one provided by SaferPayments. Once you’ve completed the Self-assessment questionnaire, you will be notified if you need to complete a Vulnerability Scan.
A Qualified Security Assessor (QSA) is a person or entity who has been certified by the PCI Security Standards Council to audit merchants for PCI DSS compliance.
Understanding the jargon

- PCI DSS
- Vulnerability Scan
- Qualified Security Assessor (QSA)
- **Attestation**
- Self-assessment questionnaires (SAQs)
- Information Security Policy
- Vulnerability Management Program
- Approved Scanning Vendors (ASV)

As part of the renewal process you’ll need to confirm your compliance, this is also known as attesting.
As part of the PCI DSS process you’ll need to complete a self-assessment questionnaire.

Understanding the jargon

- PCI DSS
- Vulnerability Scan
- Qualified Security Assessor (QSA)
- Attestation

**Self-assessment questionnaires (SAQs)**

- Information Security Policy
- Vulnerability Management Program
- Approved Scanning Vendors (ASV)
Understanding the jargon

- PCI DSS
- Vulnerability Scan
- Qualified Security Assessor (QSA)
- Attestation
- Self-assessment questionnaires (SAQs)
- Information Security Policy
- Vulnerability Management Program
- Approved Scanning Vendors (ASV)

To make sure your business keeps all cardholder details safe, download our Information Security Policy from the SaferPayments portal.
Keep your customers’ data safe by maintaining a Vulnerability Management Program. This includes using and regularly updating antivirus software and ensuring there are secure systems and applications in place.
Approved Scanning Vendors are organisations that can provide a business’ PCI DSS scan.

Understanding the jargon

- PCI DSS
- Vulnerability Scan
- Qualified Security Assessor (QSA)
- Attestation
- Self-assessment questionnaires (SAQs)
- Information Security Policy
- Vulnerability Management Program
- Approved Scanning Vendors (ASV)
† Once you are certified as compliant with the SaferPayments programme, if we are fined by the Card Schemes because you experience a data breach, we will waive our right to pass the first £35,000/€43,000 of fines on to you. To qualify for this waiver, you must meet the conditions below.
- Have answered the online questionnaire honestly and in good faith when self-certifying compliance
- Within 7 working days of discovery of the data compromise advise us in writing of any failure of security within your business or your card acceptance systems
- Retain records, logs and electronic evidence relating to a data compromise and make this available promptly upon request by Worldpay or the Card Schemes
- Co-operate with Worldpay and the involved payment networks in all investigations relating to any data compromise, including allowing forensic investigators, appointed by Worldpay, to carry out investigations and comply with all remedial actions identified by the forensic investigators at your own cost.

^ compared to remaining non-compliant on the SaferPayments fee structure