



Small Business Specialists

PCI DSS - card industry requirements

PCI DSS stands for Payment Card Industry Data Security Standard and was developed by the major card companies to try to prevent credit card details falling into the wrong hands.

In a nutshell it sets out the security standards that merchants must apply in order to comply. This covers physical and electronic security and **companies that do not comply risk losing the right to process credit cards.**

Who does it apply to?

The requirements apply to all organisations that handle and store credit card details in any way - not just those taken over the Internet. Situations where it would apply include using SSL or emails to receive credit card details from your website, taking credit card details over the 'phone, by mail order or in person. In all these cases you will be holding card details on your network, equipment or premises that you will probably either enter into a PDQ machine, or via an online "virtual PDQ".

If you use a PDQ machine or any third-party equipment then that equipment and supplier must also be compliant.

If you use a **Payment Services Provider** gateway exclusively and do not ever come into contact with, or store card details yourself, then the only requirement that will apply is that your PSP must be compliant. If you use one of the major PSPs such as ePDQ from Barclays, Protix, SecureTrading or WorldPay then you should have nothing to worry about.

What happens if it applies?

The exact requirements depend upon the number of credit card transactions you handle each year and will be set for merchants by their "Acquiring Bank", (the bank that provides your company with a Merchant Account). Generally, if you handle less than 20,000 transactions per year then you will be required to:

- ✚ complete an Annual Self Assessment Questionnaire;
- ✚ have a Quarterly Scan by an Approved Scanning Vendor (who may be recommended or required, by your Acquiring Bank);
- ✚ usually it is not required to report compliance but you must achieve and maintain compliance.

In addition, each of the Payment Brands such as Amex, JCB, Mastercard & Visa have their own compliance programmes and your Acquiring Bank may need to take account of this when monitoring their merchants' compliance.

Pitfalls:

Something that has been tripping up some people is the lack of security for their wireless networks and this is an area in which we can help if needed.

We also know some people who have taken the view that they can ignore the requirements because they only handle card data transitorily, e.g. when they get a telephone order they write the details down, enter them into an online secure virtual PDQ terminal which uses encryption and then destroy the written card details after a couple of days. However, it is unlikely that the Acquiring Banks would accept this and they would probably demand full compliance.



Small Business Specialists

What exactly is required?

You are required to do the following:

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

Cardholder Data Protection:

- Protect stored cardholder data
- Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program:

- Use and regularly update anti-virus 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

Next steps:

Sample self assessments can be downloaded from <https://www.pcisecuritystandards.org/saq/>

For more information see <https://www.pcisecuritystandards.org>

Useful information can also be found on the Barclaycard Business site at <http://www.barclaycard.co.uk/pcidss>

For help with compliance please [contact us](#)

We can supply solutions for integrating PSP solutions and our eCommerce solutions can be configured to integrate seamlessly with most major PSPs.

SecureTrading was one of the first gateway PSPs to achieve full PCI DSS compliance. We use Secure Trading and we are a **SecureTrading Partner**, so if you would like to discuss switching to SecureTrading please contact us.