

Understanding PCI-DSS



Payment Card Industry Data Security Standard (PCI-DSS) is the global security standard adopted by the card brands for all organisations that handle, store or transmit payment card information.

The standard grew out of the security requirements that Visa and Mastercard historically promoted individually. Since this issue is seen as non-competitive they, together with American Express and JCB, helped to establish an independent body, the PCI Security Council, to develop, operate and promote the standard.

Initially aimed at internet transactions, PCI-DSS has widened in scope to include all forms of card payment processing, including terminals and paper.

For merchants or card processors the standard includes 12 key requirements:

- 1 Install and maintain a firewall configuration to protect data
- 2 Do not use vendor-supplied defaults for passwords or other security parameters
- 3 Protect stored data
- 4 Encrypt the transmission of cardholder data and sensitive information
- 5 Use and regularly update anti-virus software

- 6 Develop and maintain secure systems and applications
- 7 Restrict access to data by business need-to-know
- 8 Assign a unique ID to each person with computer access
- 9 Restrict physical access to cardholder data
- 10 Track and monitor all access to network resources and cardholder data
- 11 Regularly test security systems and processes
- 12 Maintain a policy that addresses information security

Does PCI-DSS apply to you?

If you have a merchant account and accept card payments, you will need to comply with the standard at some level.

However, the level at which you need to comply with the standard will depend on:

whether you handle the card data in any form yourselves, and the volume of card transactions.

if you only process your own transactions - or - you process transactions on behalf of third parties.

Call
01525 862555

**to find more about
the simple solution to
PCI-DSS compliance**



Approval levels for Merchants (ie: those who only process transactions for themselves)

<p>LEVEL 1</p> <p>Merchants with over 6 million transactions a year, or merchants whose data has previously been compromised.</p> <p>Requires Annual Onsite Security Audit and quarterly network security scan. You will need to engage a QSA (Qualified Security Assessor) to undertake this.</p>	<p>LEVEL 2</p> <p>Merchants with 1,000,000 to 6 million transactions a year.</p> <p>Requires Annual Self Assessment Questionnaire and Quarterly Scan by an Approved Scanning Vendor (ASV)</p>	<p>LEVEL 3</p> <p>Merchants with 20,000 to 1,000,000 transactions a year.</p> <p>Requires Annual Self Assessment Questionnaire and Quarterly Scan by an Approved Scanning Vendor (ASV)</p>	<p>LEVEL 4</p> <p>Merchants with less than 20,000 transactions.</p> <p>Requires Annual Self Assessment Questionnaire and may require Quarterly Scan by an Approved Scanning Vendor (ASV) depending on Acquirer.</p>
---	--	---	--

Approval levels for Processors (ie: those who process transactions for third parties)

<p>LEVEL 1</p> <p>Visa - All VisaNet processors and all payment gateways; MasterCard - All Third Party Processors' (TPP's). All Data Storage Entities (DSE's) that store, transmit, or process greater than 1,000,000 total combined MasterCard and Maestro transactions annually. All compromised TPPs and DSE's.</p> <p>Requires Annual Onsite review by a QSA and Quarterly network scan by an ASV</p>	<p>LEVEL 2</p> <p>Visa - Service Providers (agents) not in Level 1 that store, process, or transmit more than 1 million accounts/transactions annually; MasterCard - All DSE's that store, transmit, or process less than 1 million total combined MasterCard and Maestro transactions annually.</p> <p>Visa requires Annual onsite review by a QSA and Quarterly network scan by an ASV. MasterCard requires Annual self-assessment questionnaire and Quarterly network scan.</p>	<p>LEVEL 3</p> <p>Visa - Service Providers (agents) not in Level 1 that store, process, or transmit less than 1 million accounts/transactions annually.</p> <p>Requires Annual self-assessment questionnaire and Quarterly network scan</p>
--	---	--

What if I don't comply?

The Card Schemes (Visa, Mastercard, American Express, JCB) have provision in their agreements with the Acquirers to impose fines for breaches and non-compliance. As a result, your Acquirer probably has scope within their agreement with you as a merchant, to impose similar fines or costs.

Ultimately, your Acquirer could withdraw your merchant account, meaning you would be unable to process card transactions.

Is there a simpler solution

Yes - by far the easiest way to ensure full compliance is to put your card handling "out of scope" completely, removing any actual card data handling from your own systems.

This means transferring your card handling to a trusted organisation, such as RSM2000, who already have the secure systems, policies and infrastructure in place, and are fully accredited by the PCI Security Council as a Level 1 Payment Service Provider (PSP).

Call
01525 862555

**to find more about
the simple solution to
PCI-DSS compliance**

