

**C·O·M·O·D·O**  
Creating Trust Online™

# PCI Security Compliance – The Facts

What PCI security means for your business

Comodo HackerGuardian

# PCI Security Compliance – The Facts

## Overview

The Payment Card Industry Data Security Standard (PCI DSS) is a set of 12 requirements intended to prevent consumer data theft and online fraud and was jointly developed by American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. The PCI DSS is now actively maintained by the PCI Security Standards Council, and represents a multifaceted standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures.

Compliance with the standard is mandatory for any organization that stores, transmits or processes credit card transactions. This also means that all merchants, service providers and payment card network members must be compliant if they wish to continue accepting credit card payments. Penalties for non-compliance can be substantial and include increased processing fees, fines of more than \$500,000 and suspension of the ability to process transactions.

The regulations, aimed at establishing secure practices for handling card holder data, consist of 12 requirements organized into 6 categories - known as 'Control Objectives':

<b>Build and Maintain a Secure Network</b>
<b>1. Install and Maintain a firewall configuration to protect cardholder data</b>
<b>2. Do not use vendor-supplied defaults for system passwords and other security parameters</b>
<b>Protect Card Holder Data</b>
<b>3. Protect stored cardholder data</b>
<b>4. Encrypt transmission of cardholder data across open public networks</b>
<b>Maintain a Vulnerability Management Program</b>
<b>5. Use and regularly update anti-virus software or programs</b>
<b>6. Develop and maintain secure systems and applications</b>
<b>Implement Strong Access Control Measures</b>
<b>7. Restrict access to cardholder data by business need-to-know</b>
<b>8. Assign a unique ID to each person with computer access</b>
<b>9. Restrict physical access to cardholder data</b>
<b>Regularly Monitor and Test Networks</b>
<b>10. Track and monitor all access to network resources and cardholder data</b>
<b>11. Regularly test security systems and processes</b>
<b>Maintain an Information Security Policy</b>
<b>12. Maintain a policy that addresses information security for employees and contractors</b>

*Fig. 1: PCI DSS Control Objectives and Requirements*

## What do I have to do to become compliant?

Any merchant or service provider that accepts card payments or processes card data must be compliant with all 12 requirements as stated above. However, the *validation* requirements demanded of a particular merchant are dependent upon its annual transactional volume.

	Merchant Levels	Qualification Criteria *	Annual On-Site Audit	Annual Self-Assessment Questionnaire	Quarterly External Network Scans
<b>MERCHANT</b>	1	Merchants with over <b>6 million</b> credit card transactions per year	✓		✓
	2	Merchants with between <b>1 million and 6 million</b> credit card transactions per year		✓	✓
	3	Merchants with between <b>20,000 and 1 million</b> credit card transactions per year		✓	✓
	4	Merchants with <b>less than 20,000</b> credit card transactions per year		✓	✓ **
<b>SERVICE PROVIDER</b>	1	All processors and all payment gateways	✓		✓
	2	Any service provider that is not in Level 1 and stores, processes or transmits more than 1 million accounts/transactions annually	✓		✓
	3	Any service provider that is not in Level 1 and stores, processes or transmits less than 1 million accounts/transactions annually		✓	✓

**Fig. 2: PCI Compliance Validation Requirements by transaction level**

\* Any merchant that has suffered a hack resulting in a compromise of account data may be escalated to a higher validation level.

\*\* PCI requires that all merchants perform external network scanning to achieve compliance. Merchant Level 4 validation requirements and dates are determined by the merchant's acquirer; acquirers may require submission of scan reports and/or questionnaires.

### Definition of Terms

#### Annual On-Site Audit

Level 1 merchants and any organization with a previous security breach must undergo an on-site compliance audit by a PCI approved Qualified Security Assessor (QSA)

#### Annual Self Assessment Questionnaire

Level 2, 3 and 4 merchants must complete an annual self-assessment questionnaire (SAQ) documenting and asserting their compliance with the PCI Data Security Standard

#### Quarterly Network Scans by a PCI Approved

All merchants, regardless of transactional volume **MUST** have quarterly network scans on externally facing IP addresses performed by a PCI Approved Scanning Vendor

### Scanning Vendor (ASV)

(ASV) to be PCI compliant. The scans will test the merchant network for vulnerabilities and provide the merchant with a detailed report of any security holes according to their severity level. To pass the scan criteria, all vulnerabilities with a CVSS severity rating of 4.0 or over must be remediated by the merchant. Comodo is a qualified ASV and provides the required quarterly scans as well as the necessary scan compliance report.

Although the requirements are set by the PCI Security Standards Council, it is the responsibility of the financial institution that provides the merchant services to enforce them. Therefore, both the report confirming a merchant has passed the **Quarterly Network Scan** and the **Annual Self Assessment Questionnaire** need to be submitted to your merchant bank. Your merchant bank will then report back to the Payment Card Industry that your company is PCI Compliant.

## What steps do I need to take to become compliant?

1. Complete the **Self-Assessment Questionnaire (SAQ)** according to the information contained in the Self- Assessment Questionnaire Guidelines. (use our free wizard at [http://www.hackerguardian.com/hackerguardian/ga\\_sa.html](http://www.hackerguardian.com/hackerguardian/ga_sa.html) )
2. Complete a **clean vulnerability scan** with a PCI DSS Approved Scanning Vendor (ASV), and obtain evidence of a passing scan from the ASV. (Comodo is an approved scanning vendor and offers a range of PCI scan compliancy packages to suit merchants and service providers of all sizes)
3. Complete the relevant **Attestation of Compliance** in its entirety (located in the SAQ).
4. Submit the SAQ and the accompanying Attestation of Compliance along with evidence of a passed vulnerability scan and any other requested documentation, to your acquiring bank.

## Comodo HackerGuardian PCI Services

Comodo is a PCI Approved Scanning Vendor (ASV). Through its range of HackerGuardian products, we provide everything a merchant needs to ensure compliancy with the PCI guidelines.

**HackerGuardian PCI Scan Compliancy Service** - The PCI Scan Compliancy Service allows users to run fully customizable, on-demand security audits of corporate networks using the full complement of HackerGuardian plug-ins (over 21,000 individual vulnerability tests with more added daily).



[Prove the legitimacy of your card logos](#)

After each scan, you are supplied with a report which identifies any security vulnerabilities alongside solutions and risk mitigation advice. If you successfully pass the PCI scan criteria (no vulnerabilities CVSS severity rating 4.0 or above), you will also be provided with a 'PCI Compliance Report' that can be sent to your acquiring bank as an assertion of compliance.

**Fig. 3: Payment Credential CVC logo**

Accessed through a secure online interface, the service is highly configurable and features a free Payment Credential CVC site-seal – giving website visitors instant verification that you are authorized to accept card payments.

- HackerGuardian PCI Scan Compliancy Service enables merchants and service providers to run 10 PCI scans per quarter on up to 5 IP addresses. \$79 per year.

- HackerGuardian PCI Scan Compliancy Service Enterprise is a more powerful and flexible service which provides for up to 100 scans per quarter on 20 IP addresses. \$129 per year.
- Additional IP packs can be added to any license to enable PCI compliant scanning on additional IP addresses.

**HackerGuardian Free PCI Scan** - Allows merchants of all sizes to conduct 3 on-demand network scans on a single internet connected device. Merchants can use as many of the scans as necessary to achieve the PCI standard. *(Note: The PCI Data Security Standard requires quarterly scans. This free service will provide certification to demonstrate first quarter compliance only. Merchants wishing to gain certification for a full 12 month period should consider the full HackerGuardian PCI Compliancy Service.)*

**HackerGuardian Free PCI Compliance Wizard** - The HackerGuardian PCI Compliance Wizard is an intuitive web-based application that guides merchants through every step of the PCI Self Assessment Questionnaire (SAQ).

- Preliminary questions will help you to determine which 'validation type' your company fits into and therefore of the 4 self assessments questionnaires you need to complete.
- Each of the questions is accompanied by expert help, information and advice that will help you to both interpret the question correctly and provide the appropriate answer
- Once the wizard is complete, you will receive:
  - A questionnaire summary detailing any control areas on which you failed compliance
  - A custom 'Remediation Plan' for your company containing a list of remedial actions that you need to take alongside links to recommended products and services that will help you resolve non-compliant areas.
  - A 'ready – to – submit' PCI DSS Self Assessment Questionnaire which will include your completed 'Attestation of Compliance'

Visit [www.hackerguardian.com](http://www.hackerguardian.com) to find out more about how HackerGuardian can help **your** company achieve PCI compliance

# About Comodo

Comodo is a leading global provider of Identity and Trust Assurance services on the Internet, with over 200,000 customers worldwide. Headquartered in Jersey City, NJ with global offices in the UK, Ukraine and India, the company offers businesses and consumers the intelligent security, authentication and assurance services necessary to ensure trust in online transactions.

As a leading Certification Authority, and in combination with the Digital Trust Lab (DTL), Comodo helps enterprises address digital ecommerce and infrastructure needs with reliable, third generation solutions that improve customer relationships, enhance customer trust and create efficiencies across digital ecommerce operations. Comodo's solutions include SSL certificates, integrated Web hosting management solutions, web content authentication, infrastructure services, digital e-commerce services, digital certification, identity assurance, customer privacy and vulnerability management solutions.

For additional information on Comodo – Creating Trust Online™ please visit [www.comodo.com](http://www.comodo.com)

## **Comodo**

US Headquarters,  
525 Washington Blvd.,  
Jersey City, NJ 07310  
Tel : +1.888.COMODO.1  
email : [sales@comodo.com](mailto:sales@comodo.com)

## **Comodo Group Inc.,**

3rd Floor, Office Village,  
Exchange Quay, Trafford Road,  
Salford, Manchester M5 3EQ,  
United Kingdom.  
Tel Sales: +44 (0) 161 874 7070  
Fax Sales: +44 (0) 161 877 7025

[www.comodo.com](http://www.comodo.com)