Comodo HackerGuardian™

PCI Security Compliance **The Facts**

What PCI security means for your business

COMODO
Creating Trust Online®

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':

Build and Maintain a Secure Network	1. Install and Maintain a firewall configuration to protect card-holder data
	2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Card Holder Data	3. IProtect stored cardholder data
	4. Encrypt transmission of cardholder data across open public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs
	6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	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
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data
	11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for employees and contractors

Fig. 1: PCI DSS Control Objectives and Requirements

sales@comodo.com 1 (888) 266 6361

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
MERCHANT	1	Merchants with over 6 million credit card transactions per year	✓		✓
	2	Merchants with between 1 million and 6 million credit card transactions per year		✓	✓
	3	Merchants with between 20,000 and 1 million credit card transactions per year		✓	✓
	4	Merchants with less than 20,000 credit card transactions per year		✓	✓
SERVICE PROVIDER	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. 1: PCI DSS Control Objectives and Requirements

* 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 as serting their compliance with the PCI Data Security Standard

Quarterly Network Scans by a PCI Approved Scanning Vendor (ASV) — All merchants, regardless of transactional volume MUST have quarterly network scans on externally facing IP addresses perfor med by a PCI Approved Scanning Vendor (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.

sales@comodo.com 1 (888) 266 6361

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/qa_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).

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.

- HackerGuardian PCI Scan Compliancy Service enables merchants and service providers to run 10 PCI scans per quarter on up to 5 IP addresses. $249 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. $399 per year.
- Additional IP packs can be added to any license to enable **PCI compliant** scanning on additional IP addresses.

sales@comodo.com 1 (888) 266 6361

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 webbased 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** to find out more about how HackerGuardian can help your company achieve PCI compliance

sales@comodo.com 1 (888) 266 6361

About Comodo

The Comodo companies provide the infrastructure that is essential in enabling e-merchants, other Internetconnected companies, software companies, and individual consumers to interact and conduct business via the Internet safely and securely. The Comodo companies offer SSL certificates and SSL management solutions, Code Signing certificates, Email Certificates, award winning PC security software, Endpoint Security Management, Malware scanning for websites and Vulnerability Scanning for PCI Compliance.

Continual innovation, a core competence in PKI, and a commitment to reversing the growth of Internet-crime distinguish the Comodo companies asvital players in the Internet's ongoing development. Comodo secures and authenticates online transactions and communications for over 200,000 business customers and 10,000,000 users of our desktop security products.

www.instantssl.com

Comodo CA Limited
3rd Floor, 26 Office Village,
Exchange Quay,
Trafford Road, Salford,
Manchester M5 3EQ,
United Kingdom
Tel: +44 (0) 161 874 7070
Fax: +44 (0) 161 877 7025

Comodo Group, Inc.
1255 Broad Street
Clifton, NJ 07013
United States

Tel: +1.(888).266.6361
Email: Sales@Comodo.com