

## MEETING PCI COMPLIANCE WITH SONICWALL GLOBAL MANAGEMENT SYSTEM

*PCI DSS 1.1 compliance requirements demand a new level of administration and oversight for merchants, banks and service providers to maintain a high standard for security, reliability and consistent policy control.*

### CONTENTS

The Staggering Impact of Identity Theft	2
PCI DDS: Payment Card Industry Data Security Standards	2
Understanding PCI Requirements: the “Digital Dozen”	4
Weighing the Costs and Benefits of PCI	5
How Your Organization Must Comply with PCI	6
Failings and Challenges: a PCI Audit “Top Ten List”	7
How SonicWALL Helps Meet PCI Compliance Requirements	7
SonicWALL GMS: A Solid Foundation to PCI Compliance	8
Summary	11

## Abstract

Ensuring Payment Card Industry (PCI) compliance requires expert understanding of data storage and encryption requirements, device integration considerations, and logging and reporting parameters for distributed networks. The award-winning SonicWALL Global Management System (GMS) helps organizations meet the stringent PCI requirements by offering centralized management of security rules and policies across a distributed environment, real-time monitoring and logging services, and historical compliance reporting for deployments of all sizes.

## The Staggering Impact of Identity Theft

Theft of identity information has outpaced traditional robbery to become a multibillion-dollar phenomenon, widely perpetrated by professional criminals. According to the Federal Trade Commission's (FTC) Identify Theft Survey Report, the annual total loss to organizations and individual victims for all types of reported identity theft, including both new account and existing account fraud, runs upwards of \$53 billion annually.

This same study revealed that one in four U.S. households has been a victim of identity theft in the past five years. In a survey of 4,000 adults, approximately 10 million American consumers discovered that their personal information had been used to open fraudulent bank, credit card or utility accounts, or used to commit other crimes. Americans also spent almost 300 million hours resolving issues related to identity theft. Between individual and business identity theft victims, an average of 30-60 hours per victim was spent on handling various matters related to identity theft including new accounts, existing account and other frauds. Overall out-of-pocket expense to identity theft victims was estimated at \$5 billion.

More than 50 percent of the individuals that experienced identity theft were the victims of credit card and other types of account fraud. New account fraud (where an identity thief opens up new accounts in a victim's name) and other frauds were estimated to have victimized 3.23 million people. Approximately 28 percent of identity theft victims involved the misuse of an existing credit card said that their credit cards had either been lost or stolen.

In 2006, identity theft cost businesses and financial institutions nearly \$48 billion. Security breaches of identity information data have been widely reported even among widely known and respected organizations. That same year, more than 26 million identity records were stolen from the U.S. Department of Veteran's Affairs. But these are only glaring examples of an epidemic data security problem. No organization can afford to ignore the threat any longer.

Yet many of these cases could have been mitigated or prevented altogether had the proper processes, network management system, and technologies been in place.

## PCI DSS: Payment Card Industry Data Security Standards

The Payment Card Industry Data Security Standard (PCI DSS) grew from the earlier Visa Cardholder Information Security Program (CISP) initiative in 2001. The intent of PCI DSS (commonly referred to simply as PCI) was to create an open security standard that was achievable by all merchants for the protection of cardholder data. Developed by the four major companies in the payment card industry, namely Discover, American Express, Visa and MasterCard, PCI was created to give customers the added security of knowing that their information was safe once it was given to a business. Any credit card transaction that deals with a Primary Account Number (PAN) for a card holder must abide by the PCI standard, which safeguards

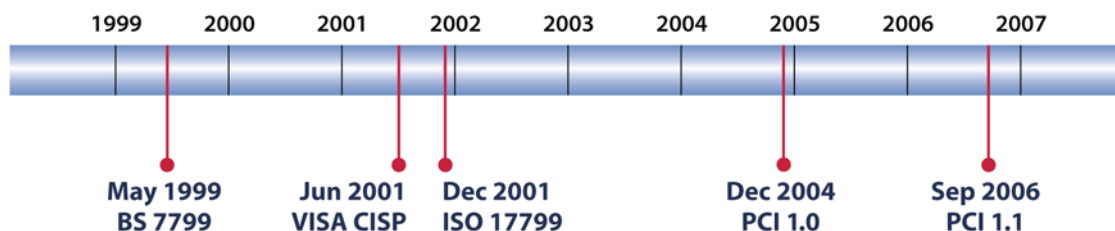
information that is stored, processed and transmitted. All merchants who accept credit cards need to be PCI compliant or risk account suspension, fines or even termination.

The founding principles contained within PCI are the most comprehensively prescriptive data security standards in existence. All incumbent standards, such as SOX, HIPAA and GLBA pale in comparison to the number of security control requirements identified in the PCI DSS 1.1 standard. The principles of the PCI DSS standard are based upon the International Standards Organization (ISO) 17799, the internationally recognized standard for information security practices. Prior to the ISO 17799 standard, the British Standard set the bar for security best practices. These comprehensive guidelines encompass many specific areas including:

- Security policy
- Organization of assets and resources
- Asset classification and control
- Personnel and physical security
- Communications and operations management
- Access control
- Systems development and maintenance
- Business continuity management
- Compliance

PCI was formed to provide a consistent set of standards across systems. It is important to note that the PCI standard is still separate from being certified by each of the credit card companies. The companies have come together to support the auditing criteria found within the standard, but certification and accreditation is still done by each respective credit card company. The PCI DSS are requirements mandated by the card issuers for handling of credit card information, classification of merchants and validation of merchant compliance. Merchants and third-party service providers are responsible for the security of cardholder data and can not store certain types of data on their systems or the systems of their third-party service providers. Merchants and service providers are also responsible for any damages or liability that may occur as a result of a data security breach or non-compliance with PCI DSS.

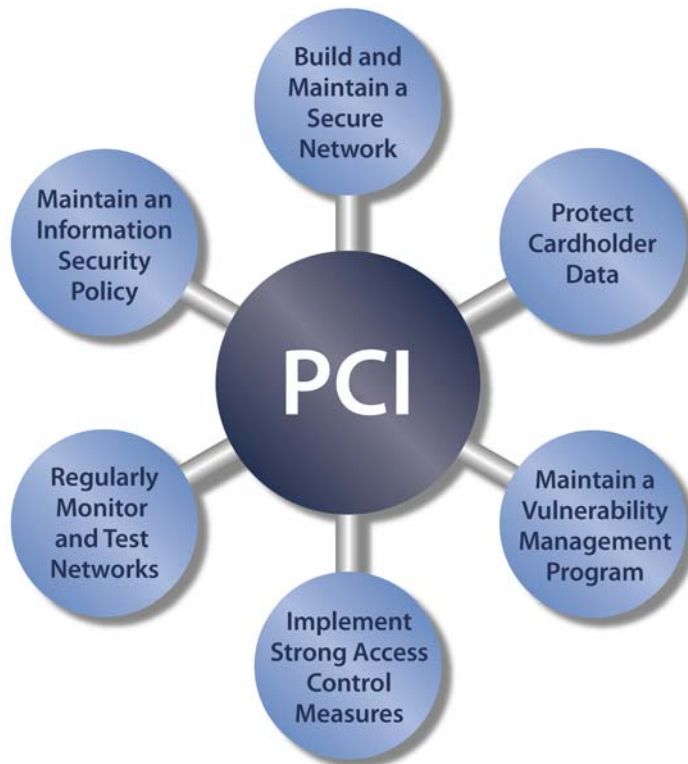
## Development of Security Standards



## Understanding PCI Requirements: the “Digital Dozen”

PCI standards are based upon six fundamental principles:

- Build and maintain a secure network
- Protect cardholder data
- Maintain a vulnerability management program
- Implement strong access control measures
- Regularly monitor and test networks
- Maintain an information security policy



These principles are further broken down into twelve requirements (commonly referred to as “The Digital Dozen”):

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
3. Protect stored data and do not store card and transaction data unnecessarily
4. Encrypt transmission of cardholder data and sensitive information across public networks
5. Use and regularly maintain secure systems and applications
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. Establish and maintain high level security principles and procedures

At a high level, the PCI standard is designed to be relatively intuitive to follow. These standard principles and mandated requirements offer an overall guideline for security best practices that should be applied not only to your credit card information, but as part of your organization’s entire business data security program.

## Weighing the Costs and Benefits of PCI

If cardholder data managed by a merchant or third-party is compromised, the responsible party may be subject to the following liabilities and fines associated with non-compliance:

- Potential fines of up to \$500,000 (at the discretion of Visa, MasterCard or other card companies)
- All fraud losses incurred from the use of the compromised account numbers from the date of compromise forward
- Cost of re-issuing cards associated with the compromise
- Cost of any additional fraud prevention/detection activities required by the card associations (i.e., a forensic audit) or costs incurred by credit card issuers associated with the compromise (i.e., additional monitoring of system for fraudulent activity)

Complying with PCI makes good business sense since it can result in a more reliable, streamlined IT infrastructure, improved service delivery, increased availability and reduction in risk. These results ultimately lead to improved customer confidence and loyalty, simplified auditing and more effective cost controls.

Furthermore, insurance costs are increased for a variety of security, privacy and service-oriented policies, as is the occurrence of civil suits filed against merchants or service providers who are negligent and do not follow the PCI mandates.

## How Your Organization Must Comply with PCI

- Any organization that handles credit cardholder information should comply with PCI. These include:
- E-commerce sites
- Brick and mortar companies taking credit card transactions via mail order or telephone order (MOTO) or point of sale (POS) systems
- Service Providers handling customers' transactions
- Transaction Processing Partners (TPP)
- Data Storage Entities (DSE), such as E-vault or Live Vault
- Member Organizations: Organizations like Visa and MasterCard that operate and manage payment industry infrastructure on behalf of banks and financial institutions

Identity theft has become a serious topic, and credit card data is one of the primary targets for identity theft. PCI was designed to provide the baseline requirements for how vendors should protect cardholder data to ensure it is not stolen or compromised. In order to understand which parties must comply with PCI, we first must look at the holistic view of a simple credit card transaction. Each participant is termed as a member. Classifications for participants are as follows:

- **Issuers:** Member banks and financial institutions who issue credit cards to individuals or corporations.
- **Acquirers:** Member banks and financial institutions who acquire and manage merchants accepting cardholder payments / transactions
- **Service Providers:** Entities that provide any service requiring the processing, storage or transmission of card information/transaction information on behalf of member organizations, acquirers or issuers.

PCI responsibilities have been split between various card associations. VISA is responsible for registering and qualifying professional firms capable of doing PCI assessments; qualifying, training and certifying individuals within those firms, and ensuring firm/individual's continuous ability to audit PCI requirements. MasterCard is responsible for registering, and qualifying companies capable of meeting PCI scanning requirements. While compliance with the PCI standard has remained low, high-profile security breaches have reinforced the need for implementing stronger controls when handling credit card data.

Depending upon an organization's transaction volume, payment channels and potential exposure, PCI classifies merchants into four levels of required compliance:

- **Level 1:** These are merchants processing over 6 million transactions per year or compromised in the past year, regardless of acceptance channel. To comply with PCI, Level 1 merchants are required to conduct annual onsite review by a Qualified Data Security Company (CDSC) or internal audit; as well as quarterly network scans by a qualified independent scan vendor.
- **Level 2:** These are merchants processing 1-6 million transactions per year, regardless of acceptance channel. To comply with PCI, Level 2 merchants are required to conduct annual self-validated assessment questionnaires, as well as quarterly network scans by a qualified independent scan vendor.
- **Level 3:** These are merchants processing 20,000 to 1 million transactions per year. To comply with PCI, Level 3 merchants are also required to conduct annual self-assessment questionnaires, as well as quarterly network scans by a qualified independent scan vendor.

- **Level 4:** These are merchants processing under 20,000 e-commerce transactions per year, and all other merchants processing up to 1 million transactions per year. To comply with PCI, Level 4 merchants are also required to conduct annual self-assessments and an annual network scan.

Additionally, PCI sets four levels for service providers:

- **Level 1:** These are service providers including all VisaNet processors (member and non-member), and all payment gateways. To comply with PCI, Level 1 service providers are required to conduct annual onsite review by a Qualified Data Security Company (CDSC) or internal audit; as well as quarterly network scans by a qualified independent scan vendor.
- **Level 2:** These are service providers not in Level 1 that store, process or transmit over 1 million Visa accounts/transactions per year. To comply with PCI, Level 2 service providers are required to conduct annual self-assessment questionnaires, as well as quarterly network scans by a qualified independent scan vendor.

## Failings and Challenges: a PCI Audit “Top Ten List”

To date, the top cited reasons for failed PCI audits, along with top challenges for organizations attempting to pass a PCI audit, include the following:

1. Storage of prohibited data CVV2, PIN, etc.
2. Un-patched systems
3. Vendor default settings and passwords
4. Poorly coded Web-facing applications (e.g., susceptibility to SQL injections)
5. Unnecessary and/or vulnerable services and servers
6. Weak encryption and unprotected user access
7. Poorly managed track data
8. Poorly monitored change management
9. Inadequate audit and enforcement of policy and password rules
10. Inadequate lock-down of mobile and wireless systems

## How SonicWALL Helps Meet PCI Compliance Requirements

SonicWALL employed the services of an independent VISA-approved PCI Qualified Security Assessor (QSA) to review SonicWALL GMS, and SonicOS Standard and Enhanced firmware, including TZ, PRO, and NSA network security platforms. This review initiative provides assurance that SonicWALL solutions can satisfy PCI criteria when configured and implemented in accordance with the DSS standard.

In an effort to facilitate any PCI compliance project and shorten the deployment cycle, a three-volume PCI Implementation Guide is available from SonicWALL, which addresses the most common installation and configuration settings on SonicWALL GMS and SonicOS Standard/Enhanced firmware. These configurations are backed and approved by an independent PCI auditor.

## SonicWALL and PCI

<b>Build and Maintain a Secure Network</b>	
Requirement 1	Install and maintain a firewall configuration to protect cardholder data
Requirement 2	Do not use vendor-supplied defaults for system passwords and other security parameters
<b>Protect Cardholder Data</b>	
Requirement 3	Protect stored data and do not store card and transaction data unnecessarily <sup>1</sup>
Requirement 4	Encrypt transmission of cardholder data and sensitive information across public networks <sup>2</sup>
<b>Maintain a Vulnerability Management Program</b>	
Requirement 5	Use and regularly update antivirus software
Requirement 6	Develop and maintain secure systems and applications
<b>Implement Strong Access Control Measures</b>	
Requirement 7	Restrict access to data by business need-to-know
Requirement 8	Assign unique ID to each person with computer access
Requirement 9	Restrict physical access to cardholder data <sup>1</sup>
<b>Regularly Monitor and Test Networks</b>	
Requirement 10	Track and monitor all access to network resources and cardholder data
Requirement 11	Regularly test security systems and processes
<b>Maintain an Information Security Policy</b>	
Requirement 12	Establish and maintain high level security principles and procedures

■ Supported by SonicWALL solutions

<sup>1</sup> Applies to CDP installations that have either an onsite appliance or offsite backup services where the Primary Account Numbers (PAN) are stored.

<sup>2</sup> Primarily a configuration issue for using strong ciphers and security protocols, which are supported by SonicWALL.

## SonicWALL GMS: A Solid Foundation for PCI Compliance

The award-winning SonicWALL GMS helps to manage PCI compliance by offering centralized management of security rules across a distributed environment, redundancy and load balancing, as well as policy and compliance reporting for deployments of all sizes. GMS provides a comprehensive foundation for PCI compliance by centrally creating and managing security policies, providing real-time monitoring and alerts and delivering intuitive compliance and usage reports, all from a single management interface.

SonicWALL has invested in engineering key enhancements to GMS to complement the latest PCI 1.1 standard. With the latest version of GMS, enterprises and solutions providers can securely expand their centralized management and reporting services to include support for SonicWALL Network Security Appliances (NSA), SSL VPN and Continuous Data Protection (CDP) product lines. With the GMS unified management interface, small business with as few as 10 SonicWALL appliances or an MSP with thousands can configure, push tasks and report on their appliances, requiring fewer man-hours to meet PCI compliance. Regardless of the compliance initiative or criteria, the GMS core architecture resides on a platform that delivers:

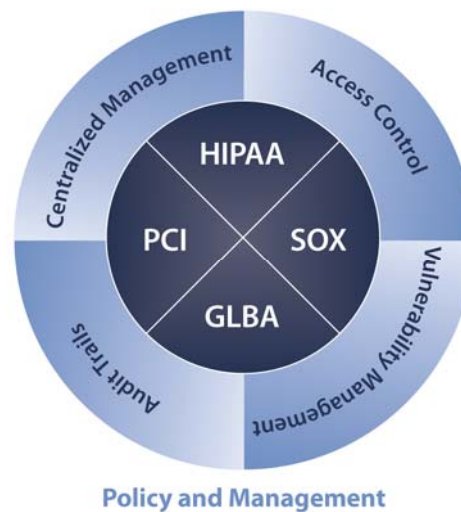
- Centralized management
- Strong access control
- Comprehensive audit trails
- Dynamic vulnerability management

GMS is highly effective in enabling organizations to monitor, enforce and comply with a range of PCI requirements in order to pass PCI audits. When it comes to secure network management and policy enforcement, we can find many common criteria across familiar regulatory initiatives such as SOX, HIPAA, GLBA and PCI. At the root of these criteria is the ability for the security infrastructure to provide a secure transport layer, strong access control, and comprehensive tracking and monitoring of all activity traversing across network resources.

## **GMS Delivers Secure Compliance Enforcement**

### **GMS Delivers Policy and Management Enforcement Through:**

- Centralized Management (Encrypted and Authenticated)
- Strong Access Control (Read, Write, etc.)
- Comprehensive Audit Trails (Monitoring, Reporting, Logging)
- Dynamic Vulnerability Management (UTM Subscriptions)



Some examples of PCI compliance in which GMS can be particularly applicable include:

- **Admin password** - After a fresh install, GMS requires the administrator to change the password for the admin account at the time of the first login
- **User passwords** – A checkbox labeled “Change Password” is displayed on all group screens, including End Users, Operators and Administrators, requiring users to change the password at first login
- **Temporary accounts** – GMS can display a calendar for the administrator to select a date after which a temporary account will expire, available on all group and individual account screens
- **Inactive accounts** – GMS provides two objects in the management interface to support the ability to delete inactive accounts automatically
- **User access restricted by time of day** – GMS can let administrators limit user access to certain times of the day, and certain days of the week
- **90 day password rotation** – GMS provides a mechanism to force users to change their password every 90 days, or at a configured interval
- **Password length and characters** – GMS validates that all passwords are a minimum of seven characters in length, and contain both alphabetic and numeric characters
- **New password rule enforcement** – GMS enforces a rule that all new passwords must be different from each of the previous four passwords
- **Lockout repeated failed login attempts** – GMS can lock out an account for a default of 30 minutes after six or fewer failed login attempts

These features provide a means to safeguard against inappropriate configurations, oversights in account management privileges, encryption of database entries and enforcement of strong ciphers for remote systems. All of these features can be defined by the administrator allowing for greater customization. Furthermore, SonicWALL has taken a proactive step by working with the PCI constituents in evolving our security platforms to address the enhancements made to this standard.

GMS provides robust reporting functionality, including:

- Web usage summary reports, which contain information on the amount of HTTP bandwidth handled by your SonicWALL device during each hour of the specified day
- Bandwidth summary reports, which display the amount of data transferred through one more selected SonicWALL appliances
- Intrusion prevention reports, which list the number of attempted intrusions that occurred during the specified time period
- Top virus attack reports, which show the number of virus attacks that were directed at or through the selected SonicWALL appliance
- Attack summary reports, which show the number of attacks that were directed at or through the selected SonicWALL appliance

Automating the process of reporting is one of the largest challenges for any regulatory mandates. Many companies are manually handling control management and report generation for monitoring, auditing and reporting, but automation is the key towards achieving and maintaining a comprehensive compliance.

## Summary

PCI DSS is the industry response to an epidemic problem that must be addressed by all businesses, regardless of regulatory mandates. The PCI standard represents security best practices that should be applied to all data and networking environments—not only retailers, merchants and service providers handling credit card information. Compliance provides business benefits far beyond the avoidance of fines.

SonicWALL GMS provides a solid foundation for meeting PCI compliance and passing PCI audits. GMS delivers centralized security and network management using a single console to deploy, manage and monitor a distributed networked environment and policies from any location. Administrators can define, distribute, enforce and deploy service and security policies ranging from a single site to thousands of distributed SonicWALL appliances. Sophisticated VPN deployment and configuration enables distributed enterprise networks to reduce the administration time, costs and complexity associated with regulating corporate security policies, VPN connectivity and network configurations. For service providers, GMS allows for customized security policies across thousands of managed customers.

SonicWALL GMS and SonicWALL appliances running SonicOS Standard/Enhanced firmware are backed and approved by an independent PCI Qualified Security Assessor (QSA), ensuring their capacity to serve as technological control components in any network striving to achieve PCI compliance.