Payment Card Industry (PCI)
Data Security Standard

Requirements and Security Assessment Procedures

Version 1.2

October 2008

Table of Contents

Introduction and PCI Data Security Standard Overview

The Payment Card Industry (PCI) Data Security Standard (DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. This document, *PCI Data Security Standard Requirements and Security Assessment Procedures,* uses as its foundation the 12 PCI DSS requirements, and combines them with corresponding testing procedures into a security assessment tool. It is designed for use by assessors conducting onsite reviews for merchants and service providers who must validate compliance with the PCI DSS. Below is a high-level overview of the 12 PCI DSS requirements. The next several pages provide background about preparing for, conducting, and reporting a PCI DSS assessment, whereas the detailed PCI DSS requirements begin on page 13.

PCI Data Security Standard – High-Level Overview

Build and Maintain a Secure Network	
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
Protect Cardholder Data	
Requirement 3:	Protect stored cardholder data
Requirement 4:	Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	
Requirement 5:	Use and regularly update anti-virus software
Requirement 6:	Develop and maintain secure systems and applications
Implement Strong Access Control Measures	
Requirement 7:	Restrict access to cardholder data by business need-to-know
Requirement 8:	Assign a unique ID to each person with computer access
Requirement 9:	Restrict physical access to cardholder data
Regularly Monitor and Test Networks	
Requirement 10:	Track and monitor all access to network resources and cardholder data
Requirement 11:	Regularly test security systems and processes
Maintain an Information Security Policy	
Requirement 12:	Maintain a policy that addresses information security

PCI DSS Applicability Information

The following table illustrates commonly used elements of cardholder and sensitive authentication data; whether storage of each data element is permitted or prohibited; and whether each data element must be protected. This table is not exhaustive, but is presented to illustrate the different types of requirements that apply to each data element.

	Data Element	Storage Permitted	Protection Required	PCI DSS Req. 3.4
Cardholder Data	Primary Account Number (PAN)	Yes	Yes	Yes
	Cardholder Name [1]	Yes	Yes [1]	No
	Service Code [1]	Yes	Yes [1]	No
	Expiration Date [1]	Yes	Yes [1]	No
Sensitive Authentication Data [2]	Full Magnetic Stripe Data [3]	No	N/A	N/A
	CAV2/CVC2/CVV2/CID	No	N/A	N/A
	PIN/PIN Block	No	N/A	N/A

1 *These data elements must be protected if stored in conjunction with the PAN. This protection should be per PCI DSS requirements for general protection of the cardholder data environment. Additionally, other legislation (for example, related to consumer personal data protection, privacy, identity theft, or data security) may require specific protection of this data, or proper disclosure of a company's practices if consumer-related personal data is being collected during the course of business. PCI DSS, however, does not apply if PANs are not stored, processed, or transmitted.*

2 *Sensitive authentication data must not be stored after authorization (even if encrypted).*

3 *Full track data from the magnetic stripe, magnetic stripe image on the chip, or elsewhere.*

Scope of Assessment for Compliance with PCI DSS Requirements

The PCI DSS security requirements apply to all system components. "System components" are defined as any network component, server, or application that is included in or connected to the cardholder data environment. The cardholder data environment is that part of the network that possesses cardholder data or sensitive authentication data. Network components include but are not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances. Server types include, but are not limited to the following: web, application, database, authentication, mail, proxy, network time protocol (NTP), and domain name server (DNS). Applications include all purchased and custom applications, including internal and external (Internet) applications.

Network Segmentation

Network segmentation of, or isolating (segmenting), the cardholder data environment from the remainder of the corporate network is not a PCI DSS requirement. However, it is recommended as a method that may reduce:

- The scope of the PCI DSS assessment
- The cost of the PCI DSS assessment
- The cost and difficulty of implementing and maintaining PCI DSS controls
- The risk to an organization (reduced by consolidating cardholder data into fewer, more controlled locations)

Without adequate network segmentation (sometimes called a "flat network") the entire network is in scope of the PCI DSS assessment. Network segmentation can be achieved through internal network firewalls, routers with strong access control lists or other technology that restricts access to a particular segment of a network.

An important prerequisite to reduce the scope of the cardholder data environment is a clear understanding of business needs and processes related to the storage, processing or transmission of cardholder data. Restricting cardholder data to as few locations as possible by elimination of unnecessary data, and consolidation of necessary data, may require reengineering of long-standing business practices.

Documenting cardholder data flows via a dataflow diagram helps fully understand all cardholder data flows and ensures that any network segmentation is effective at isolating the cardholder data environment.

If network segmentation is in place and will be used to reduce the scope of the PCI DSS assessment, the assessor must verify that the segmentation is adequate to reduce the scope of the assessment. At a high level, adequate network segmentation isolates systems that store, process, or transmit cardholder data from those that do not. However, the adequacy of a specific implementation of network segmentation is highly variable and dependent upon such things as a given network's configuration, the technologies deployed, and other controls that may be implemented.

Appendix F: PCI DSS Reviews – Scoping and Selecting Samples provides more information on the effect of scoping during a PCI DSS assessment.

Wireless

If wireless technology is used to store, process, or transmit cardholder data (for example, point-of-sale transactions, “line-busting”), or if a wireless local area network (LAN) is connected to or part of the cardholder data environment (for example, not clearly separated by a firewall), the PCI DSS requirements and testing procedures for wireless environments apply and must be performed as well (for example, Requirements 1.2.3, 2.1.1, and 4.1.1). Before wireless technology is implemented, a company should carefully evaluate the need for the technology against the risk. Consider deploying wireless technology only for non-sensitive data transmission.

Third Parties/Outsourcing

For service providers required to undergo an annual onsite assessment, compliance validation must be performed on all system components where cardholder data is stored, processed, or transmitted.

A service provider or merchant may use a third-party provider to store, process, or transmit cardholder data on their behalf, or to manage components such as routers, firewalls, databases, physical security, and/or servers. If so, there may be an impact on the security of the cardholder data environment.

For those entities that outsource storage, processing, or transmission of cardholder data to third-party service providers, the Report on Compliance (ROC) must document the role of each service provider, clearly identifying which requirements apply to the reviewed entity and which apply to the service provider. There are two options for third-party service providers to validate compliance: 1) They can undergo a PCI DSS assessment on their own and provide evidence to their customers to demonstrate their compliance, or 2) If they do not undergo their own PCI DSS assessment, they will need to have their services reviewed during the course of each of their customer's PCI DSS assessments. See the bullet beginning “For managed service provider (MSP) reviews” under Part 3 in the “Instructions and Content for Report on Compliance” section below for more information.

Additionally, merchants and service providers must manage and monitor the PCI DSS compliance of all associated third parties with access to cardholder data. *Refer to Requirement 12.8 in this document for details.*

Sampling of Business Facilities and System Components

The assessor may select representative samples of business facilities and system components in order to assess PCI DSS requirements. These samples must include both business facilities and system components, must be a representative selection of all of the types and locations of business facilities as well as types of system components, and must be sufficiently large to provide the assessor with assurance that controls are implemented as expected.

Examples of business facilities include corporate offices, stores, franchise merchants, and business facilities in different locations. Sampling should include system components for each business facility. For example, for each business facility, include a variety of operating systems, functions, and applications that are applicable to the area under review. Within each business facility, the reviewer could choose Sun servers running Apache WWW, Windows servers running Oracle, mainframe systems running legacy card processing applications, data transfer servers running HP-UX, and Linux Servers running MYSQL. If all applications run from a single OS (for example, Windows or Sun), then the sample

should still include a variety of applications (for example, database servers, web servers, data transfer servers). (*See Appendix F: PCI DSS Reviews – Scoping and Sampling.*)

When selecting samples of business facilities and system components, assessors should consider the following:

- If there are standard, required PCI DSS processes in place that each facility must follow, the sample can be smaller than is necessary if there are no standard processes, to provide reasonable assurance that each facility is configured per the standard process.
- If there is more than one type of standard process in place (for example, for different types of system components or facilities), then the sample must be large enough to include system components or facilities secured with each type of process.
- If there are no standard PCI DSS processes in place and each facility is responsible for their processes, then sample size must be larger to be assured that each facility understands and implements PCI DSS requirements appropriately.

Please also refer to Appendix F: PCI DSS Reviews – Scoping and Selecting Samples.

Compensating Controls

On an annual basis, any compensating controls must be documented, reviewed and validated by the assessor and included with the Report on Compliance submission, per *Appendix B: Compensating Controls* and *Appendix C: Compensating Controls Worksheet.*

For each and every compensating control, the Compensating Controls Worksheet (Appendix C) **must** be completed. Additionally, compensating control results should be documented in the ROC in the corresponding PCI DSS requirement section.

See the above-mentioned Appendices B and C for more details on “compensating controls.”

Instructions and Content for Report on Compliance

This document must be used as the template for creating the *Report on Compliance*. The assessed entity should follow each payment brand's respective reporting requirements to ensure each payment brand acknowledges the entity's compliance status. Contact each payment brand to determine reporting requirements and instructions.

Report Content and Format

Follow these instructions for report content and format when completing a Report on Compliance:

1. Executive Summary

Include the following:

- Describe the entity's payment card business, including:
  - Their business role with payment cards, which is how and why they store, process, and/or transmit cardholder data

    Note: This is not intended to be a cut-and-paste from the entity's web site, but should be a tailored description that shows the assessor understands payment and the entity's role.
  - How they process payment (directly, indirectly, etc.)
  - What types of payment channels they serve, such as card-not-present, (for example, mail-order-telephone-order (MOTO), e-Commerce), or card-present
  - Any entities that they connect to for payment transmission or processing, including processor relationships
- A high-level network diagram (either obtained from the entity or created by assessor) of the entity's networking topography that includes:
  - Connections into and out of the network
  - Critical components within the cardholder data environment, including POS devices, systems, databases, and web servers, as applicable
  - Other necessary payment components, as applicable

2. Description of Scope of Work and Approach Taken

Describe the scope, per the Scope of Assessment section of this document, including the following:

- Environment on which assessment focused (for example, client's Internet access points, internal corporate network, processing connections)
- If network segmentation is in place and was used to reduce scope of the PCI DSS review, briefly explain that segmentation and how assessor validated the effectiveness of the segmentation
- Document and justify sampling used for both entities (stores, facilities, etc.) and system components selected, including:
  - Total population
  - Number sampled
  - Rationale for sample selected
  - Why sample size is sufficient to allow assessor to place reasonable reliance that controls reviewed represent controls in place throughout entity
  - Describe any locations or environments that store, process, or transmit cardholder data that were EXCLUDED from the scope of the review, and why these locations/environments were excluded
- List any wholly-owned entities that require compliance with the PCI DSS, and whether they are reviewed separately or as part of this assessment
- List any International entities that require compliance with the PCI DSS, and whether they are reviewed separately or as part of this assessment
- List any wireless LANs and/or wireless payment applications (for example, POS terminals) that are connected to, or could impact the security of the cardholder data environment, and describe security in place for these wireless environments
- The version of the PCI DSS Requirements and Security Assessment Procedures document used to conduct the assessment
- Timeframe of assessment

3. Details about Reviewed Environment

Include the following details in this section:

- A diagram of each piece of the communication link, including LAN, WAN or Internet
- Description of cardholder data environment, for example:
  - Document transmission and processing of cardholder data, including authorization, capture, settlement, chargeback and other flows as applicable

- List of files and tables that store cardholder data, supported by an inventory created (or obtained from the client) and retained by the assessor in the work papers. This inventory should include, for each cardholder data store (file, table, etc.):
  - List all of the elements of stored cardholder data
  - How data is secured
  - How access to data stores are logged

- List of hardware and critical software in use in the cardholder data environment, along with description of function/use for each
- List of service providers and other entities with which the company shares cardholder data (Note: these entities are subject to PCI DSS Requirement 12.8)
- List of third-party payment application products and versions numbers in use, including whether each payment application has been validated according to PA-DSS. Even if a payment application has been PA-DSS validated, the assessor still needs to verify that the application has been implemented in a PCI DSS compliant manner and environment, and according to the payment application vendor's PA-DSS *Implementation Guide. Note: It is not a PCI DSS requirement to use PA-DSS validated applications. Please consult with each payment brand individually to understand their PA-DSS compliance requirements.*
- List of individuals interviewed and their titles
- List of documentation reviewed
- For managed service provider (MSP) reviews, the assessor must clearly identify which requirements in this document apply to the MSP (and are included in the review), and which are not included in the review and are the responsibility of the MSP's customers to include in their reviews. Include information about which of the MSP's IP addresses are scanned as part of the MSP's quarterly vulnerability scans, and which IP addresses are the responsibility of the MSP's customers to include in their own quarterly scans.

4. Contact Information and Report Date

Include:

- Contact information for merchant or service provider and assessor
- Date of report

5. Quarterly Scan Results

- Summarize the four most recent quarterly scan results in the Executive Summary as well as in comments at Requirement 11.2

  Note: It is not required that four passing quarterly scans must be completed for initial PCI DSS compliance if the assessor verifies 1) the most recent scan result was a passing scan, 2) the entity has documented policies and procedures requiring quarterly scanning going forward, and 3) any vulnerabilities noted in the initial scan have been corrected as shown in a re-scan. For subsequent years after the initial PCI DSS review, four passing quarterly scans must have occurred.

- Scan must cover all externally accessible (Internet-facing) IP addresses in existence at the entity, in accordance with the *PCI DSS Security Scanning Procedures*

6. Findings and Observations

- Summarize in the Executive Summary any findings that may not fit into the standard Report on Compliance template format.
- All assessors *must* use the Detailed PCI DSS Requirements and Security Assessment Procedures template to provide detailed report descriptions and findings on each requirement and sub-requirement.
- The assessor *must* review and document any compensating controls considered to conclude that a control is in place.

  See Compensating Controls section above and Appendices B and C for more details on "compensating controls."

Revalidation of Open Items

A "controls in place" report is required to verify compliance. The report is considered non-compliant if it contains "open items," or items that will be finished at a future date. The merchant/service provider must address these items before validation is completed. After these items are addressed by the merchant/service provider, the assessor will then reassess to validate that the remediation occurred and that all requirements are satisfied. After revalidation, the assessor will issue a new Report on Compliance, verifying that the cardholder data environment is fully compliant, and submit it consistent with instructions (see below).

PCI DSS Compliance – Completion Steps

1. Complete the Report on Compliance (ROC) according to the section above entitled "Instructions and Content for Report on Compliance."
2. Ensure passing vulnerability scan(s) have been completed by a PCI SSC Approved Scanning Vendor (ASV), and obtain evidence of passing scan(s) from the ASV.
3. Complete the Attestation of Compliance, for either Service Providers or Merchants as applicable, in its entirety. See Appendices D and E for Attestations of Compliance.
4. Submit the ROC, evidence of a passing scan, and the Attestation of Compliance, along with any other requested documentation, to the acquirer (for merchants) or to the payment brand or other requester (for service providers).

Detailed PCI DSS Requirements and Security Assessment Procedures

For the *PCI DSS Requirements and Security Assessment Procedures,* the following defines the table column headings:

- **PCI DSS Requirements** – This column defines the Data Security Standard and lists requirements to achieve PCI DSS compliance; compliance will be validated against these requirements.
- **Testing Procedures** – This column shows processes to be followed by the assessor to validate that PCI DSS requirements are "in place"
- **In Place** – This column must be used by the assessor to provide a brief description of controls found in place, including those controls found to be in place as a result of compensating controls. (Note: that this column must *not* be used for items that are not yet in place or for open items to be completed at a future date.)
- **Not in Place** – This column must be used by the assessor to provide a brief description controls that are not in place. Note that a non-compliant report should not be submitted to a payment brand or acquirer unless specifically requested. See Appendix D and Appendix E: Attestations of Compliance for further instructions on non-compliant reports.
- **Target Date/Comments** – For those controls "Not In Place" the assessor may include a target date that the merchant or service provider expects to have controls "In Place". Any additional notes or comments may be included here as well.

Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Firewalls are computer devices that control computer traffic allowed between a company's network (internal) and untrusted networks (external), as well as traffic into and out of more sensitive areas within a company's internal trusted network. The cardholder data environment is an example of a more sensitive area within the trusted network of a company.

A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

All systems must be protected from unauthorized access from untrusted networks, whether entering the system via the Internet as e-commerce, employees' Internet access through desktop browsers, employees' e-mail access, dedicated connection such as business to business connections, via wireless networks, or via other sources. Often, seemingly insignificant paths to and from untrusted networks can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
1.1 Establish firewall and router configuration standards that include the following:	**1.1** Obtain and inspect the firewall and router configuration standards and other documentation specified below to verify that standards are complete. Complete the following:			
1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations	**1.1.1** Verify that there is a formal process for testing and approval of all network connections and changes to firewall and router configurations.			
1.1.2 Current network diagram with all connections to cardholder data, including any wireless networks	**1.1.2.a** Verify that a current network diagram (for example, one that shows cardholder data flows over the network) exists and that it documents all connections to cardholder data, including any wireless networks.			
	1.1.2.b Verify that the diagram is kept current.			
1.1.3 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	**1.1.3** Verify that firewall configuration standards include requirements for a firewall at each Internet connection and between any DMZ and the internal network zone. Verify that the current network diagram is consistent with the firewall configuration standards.			
1.1.4 Description of groups, roles, and responsibilities for logical management of network components	**1.1.4** Verify that firewall and router configuration standards include a description of groups, roles, and responsibilities for logical management of network components.			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
1.1.5 Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure	**1.1.5.a** Verify that firewall and router configuration standards include a documented list of services, protocols and ports necessary for business—for example, hypertext transfer protocol (HTTP) and Secure Sockets Layer (SSL), Secure Shell (SSH), and Virtual Private Network (VPN) protocols.			
	1.1.5.b Identify insecure services, protocols, and ports allowed; and verify they are necessary and that security features are documented and implemented by examining firewall and router configuration standards and settings for each service. An example of an insecure service, protocol, or port is FTP, which passes user credentials in clear-text.			
1.1.6 Requirement to review firewall and router rule sets at least every six months	**1.1.6.a** Verify that firewall and router configuration standards require review of firewall and router rule sets at least every six months.			
	1.1.6.b Obtain and examine documentation to verify that the rule sets are reviewed at least every six months.			
1.2 Build a firewall configuration that restricts connections between untrusted networks and any system components in the cardholder data environment.	**1.2** Examine firewall and router configurations to verify that connections are restricted between untrusted networks and system components in the cardholder data environment, as follows:			
Note: An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.				
1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.	**1.2.1.a** Verify that inbound and outbound traffic is limited to that which is necessary for the cardholder data environment, and that the restrictions are documented.			
	1.2.1.b Verify that all other inbound and outbound traffic is specifically denied, for example by using an explicit "deny all" or an implicit deny after allow statement.			
1.2.2 Secure and synchronize router configuration files.	**1.2.2** Verify that router configuration files are secure and synchronized—for example, running configuration files (used for normal running of the routers) and start-up configuration files (used when machines are re-booted), have the same, secure configurations.			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
1.2.3 Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.	**1.2.3** Verify that there are perimeter firewalls installed between any wireless networks and systems that store cardholder data, and that these firewalls deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.			
1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.	**1.3** Examine firewall and router configurations, as detailed below, to determine that there is no direct access between the Internet and system components, including the choke router at the Internet, the DMZ router and firewall, the DMZ cardholder segment, the perimeter router, and the internal cardholder network segment.			
1.3.1 Implement a DMZ to limit inbound and outbound traffic to only protocols that are necessary for the cardholder data environment.	**1.3.1** Verify that a DMZ is implemented to limit inbound and outbound traffic to only protocols that are necessary for the cardholder data environment.			
1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ.	**1.3.2** Verify that inbound Internet traffic is limited to IP addresses within the DMZ.			
1.3.3 Do not allow any direct routes inbound or outbound for traffic between the Internet and the cardholder data environment.	**1.3.3** Verify there is no direct route inbound or outbound for traffic between the Internet and the cardholder data environment.			
1.3.4 Do not allow internal addresses to pass from the Internet into the DMZ.	**1.3.4** Verify that internal addresses cannot pass from the Internet into the DMZ**.**			
1.3.5 Restrict outbound traffic from the cardholder data environment to the Internet such that outbound traffic can only access IP addresses within the DMZ.	**1.3.5** Verify that outbound traffic from the cardholder data environment to the Internet can only access IP addresses within the DMZ.			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
1.3.6 Implement stateful inspection, also known as dynamic packet filtering. (That is, only ”established” connections are allowed into the network.)	**1.3.6** Verify that the firewall performs stateful inspection (dynamic packet filtering). [Only established connections should be allowed in, and only if they are associated with a previously established session (run a port scanner on all TCP ports with “syn reset” or ”syn ack” bits set—a response means packets are allowed through even if they are not part of a previously established session).]			
1.3.7 Place the database in an internal network zone, segregated from the DMZ.	**1.3.7** Verify that the database is on an internal network zone, segregated from the DMZ.			
1.3.8 Implement IP masquerading to prevent internal addresses from being translated and revealed on the Internet, using RFC 1918 address space. Use network address translation (NAT) technologies—for example, port address translation (PAT).	**1.3.8** For the sample of firewall and router components, verify that NAT or other technology using RFC 1918 address space is used to restrict broadcast of IP addresses from the internal network to the Internet (IP masquerading).			
1.4 Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization’s network.	**1.4.a** Verify that mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), and which are used to access the organization’s network, have personal firewall software installed and active.			
	1.4.b Verify that the personal firewall software is configured by the organization to specific standards and is not alterable by mobile computer users.			

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Malicious individuals (external and internal to a company) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily determined via public information.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
2.1 Always change vendor-supplied defaults **before** installing a system on the network—for example, include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.	**2.1** Choose a sample of system components, critical servers, and wireless access points, and attempt to log on (with system administrator help) to the devices using default vendor-supplied accounts and passwords, to verify that default accounts and passwords have been changed. (Use vendor manuals and sources on the Internet to find vendor-supplied accounts/passwords.)			
2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings. Ensure wireless device security settings are enabled for strong encryption technology for authentication and transmission.	**2.1.1** Verify the following regarding vendor default settings for wireless environments and ensure that all wireless networks implement strong encryption mechanisms (for example, AES): ▪ Encryption keys were changed from default at installation, and are changed anytime anyone with knowledge of the keys leaves the company or changes positions ▪ Default SNMP community strings on wireless devices were changed ▪ Default passwords/passphrases on access points were changed ▪ Firmware on wireless devices is updated to support strong encryption for authentication and transmission over wireless networks (for example, WPA/WPA2) ▪ Other security-related wireless vendor defaults, if applicable			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.	**2.2.a** Examine the organization's system configuration standards for all types of system components and verify the system configuration standards are consistent with industry-accepted hardening standards—for example, SysAdmin Audit Network Security (SANS), National Institute of Standards Technology (NIST), and Center for Internet Security (CIS).			
	2.2.b Verify that system configuration standards include each item below (at 2.2.1 – 2.2.4).			
	2.2.c Verify that system configuration standards are applied when new systems are configured.			
2.2.1 Implement only one primary function per server.	**2.2.1** For a sample of system components, verify that only one primary function is implemented per server. For example, web servers, database servers, and DNS should be implemented on separate servers.			
2.2.2 Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the device's specified function).	**2.2.2** For a sample of system components, inspect enabled system services, daemons, and protocols. Verify that unnecessary or insecure services or protocols are not enabled, or are justified and documented as to appropriate use of the service. For example, FTP is not used, or is encrypted via SSH or other technology.			
2.2.3 Configure system security parameters to prevent misuse.	**2.2.3.a** Interview system administrators and/or security managers to verify that they have knowledge of common security parameter settings for system components.			
	2.2.3.b Verify that common security parameter settings are included in the system configuration standards.			
	2.2.3.c For a sample of system components, verify that common security parameters are set appropriately.			
2.2.4 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	**2.2.4** For a sample of system components, verify that all unnecessary functionality (for example, scripts, drivers, features, subsystems, file systems, etc.) is removed. Verify enabled functions are documented and support secure configuration, and that only documented functionality is present on the sampled machines.			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
2.3 Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.	**2.3** For a sample of system components, verify that non-console administrative access is encrypted by: ▪ Observing an administrator log on to each system to verify that a strong encryption method is invoked before the administrator's password is requested; ▪ Reviewing services and parameter files on systems to determine that Telnet and other remote log-in commands are not available for use internally; and ▪ Verifying that administrator access to the web-based management interfaces is encrypted with strong cryptography.			
2.4 Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in *Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers.*	**2.4** Perform testing procedures **A.1.1** through **A.1.4** detailed in *Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers* for PCI DSS assessments of shared hosting providers, to verify that shared hosting providers protect their entities' (merchants and service providers) hosted environment and data.			

Protect Cardholder Data

Requirement 3: Protect stored cardholder data

Protection methods such as encryption, truncation, masking, and hashing are critical components of cardholder data protection. If an intruder circumvents other network security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed, and not sending PAN in unencrypted e-mails.

Please refer to the *PCI DSS Glossary of Terms, Abbreviations, and Acronyms* for definitions of "strong cryptography" and other PCI DSS terms.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
3.1 Keep cardholder data storage to a minimum. Develop a data retention and disposal policy. Limit storage amount and retention time to that which is required for business, legal, and/or regulatory purposes, as documented in the data retention policy.	**3.1** Obtain and examine the company policies and procedures for data retention and disposal, and perform the following ▪ Verify that policies and procedures include legal, regulatory, and business requirements for data retention, including specific requirements for retention of cardholder data (for example, cardholder data needs to be held for X period for Y business reasons) ▪ Verify that policies and procedures include provisions for disposal of data when no longer needed for legal, regulatory, or business reasons, including disposal of cardholder data ▪ Verify that policies and procedures include coverage for all storage of cardholder data ▪ Verify that policies and procedures include a programmatic (automatic) process to remove, at least on a quarterly basis, stored cardholder data that exceeds business retention requirements, or, alternatively, requirements for a review, conducted at least on a quarterly basis, to verify that stored cardholder data does not exceed business retention requirements			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
3.2 Do not store sensitive authentication data after authorization (even if encrypted). Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3:	**3.2** If sensitive authentication data is received and deleted, obtain and review the processes for deleting the data to verify that the data is unrecoverable. For each item of sensitive authentication data below, perform the following steps:			
3.2.1 Do not store the full contents of any track from the magnetic stripe (located on the back of a card, contained in a chip, or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data. *Note: In the normal course of business, the following data elements from the magnetic stripe may need to be retained:* ▪ *The cardholder's name,* ▪ *Primary account number (PAN),* ▪ *Expiration date, and* ▪ *Service code* *To minimize risk, store only these data elements as needed for business.* *Note: See* PCI DSS Glossary of Terms, Abbreviations, and Acronyms *for additional information.*	**3.2.1** For a sample of system components, examine the following and verify that the full contents of any track from the magnetic stripe on the back of card are not stored under any circumstance: ▪ Incoming transaction data ▪ All logs (for example, transaction, history, debugging, error) ▪ History files ▪ Trace files ▪ Several database schemas ▪ Database contents			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
3.2.2 Do not store the card-verification code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions. *Note: See* PCI DSS Glossary of Terms, Abbreviations, and Acronyms *for additional information.*	**3.2.2** For a sample of system components, verify that the three-digit or four-digit card-verification code or value printed on the front of the card or the signature panel (CVV2, CVC2, CID, CAV2 data) is not stored under any circumstance: ▪ Incoming transaction data ▪ All logs (for example, transaction, history, debugging, error) ▪ History files ▪ Trace files ▪ Several database schemas ▪ Database contents			
3.2.3 Do not store the personal identification number (PIN) or the encrypted PIN block.	**3.2.3** For a sample of system components, examine the following and verify that PINs and encrypted PIN blocks are not stored under any circumstance: ▪ Incoming transaction data ▪ All logs (for example, transaction, history, debugging, error) ▪ History files ▪ Trace files ▪ Several database schemas ▪ Database contents			
3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed). *Notes:* ▪ *This requirement does not apply to employees and other parties with a legitimate business need to see the full PAN.* ▪ *This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, for point-of-sale (POS) receipts.*	**3.3** Obtain and examine written policies and examine displays of PAN (for example, on screen, on paper receipts) to verify that primary account numbers (PANs) are masked when displaying cardholder data, except for those with a legitimate business need to see full PAN.			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
3.4 Render PAN, at minimum, unreadable anywhere it is stored (including on portable digital media, backup media, in logs) by using any of the following approaches: ▪ One-way hashes based on strong cryptography ▪ Truncation ▪ Index tokens and pads (pads must be securely stored) ▪ Strong cryptography with associated key-management processes and procedures The MINIMUM account information that must be rendered unreadable is the PAN. *Notes:* ▪ *If for some reason, a company is unable render the PAN unreadable, refer to* Appendix B: Compensating Controls. ▪ *"Strong cryptography" is defined in* the PCI DSS Glossary of Terms, Abbreviations, and Acronyms.	**3.4.a** Obtain and examine documentation about the system used to protect the PAN, including the vendor, type of system/process, and the encryption algorithms (if applicable). Verify that the PAN is rendered unreadable using one of the following methods: ▪ One-way hashes based on strong cryptography ▪ Truncation ▪ Index tokens and pads, with the pads being securely stored ▪ Strong cryptography, with associated key-management processes and procedures			
	3.4.b Examine several tables or files from a sample of data repositories to verify the PAN is rendered unreadable (that is, not stored in plain-text).			
	3.4.c Examine a sample of removable media (for example, back-up tapes) to confirm that the PAN is rendered unreadable.			
	3.4.d Examine a sample of audit logs to confirm that the PAN is sanitized or removed from the logs.			
3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (for example, by not using local user account databases). Decryption keys must	**3.4.1.a** If disk encryption is used, verify that logical access to encrypted file systems is implemented via a mechanism that is separate from the native operating systems mechanism (for example, not using local user account databases).			
	3.4.1.b Verify that cryptographic keys are stored securely (for example, stored on removable media that is adequately protected with strong access controls).			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
not be tied to user accounts.	**3.4.1.c** Verify that cardholder data on removable media is encrypted wherever stored. *Note: Disk encryption often cannot encrypt removable media, so data stored on this media will need to be encrypted separately.*			
3.5 Protect cryptographic keys used for encryption of cardholder data against both disclosure and misuse:	**3.5** Verify processes to protect keys used for encryption of cardholder data against disclosure and misuse by performing the following:			
3.5.1 Restrict access to cryptographic keys to the fewest number of custodians necessary.	**3.5.1** Examine user access lists to verify that access to keys is restricted to very few custodians.			
3.5.2 Store cryptographic keys securely in the fewest possible locations and forms.	**3.5.2** Examine system configuration files to verify that keys are stored in encrypted format and that key-encrypting keys are stored separately from data-encrypting keys.			
3.6 Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following:	**3.6.a** Verify the existence of key-management procedures for keys used for encryption of cardholder data. *Note: Numerous industry standards for key management are available from various resources including NIST, which can be found at http://csrc.nist.gov.*			
	3.6.b For service providers only: If the service provider shares keys with their customers for transmission of cardholder data, verify that the service provider provides documentation to customers that includes guidance on how to securely store and change customer's keys (used to transmit data between customer and service provider).			
	3.6.c Examine the key-management procedures and perform the following:			
3.6.1 Generation of strong cryptographic keys	**3.6.1** Verify that key-management procedures are implemented to require the generation of strong keys.			
3.6.2 Secure cryptographic key distribution	**3.6.2** Verify that key-management procedures are implemented to require secure key distribution.			
3.6.3 Secure cryptographic key storage	**3.6.3** Verify that key-management procedures are implemented to require secure key storage.			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
3.6.4 Periodic cryptographic key changes ▪ As deemed necessary and recommended by the associated application (for example, re-keying); preferably automatically ▪ At least annually	**3.6.4** Verify that key-management procedures are implemented to require periodic key changes at least annually.			
3.6.5 Retirement or replacement of old or suspected compromised cryptographic keys	**3.6.5.a** Verify that key-management procedures are implemented to require the retirement of old keys (for example: archiving, destruction, and revocation as applicable).			
	3.6.5.b Verify that the key-management procedures are implemented to require the replacement of known or suspected compromised keys.			
3.6.6 Split knowledge and establishment of dual control of cryptographic keys	**3.6.6** Verify that key-management procedures are implemented to require split knowledge and dual control of keys (for example, requiring two or three people, each knowing only their own part of the key, to reconstruct the whole key).			
3.6.7 Prevention of unauthorized substitution of cryptographic keys	**3.6.7** Verify that key-management procedures are implemented to require the prevention of unauthorized substitution of keys.			
3.6.8 Requirement for cryptographic key custodians to sign a form stating that they understand and accept their key-custodian responsibilities	**3.6.8** Verify that key-management procedures are implemented to require key custodians to sign a form specifying that they understand and accept their key-custodian responsibilities.			

Requirement 4: Encrypt transmission of cardholder data across open, public networks

Sensitive information must be encrypted during transmission over networks that are easily accessed by malicious individuals. Misconfigured wireless networks and vulnerabilities in legacy encryption and authentication protocols can be continued targets of malicious individuals who exploit these vulnerabilities to gain privileged access to cardholder data environments.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
4.1 Use strong cryptography and security protocols such as SSL/TLS or IPSEC to safeguard sensitive cardholder data during transmission over open, public networks. *Examples of open, public networks that are in scope of the PCI DSS are:* ▪ *The Internet,* ▪ *Wireless technologies,* ▪ *Global System for Mobile communications (GSM), and* ▪ *General Packet Radio Service (GPRS).*	**4.1.a** Verify the use of encryption (for example, SSL/TLS or IPSEC) wherever cardholder data is transmitted or received over open, public networks ▪ Verify that strong encryption is used during data transmission ▪ For SSL implementations: - Verify that the server supports the latest patched versions. - Verify that HTTPS appears as a part of the browser Universal Record Locator (URL). - Verify that no cardholder data is required when HTTPS does not appear in the URL. ▪ Select a sample of transactions as they are received and observe transactions as they occur to verify that cardholder data is encrypted during transit. ▪ Verify that only trusted SSL/TLS keys/certificates are accepted. ▪ Verify that the proper encryption strength is implemented for the encryption methodology in use. (Check vendor recommendations/best practices.)			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
4.1.1 Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission. ▪ *For new wireless implementations, it is prohibited to implement WEP after March 31, 2009.* ▪ *For current wireless implementations, it is prohibited to use WEP after June 30, 2010.*	**4.1.1** For wireless networks transmitting cardholder data or connected to the cardholder data environment, verify that industry best practices (for example, IEEE 802.11i) are used to implement strong encryption for authentication and transmission.			
4.2 Never send unencrypted PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat).	**4.2.a** Verify that strong cryptography is used whenever cardholder data is sent via end-user messaging technologies.			
	4.2.b Verify the existence of a policy stating that unencrypted PANs are not to be sent via end-user messaging technologies.			

Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software or programs

Malicious software, commonly referred to as "malware"—including viruses, worms, and Trojans—enters the network during many business approved activities including employees' e-mail and use of the Internet, mobile computers, and storage devices, resulting in the exploitation of system vulnerabilities. Anti-virus software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	**5.1** For a sample of system components including all operating system types commonly affected by malicious software, verify that anti-virus software is deployed if applicable anti-virus technology exists.			
5.1.1 Ensure that all anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.	**5.1.1** For a sample of system components, verify that all anti-virus programs detect, remove, and protect against all known types of malicious software (for example, viruses, Trojans, worms, spyware, adware, and rootkits).			
5.2 Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.	**5.2** Verify that all anti-virus software is current, actively running, and capable of generating logs by performing the following:			
	5.2.a Obtain and examine the policy and verify that it requires updating of anti-virus software and definitions.			
	5.2.b Verify that the master installation of the software is enabled for automatic updates and periodic scans.			
	5.2.c For a sample of system components including all operating system types commonly affected by malicious software, verify that automatic updates and periodic scans are enabled.			
	5.2d For a sample of system components, verify that antivirus software log generation is enabled and that such logs are retained in accordance with PCI DSS Requirement 10.7			

Requirement 6: Develop and maintain secure systems and applications

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches, which must be installed by the entities that manage the systems. All critical systems must have the most recently released, appropriate software patches to protect against exploitation and compromise of cardholder data by malicious individuals and malicious software.

Note: Appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations. For in-house developed applications, numerous vulnerabilities can be avoided by using standard system development processes and secure coding techniques.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
6.1 Ensure that all system components and software have the latest vendor-supplied security patches installed. Install critical security patches within one month of release. *Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*	**6.1.a** For a sample of system components and related software, compare the list of security patches installed on each system to the most recent vendor security patch list, to verify that current vendor patches are installed.			
	6.1.b Examine policies related to security patch installation to verify they require installation of all critical new security patches within one month.			
6.2 Establish a process to identify newly discovered security vulnerabilities (for example, subscribe to alert services freely available on the Internet). Update configuration standards as required by PCI DSS Requirement 2.2 to address new vulnerability issues.	**6.2.a** Interview responsible personnel to verify that processes are implemented to identify new security vulnerabilities.			
	6.2.b Verify that processes to identify new security vulnerabilities include using outside sources for security vulnerability information and updating the system configuration standards reviewed in Requirement 2.2 as new vulnerability issues are found.			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
6.3 Develop software applications in accordance with PCI DSS (for example, secure authentication and logging) and based on industry best practices, and incorporate information security throughout the software development life cycle. These processes must include the following:	**6.3.a** Obtain and examine written software development processes to verify that the processes are based on industry standards, security is included throughout the life cycle, and software applications are developed in accordance with PCI DSS.			
	6.3.b From an examination of written software development processes, interviews of software developers, and examination of relevant data (network configuration documentation, production and test data, etc.), verify that:			
6.3.1 Testing of all security patches, and system and software configuration changes before deployment, including but not limited to the following:	**6.3.1** All changes (including patches) are tested before being deployed into production.			
6.3.1.1 Validation of all input (to prevent cross-site scripting, injection flaws, malicious file execution, etc.)	**6.3.1.1** Validation of all input (to prevent cross-site scripting, injection flaws, malicious file execution, etc.)			
6.3.1.2 Validation of proper error handling	**6.3.1.2** Validation of proper error handling			
6.3.1.3 Validation of secure cryptographic storage	**6.3.1.3** Validation of secure cryptographic storage			
6.3.1.4 Validation of secure communications	**6.3.1.4** Validation of secure communications			
6.3.1.5 Validation of proper role-based access control (RBAC)	**6.3.1.5** Validation of proper role-based access control (RBAC)			
6.3.2 Separate development/test and production environments	**6.3.2** The development/test environments are separate from the production environment, with access control in place to enforce the separation.			
6.3.3 Separation of duties between development/test and production environments	**6.3.3** There is a separation of duties between personnel assigned to the development/test environments and those assigned to the production environment.			
6.3.4 Production data (live PANs) are not used for testing or development	**6.3.4** Production data (live PANs) are not used for testing and development, or are sanitized before use.			
6.3.5 Removal of test data and accounts before production systems become active	**6.3.5** Test data and accounts are removed before a production system becomes active.			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
6.3.6 Removal of custom application accounts, user IDs, and passwords before applications become active or are released to customers	**6.3.6** Custom application accounts, user IDs and/or passwords are removed before system goes into production or is released to customers.			
6.3.7 Review of custom code prior to release to production or customers in order to identify any potential coding vulnerability *Note: This requirement for code reviews applies to all custom code (both internal and public-facing), as part of the system development life cycle required by PCI DSS Requirement 6.3. Code reviews can be conducted by knowledgeable internal personnel or third parties. Web applications are also subject to additional controls, if they are public facing, to address ongoing threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.6.*	**6.3.7.a** Obtain and review policies to confirm all custom application code changes for *internal applications* must be reviewed (either using manual or automated processes), as follows: ▪ Code changes are reviewed by individuals other then the originating code author, and by individuals who are knowledgeable in code review techniques and secure coding practices. ▪ Appropriate corrections are implemented prior to release. ▪ Code review results are reviewed and approved by management prior to release.			
	6.3.7.b Obtain and review policies to confirm that all custom application code changes for *web applications* must be reviewed (using either manual or automated processes) as follows: ▪ Code changes are reviewed by individuals other then the originating code author, and by individuals who are knowledgeable in code review techniques and secure coding practices. ▪ Code reviews ensure code is developed according to secure coding guidelines such as the *Open Web Security Project Guide* (see PCI DSS Requirement 6.5). ▪ Appropriate corrections are implemented prior to release. ▪ Code review results are reviewed and approved by management prior to release.			
	6.3.7.c Select a sample of recent custom application changes and verify that custom application code is reviewed according to 6.3.7a and 6.3.7b above.			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
6.4 Follow change control procedures for all changes to system components. The procedures must include the following:	**6.4.a** Obtain and examine company change-control procedures related to implementing security patches and software modifications, and verify that the procedures require items 6.4.1 – 6.4.4 below.			
	6.4.b For a sample of system components and recent changes/security patches, trace those changes back to related change control documentation. For each change examined, perform the following:			
6.4.1 Documentation of impact	**6.4.1** Verify that documentation of customer impact is included in the change control documentation for each sampled change.			
6.4.2 Management sign-off by appropriate parties	**6.4.2** Verify that management sign-off by appropriate parties is present for each sampled change.			
6.4.3 Testing of operational functionality	**6.4.3** Verify that operational functionality testing is performed for each sampled change.			
6.4.4 Back-out procedures	**6.4.4** Verify that back-out procedures are prepared for each sampled change			
6.5 Develop all web applications (internal and external, and including web administrative access to application) based on secure coding guidelines such as the *Open Web Application Security Project Guide.* Cover prevention of common coding vulnerabilities in software development processes, to include the following: *Note: The vulnerabilities listed at 6.5.1 through 6.5.10 were current in the OWASP guide when PCI DSS v1.2 was published. However, if and when the OWASP guide is updated, the current version must be used for these requirements.*	**6.5.a** Obtain and review software development processes for any web-based applications. Verify that processes require training in secure coding techniques for developers, and are based on guidance such as the OWASP guide (http://www.owasp.org).			
	6.5.b Interview a sample of developers and obtain evidence that they are knowledgeable in secure coding techniques.			
	6.5.c Verify that processes are in place to ensure that web applications are not vulnerable to the following:			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
6.5.1 Cross-site scripting (XSS)	**6.5.1** Cross-site scripting (XSS) (Validate all parameters before inclusion.)			
6.5.2 Injection flaws, particularly SQL injection. Also consider LDAP and Xpath injection flaws as well as other injection flaws.	**6.5.2** Injection flaws, particularly SQL injection (Validate input to verify user data cannot modify meaning of commands and queries.)			
6.5.3 Malicious file execution	**6.5.3** Malicious file execution (Validate input to verify application does not accept filenames or files from users.)			
6.5.4 Insecure direct object references	**6.5.4** Insecure direct object references (Do not expose internal object references to users.)			
6.5.5 Cross-site request forgery (CSRF)	**6.5.5** Cross-site request forgery (CSRF) (Do not reply on authorization credentials and tokens automatically submitted by browsers.)			
6.5.6 Information leakage and improper error handling	**6.5.6** Information leakage and improper error handling (Do not leak information via error messages or other means.)			
6.5.7 Broken authentication and session management	**6.5.7** Broken authentication and session management (Properly authenticate users and protect account credentials and session tokens.)			
6.5.8 Insecure cryptographic storage	**6.5.8** Insecure cryptographic storage (Prevent cryptographic flaws.)			
6.5.9 Insecure communications	**6.5.9** Insecure communications (Properly encrypt all authenticated and sensitive communications.)			
6.5.10 Failure to restrict URL access	**6.5.10** Failure to restrict URL access (Consistently enforce access control in presentation layer and business logic for all URLs.)			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by *either* of the following methods: ▪ Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes ▪ Installing a web-application firewall in front of public-facing web applications	**6.6** For *public-facing* web applications, ensure that *either* one of the following methods are in place as follows: ▪ Verify that public-facing web applications are reviewed (using either manual or automated vulnerability security assessment tools or methods), as follows: - At least annually - After any changes - By an organization that specializes in application security - That all vulnerabilities are corrected - That the application is re-evaluated after the corrections ▪ Verify that a web-application firewall is in place in front of public-facing web applications to detect and prevent web-based attacks. *Note: "An organization that specializes in application security" can be either a third-party company or an internal organization, as long as the reviewers specialize in application security and can demonstrate independence from the development team.*			

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need to know

To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities.

"Need to know" is when access rights are granted to only the least amount of data and privileges needed to perform a job.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following:	**7.1** Obtain and examine written policy for data control, and verify that the policy incorporates the following:			
7.1.1 Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities	**7.1.1** Confirm that access rights for privileged user IDs are restricted to least privileges necessary to perform job responsibilities.			
7.1.2 Assignment of privileges is based on individual personnel's job classification and function	**7.1.2** Confirm that privileges are assigned to individuals based on job classification and function (also called "role-based access control" or RBAC).			
7.1.3 Requirement for an authorization form signed by management that specifies required privileges	**7.1.3** Confirm that an authorization form is required for all access, that it must specify required privileges, and that it must be signed by management.			
7.1.4 Implementation of an automated access control system	**7.1.4** Confirm that access controls are implemented via an automated access control system.			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
7.2 Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system must include the following:	**7.2** Examine system settings and vendor documentation to verify that an access control system is implemented as follows:			
7.2.1 Coverage of all system components	**7.2.1** Confirm that access control systems are in place on all system components.			
7.2.2 Assignment of privileges to individuals based on job classification and function	**7.2.2** Confirm that access control systems are configured to enforce privileges assigned to individuals based on job classification and function.			
7.2.3 Default "deny-all" setting	**7.2.3** Confirm that the access control systems has a default "deny-all" setting. *Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*			

Requirement 8: Assign a unique ID to each person with computer access.

Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for his or her actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
8.1 Assign all users a unique ID before allowing them to access system components or cardholder data.	**8.1** Verify that all users are assigned a unique ID for access to system components or cardholder data.			
8.2 In addition to assigning a unique ID**,** employ at least one of the following methods to authenticate all users: ▪ Password or passphrase ▪ Two-factor authentication (for example, token devices, smart cards, biometrics, or public keys)	**8.2** To verify that users are authenticated using unique ID and additional authentication (for example, a password) for access to the cardholder data environment, perform the following: ▪ Obtain and examine documentation describing the authentication method(s) used. ▪ For each type of authentication method used and for each type of system component, observe an authentication to verify authentication is functioning consistent with documented authentication method(s).			
8.3 Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. Use technologies such as remote authentication and dial-in service (RADIUS); terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates.	**8.3** To verify that two-factor authentication is implemented for all remote network access, observe an employee (for example, an administrator) connecting remotely to the network and verify that both a password and an additional authentication item (for example, smart card, token, PIN) are required.			
8.4 Render all passwords unreadable during transmission and storage on all system components using strong cryptography (defined in *PCI DSS Glossary of Terms, Abbreviations, and Acronyms*).	**8.4.a** For a sample of system components, examine password files to verify that passwords are unreadable during transmission and storage.			
	8.4.b For service providers only, observe password files to verify that customer passwords are encrypted.			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
8.5 Ensure proper user authentication and password management for non-consumer users and administrators on all system components as follows:	**8.5** Review procedures and interview personnel to verify that procedures are implemented for user authentication and password management, by performing the following:			
8.5.1 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	**8.5.1.a** Select a sample of user IDs, including both administrators and general users. Verify that each user is authorized to use the system according to company policy by performing the following: ▪ Obtain and examine an authorization form for each ID. ▪ Verify that the sampled user IDs are implemented in accordance with the authorization form (including with privileges as specified and all signatures obtained), by tracing information from the authorization form to the system.			
8.5.2 Verify user identity before performing password resets.	**8.5.2** Examine password procedures and observe security personnel to verify that, if a user requests a password reset by phone, e-mail, web, or other non-face-to-face method, the user's identity is verified before the password is reset.			
8.5.3 Set first-time passwords to a unique value for each user and change immediately after the first use.	**8.5.3** Examine password procedures and observe security personnel to verify that first-time passwords for new users are set to a unique value for each user and changed after first use.			
8.5.4 Immediately revoke access for any terminated users.	**8.5.4** Select a sample of employees terminated in the past six months, and review current user access lists to verify that their IDs have been deactivated or removed.			
8.5.5 Remove/disable inactive user accounts at least every 90 days.	**8.5.5** Verify that inactive accounts over 90 days old are either removed or disabled.			
8.5.6 Enable accounts used by vendors for remote maintenance only during the time period needed.	**8.5.6** Verify that any accounts used by vendors to support and maintain system components are disabled, enabled only when needed by the vendor, and monitored while being used.			
8.5.7 Communicate password procedures and policies to all users who have access to cardholder data.	**8.5.7** Interview the users from a sample of user IDs, to verify that they are familiar with password procedures and policies.			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
8.5.8 Do not use group, shared, or generic accounts and passwords.	**8.5.8.a** For a sample of system components, examine user ID lists to verify the following ▪ Generic user IDs and accounts are disabled or removed. ▪ Shared user IDs for system administration activities and other critical functions do not exist. ▪ Shared and generic user IDs are not used to administer any system components.			
	8.5.8.b Examine password policies/procedures to verify that group and shared passwords are explicitly prohibited.			
	8.5.8.c Interview system administrators to verify that group and shared passwords are not distributed, even if requested.			
8.5.9 Change user passwords at least every 90 days.	**8.5.9** For a sample of system components, obtain and inspect system configuration settings to verify that user password parameters are set to require users to change passwords at least every 90 days. For service providers only, review internal processes and customer/user documentation to verify that customer passwords are required to change periodically and that customers are given guidance as to when, and under what circumstances, passwords must change.			
8.5.10 Require a minimum password length of at least seven characters.	**8.5.10** For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require passwords to be at least seven characters long. For service providers only, review internal processes and customer/user documentation to verify that customer passwords are required to meet minimum length requirements.			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
8.5.11 Use passwords containing both numeric and alphabetic characters.	**8.5.11** For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require passwords to contain both numeric and alphabetic characters. For service providers only, review internal processes and customer/user documentation to verify that customer passwords are required to contain both numeric and alphabetic characters.			
8.5.12 Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.	**8.5.12** For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require that new passwords cannot be the same as the four previously used passwords. For service providers only, review internal processes and customer/user documentation to verify that new customer passwords cannot be the same as the previous four passwords.			
8.5.13 Limit repeated access attempts by locking out the user ID after not more than six attempts.	**8.5.13** For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require that a user's account is locked out after not more than six invalid logon attempts. For service providers only, review internal processes and customer/user documentation to verify that customer accounts are temporarily locked-out after not more than six invalid access attempts.			
8.5.14 Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.	**8.5.14** For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require that once a user account is locked out, it remains locked for a minimum of 30 minutes or until a system administrator resets the account.			
8.5.15 If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal.	**8.5.15** For a sample of system components, obtain and inspect system configuration settings to verify that system/session idle time out features have been set to 15 minutes or less.			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
8.5.16 Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users.	**8.5.16.a** Review database and application configuration settings and verify that user authentication and access to databases includes the following: ▪ All users are authenticated prior to access. ▪ All user access to, user queries of, and user actions on (for example, move, copy, delete), the database are through programmatic methods only (for example, through stored procedures). ▪ Direct access or queries to databases are restricted to database administrators.			
	8.5.16.b Review database applications and the related application IDs to verify that application IDs can only be used by the applications (and not by individual users or other processes).			

Requirement 9: Restrict physical access to cardholder data.

Any physical access to data or systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.	**9.1** Verify the existence of physical security controls for each computer room, data center, and other physical areas with systems in the cardholder data environment. ▪ Verify that access is controlled with badge readers or other devices including authorized badges and lock and key. ▪ Observe a system administrator's attempt to log into consoles for randomly selected systems in the cardholder environment and verify that they are "locked" to prevent unauthorized use.			
9.1.1 Use video cameras or other access control mechanisms to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law. *Note: "Sensitive areas" refers to any data center, server room or any area that houses systems that store, process, or transmit cardholder data. This excludes the areas where only point-of-sale terminals are present, such as the cashier areas in a retail store.*	**9.1.1** Verify that video cameras or other access control mechanisms are in place to monitor the entry/exit points to sensitive areas. Video cameras or other mechanisms should be protected from tampering or disabling. Verify that video cameras or other mechanisms are monitored and that data from cameras or other mechanisms is stored for at least three months.			
9.1.2 Restrict physical access to publicly accessible network jacks.	**9.1.2** Verify by interviewing network administrators and by observation that network jacks are enabled only when needed by authorized employees. For example, conference rooms used to host visitors should not have network ports enabled with DHCP. Alternatively, verify that visitors are escorted at all times in areas with active network jacks.			
9.1.3 Restrict physical access to wireless access points, gateways, and handheld devices.	**9.1.3** Verify that physical access to wireless access points, gateways, and handheld devices is appropriately restricted.			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
9.2 Develop procedures to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder data is accessible. *For purposes of this requirement, "employee" refers to full-time and part-time employees, temporary employees and personnel, and contractors and consultants who are "resident" on the entity's site. A "visitor" is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the facility for a short duration, usually not more than one day.*	**9.2.a** Review processes and procedures for assigning badges to employees, and visitors, and verify these processes include the following: ▪ Granting new badges, changing access requirements, and revoking terminated employee and expired visitor badges ▪ Limited access to badge system			
	9.2.b Observe people within the facility to verify that it is easy to distinguish between employees and visitors.			
9.3 Make sure all visitors are handled as follows:	**9.3** Verify that employee/visitor controls are in place as follows:			
9.3.1 Authorized before entering areas where cardholder data is processed or maintained	**9.3.1** Observe visitors to verify the use of visitor ID badges. Attempt to gain access to the data center to verify that a visitor ID badge does not permit unescorted access to physical areas that store cardholder data.			
9.3.2 Given a physical token (for example, a badge or access device) that expires and that identifies the visitors as non-employee	**9.3.2** Examine employee and visitor badges to verify that ID badges clearly distinguish employees from visitors/outsiders and that visitor badges expire.			
9.3.3 Asked to surrender the physical token before leaving the facility or at the date of expiration	**9.3.3** Observe visitors leaving the facility to verify visitors are asked to surrender their ID badge upon departure or expiration.			
9.4 Use a visitor log to maintain a physical audit trail of visitor activity. Document the visitor's name, the firm represented, and the employee authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law.	**9.4.a** Verify that a visitor log is in use to record physical access to the facility as well as for computer rooms and data centers where cardholder data is stored or transmitted.			
	9.4.b Verify that the log contains the visitor's name, the firm represented, and the employee authorizing physical access, and is retained for at least three months.			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
9.5 Store media back-ups in a secure location, preferably an off-site facility, such as an alternate or back-up site, or a commercial storage facility. Review the location's security at least annually.	**9.5** Verify that the storage location is reviewed at least annually to determine that back-up media storage is secure.			
9.6 Physically secure all paper and electronic media that contain cardholder data.	**9.6** Verify that procedures for protecting cardholder data include controls for physically securing paper and electronic media (including computers, removable electronic media, networking, and communications hardware, telecommunication lines, paper receipts, paper reports, and faxes).			
9.7 Maintain strict control over the internal or external distribution of any kind of media that contains cardholder data, including the following:	**9.7** Verify that a policy exists to control distribution of media containing cardholder data, and that the policy covers all distributed media including that distributed to individuals.			
9.7.1 Classify the media so it can be identified as confidential.	**9.7.1** Verify that all media is classified so that it can be identified as "confidential."			
9.7.2 Send the media by secured courier or other delivery method that can be accurately tracked.	**9.7.2** Verify that all media sent outside the facility is logged and authorized by management and sent via secured courier or other delivery method that can be tracked.			
9.8 Ensure management approves any and all media containing cardholder data that is moved from a secured area (especially when media is distributed to individuals).	**9.8** Select a recent sample of several days of offsite tracking logs for all media containing cardholder data, and verify the presence in the logs of tracking details and proper management authorization.			
9.9 Maintain strict control over the storage and accessibility of media that contains cardholder data.	**9.9** Obtain and examine the policy for controlling storage and maintenance of hardcopy and electronic media and verify that the policy requires periodic media inventories.			
9.9.1 Properly maintain inventory logs of all media and conduct media inventories at least annually.	**9.9.1** Obtain and review the media inventory log to verify that periodic media inventories are performed at least annually.			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
9.10 Destroy media containing cardholder data when it is no longer needed for business or legal reasons as follows:	**9.10** Obtain and examine the periodic media destruction policy and verify that it covers all media containing cardholder data and confirm the following:			
9.10.1 Shred, incinerate, or pulp hardcopy materials so that cardholder data cannot be reconstructed.	**9.10.1.a** Verify that hard-copy materials are cross-cut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed.			
	9.10.1.b Examine storage containers used for information to be destroyed to verify that the containers are secured. For example, verify that a "to-be-shredded" container has a lock preventing access to its contents.			
9.10.2 Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.	**9.10.2** Verify that cardholder data on electronic media is rendered unrecoverable via a secure wipe program in accordance with industry-accepted standards for secure deletion, or otherwise physically destroying the media (for example, degaussing).			

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data.

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult without system activity logs.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
10.1 Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.	**10.1** Verify through observation and interviewing the system administrator, that audit trails are enabled and active for system components.			
10.2 Implement automated audit trails for all system components to reconstruct the following events:	**10.2** Through interviews, examination of audit logs, and examination of audit log settings, perform the following:			
10.2.1 All individual accesses to cardholder data	**10.2.1** Verify all individual access to cardholder data is logged.			
10.2.2 All actions taken by any individual with root or administrative privileges	**10.2.2** Verify actions taken by any individual with root or administrative privileges is logged.			
10.2.3 Access to all audit trails	**10.2.3** Verify access to all audit trails is logged.			
10.2.4 Invalid logical access attempts	**10.2.4** Verify invalid logical access attempts are logged.			
10.2 5 Use of identification and authentication mechanisms	**10.2.5** Verify use of identification and authentication mechanisms is logged.			
10.2.6 Initialization of the audit logs	**10.2.6** Verify initialization of audit logs is logged.			
10.2.7 Creation and deletion of system-level objects	**10.2.7** Verify creation and deletion of system level objects are logged.			
10.3 Record at least the following audit trail entries for all system components for each event:	**10.3** Through interviews and observation, for each auditable event (from 10.2), perform the following:			
10.3.1 User identification	**10.3.1** Verify user identification is included in log entries.			
10.3.2 Type of event	**10.3.2** Verify type of event is included in log entries.			
10.3.3 Date and time	**10.3.3** Verify date and time stamp is included in log entries.			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
10.3.4 Success or failure indication	**10.3.4** Verify success or failure indication is included in log entries.			
10.3.5 Origination of event	**10.3.5** Verify origination of event is included in log entries.			
10.3.6 Identity or name of affected data, system component, or resource	**10.3.6** Verify identity or name of affected data, system component, or resources is included in log entries.			
10.4 Synchronize all critical system clocks and times.	**10.4** Obtain and review the process for acquiring and distributing the correct time within the organization, as well as the time-related system-parameter settings for a sample of system components. Verify the following is included in the process and implemented:			
	10.4.a Verify that a known, stable version of NTP (Network Time Protocol) or similar technology, kept current per PCI DSS Requirements 6.1 and 6.2, is used for time synchronization.			
	10.4.b Verify that internal servers are not all receiving time signals from external sources. [Two or three central time servers within the organization receive external time signals [directly from a special radio, GPS satellites, or other external sources based on International Atomic Time and UTC (formerly GMT)], peer with each other to keep accurate time, and share the time with other internal servers.]			
	10.4.c Verify that specific external hosts are designated from which the timeservers will accept NTP time updates (to prevent a malicious individual from changing the clock). Optionally, those updates can be encrypted with a symmetric key, and access control lists can be created that specify the IP addresses of client machines that will be provided with the NTP service (to prevent unauthorized use of internal time servers). See www.ntp.org for more information			
10.5 Secure audit trails so they cannot be altered.	**10.5** Interview system administrator and examine permissions to verify that audit trails are secured so that they cannot be altered as follows:			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
10.5.1 Limit viewing of audit trails to those with a job-related need.	**10.5.1** Verify that only individuals who have a job-related need can view audit trail files.			
10.5.2 Protect audit trail files from unauthorized modifications.	**10.5.2** Verify that current audit trail files are protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation.			
10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.	**10.5.3** Verify that current audit trail files are promptly backed up to a centralized log server or media that is difficult to alter.			
10.5.4 Write logs for external-facing technologies onto a log server on the internal LAN.	**10.5.4** Verify that logs for external-facing technologies (for example, wireless, firewalls, DNS, mail) are offloaded or copied onto a secure centralized internal log server or media.			
10.5.5 Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).	**10.5.5** Verify the use of file-integrity monitoring or change-detection software for logs by examining system settings and monitored files and results from monitoring activities.			
10.6 Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion-detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS). *Note: Log harvesting, parsing, and alerting tools may be used to meet compliance with Requirement 10.6*	**10.6.a** Obtain and examine security policies and procedures to verify that they include procedures to review security logs at least daily and that follow-up to exceptions is required.			
	10.6.b Through observation and interviews, verify that regular log reviews are performed for all system components.			
10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from back-up).	**10.7.a** Obtain and examine security policies and procedures and verify that they include audit log retention policies and require audit log retention for at least one year.			
	10.7.b Verify that audit logs are available for at least one year and processes are in place to restore at least the last three months' logs for immediate analysis.			

Requirement 11: Regularly test security systems and processes.

Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. System components, processes, and custom software should be tested frequently to ensure security controls continue to reflect a changing environment.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
11.1 Test for the presence of wireless access points by using a wireless analyzer at least quarterly or deploying a wireless IDS/IPS to identify all wireless devices in use.	**11.1.a** Verify that a wireless analyzer is used at least quarterly, or that a wireless IDS/IPS is implemented and configured to identify all wireless devices.			
	11.1.b If a wireless IDS/IPS is implemented, verify the configuration will generate alerts to personnel.			
	11.1 c Verify the organization's Incident Response Plan (Requirement 12.9) includes a response in the event unauthorized wireless devices are detected.			
11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades). *Note: Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV) qualified by Payment Card Industry Security Standards Council (PCI SSC). Scans conducted after network changes may be performed by the company's internal staff.*	**11.2.a** Inspect output from the most recent four quarters of internal network, host, and application vulnerability scans to verify that periodic security testing of the devices within the cardholder data environment occurs. Verify that the scan process includes rescans until passing results are obtained. *Note: External scans conducted after network changes, and internal scans, may be performed by the company's qualified internal personnel or third parties.*			
	11.2.b Verify that external scanning is occurring on a quarterly basis in accordance with the PCI Security Scanning Procedures, by inspecting output from the four most recent quarters of external vulnerability scans to verify that: ▪ Four quarterly scans occurred in the most recent 12-month period; ▪ The results of each scan satisfy the PCI Security Scanning Procedures (for example, no urgent, critical, or high vulnerabilities); ▪ The scans were completed by an Approved Scanning Vendor (ASV) qualified by PCI SSC. *Note: It is not required that four passing quarterly scans must be completed for initial PCI DSS compliance if the*			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
	assessor verifies 1) the most recent scan result was a passing scan, 2) the entity has documented policies and procedures requiring quarterly scanning, and 3) vulnerabilities noted in the scan results have been corrected as shown in a re-scan. For subsequent years after the initial PCI DSS review, four passing quarterly scans must have occurred.			
	11.2.c Verify that internal and/or external scanning is performed after any significant change in the network, by inspecting scan results for the last year. Verify that the scan process includes rescans until passing results are obtained.			
11.3 Perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). These penetration tests must include the following:	**11.3.a** Obtain and examine the results from the most recent penetration test to verify that penetration testing is performed at least annually and after any significant changes to the environment. Verify that noted vulnerabilities were corrected and testing repeated.			
	11.3.b Verify that the test was performed by a qualified internal resource or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).			
11.3.1 Network-layer penetration tests	**11.3.1** Verify that the penetration test includes network-layer penetration tests. These tests should include components that support network functions as well as operating systems.			
11.3.2 Application-layer penetration tests	**11.3.2** Verify that the penetration test includes application-layer penetration tests. For web applications, the tests should include, at a minimum, the vulnerabilities listed in Requirement 6.5.			
11.4 Use intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic in the cardholder data environment and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines up-to-date.	**11.4.a** Verify the use of intrusion-detection systems and/or intrusion-prevention systems and that all traffic in the cardholder data environment is monitored.			
	11.4.b Confirm IDS and/or IPS are configured to alert personnel of suspected compromises.			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
	11.4.c Examine IDS/IPS configurations and confirm IDS/IPS devices are configured, maintained, and updated per vendor instructions to ensure optimal protection.			
11.5 Deploy file-integrity monitoring software to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly. *Note: For file-integrity monitoring purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. File-integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider).*	**11.5** Verify the use of file-integrity monitoring products within the cardholder data environment by observing system settings and monitored files, as well as reviewing results from monitoring activities. Examples of files that should be monitored: ▪ System executables ▪ Application executables ▪ Configuration and parameter files ▪ Centrally stored, historical or archived, log and audit files			

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security for employees and contractors.

A strong security policy sets the security tone for the whole company and informs employees what is expected of them. All employees should be aware of the sensitivity of data and their responsibilities for protecting it. For the purposes of this requirement, "employees" refers to full-time and part-time employees, temporary employees and personnel, and contractors and consultants who are "resident" on the company's site.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
12.1 Establish, publish, maintain, and disseminate a security policy that accomplishes the following:	**12.1** Examine the information security policy and verify that the policy is published and disseminated to all relevant system users (including vendors, contractors, and business partners).			
12.1.1 Addresses all PCI DSS requirements.	**12.1.1** Verify that the policy addresses all PCI DSS requirements.			
12.1.2 Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment.	**12.1.2** Verify that the information security policy includes an annual risk assessment process that identifies threats, vulnerabilities, and results in a formal risk assessment.			
12.1.3 Includes a review at least once a year and updates when the environment changes.	**12.1.3** Verify that the information security policy is reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment.			
12.2 Develop daily operational security procedures that are consistent with requirements in this specification (for example, user account maintenance procedures, and log review procedures).	**12.2.a** Examine the daily operational security procedures. Verify that they are consistent with this specification, and include administrative and technical procedures for each of the requirements.			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
12.3 Develop usage policies for critical employee-facing technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, personal data/digital assistants (PDAs), e-mail usage and Internet usage) to define proper use of these technologies for all employees and contractors. Ensure these usage policies require the following:	**12.3** Obtain and examine the policy for critical employee-facing technologies and perform the following:			
12.3.1 Explicit management approval	**12.3.1** Verify that the usage policies require explicit management approval to use the technologies.			
12.3.2 Authentication for use of the technology	**12.3.2** Verify that the usage policies require that all technology use be authenticated with user ID and password or other authentication item (for example, token).			
12.3.3 A list of all such devices and personnel with access	**12.3.3** Verify that the usage policies require a list of all devices and personnel authorized to use the devices.			
12.3.4 Labeling of devices with owner, contact information, and purpose	**12.3.4** Verify that the usage policies require labeling of devices with owner, contact information, and purpose.			
12.3.5 Acceptable uses of the technology	**12.3.5** Verify that the usage policies require acceptable uses for the technology.			
12.3.6 Acceptable network locations for the technologies	**12.3.6** Verify that the usage policies require acceptable network locations for the technology.			
12.3.7 List of company-approved products	**12.3.7** Verify that the usage policies require a list of company-approved products.			
12.3.8 Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity	**12.3.8** Verify that the usage policies require automatic disconnect of sessions for remote-access technologies after a specific period of inactivity.			
12.3.9 Activation of remote-access technologies for vendors only when needed by vendors, with immediate deactivation after use	**12.3.9** Verify that the usage policies require activation of remote-access technologies used by vendors only when needed by vendors, with immediate deactivation after use.			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
12.3.10 When accessing cardholder data via remote-access technologies, prohibit copy, move, and storage of cardholder data onto local hard drives and removable electronic media.	**12.3.10** Verify that the usage policies prohibit copying, moving, or storing of cardholder data onto local hard drives, and removable electronic media when accessing such data via remote-access technologies.			
12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all employees and contractors.	**12.4** Verify that information security policies clearly define information security responsibilities for both employees and contractors.			
12.5 Assign to an individual or team the following information security management responsibilities:	**12.5** Verify the formal assignment of information security to a Chief Security Officer or other security-knowledgeable member of management. Obtain and examine information security policies and procedures to verify that the following information security responsibilities are specifically and formally assigned:			
12.5.1 Establish, document, and distribute security policies and procedures.	**12.5.1** Verify that responsibility for creating and distributing security policies and procedures is formally assigned.			
12.5.2 Monitor and analyze security alerts and information, and distribute to appropriate personnel.	**12.5.2** Verify that responsibility for monitoring and analyzing security alerts and distributing information to appropriate information security and business unit management personnel is formally assigned.			
12.5.3 Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.	**12.5.3** Verify that responsibility for creating and distributing security incident response and escalation procedures is formally assigned.			
12.5.4 Administer user accounts, including additions, deletions, and modifications	**12.5.4** Verify that responsibility for administering user account and authentication management is formally assigned.			
12.5.5 Monitor and control all access to data.	**12.5.5** Verify that responsibility for monitoring and controlling all access to data is formally assigned.			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
12.6 Implement a formal security awareness program to make all employees aware of the importance of cardholder data security.	**12.6.a** Verify the existence of a formal security awareness program for all employees.			
	12.6.b Obtain and examine security awareness program procedures and documentation and perform the following:			
12.6.1 Educate employees upon hire and at least annually.	**12.6.1.a** Verify that the security awareness program provides multiple methods of communicating awareness and educating employees (for example, posters, letters, memos, web based training, meetings, and promotions).			
	12.6.1.b Verify that employees attend awareness training upon hire and at least annually.			
12.6.2 Require employees to acknowledge at least annually that they have read and understood the company's security policy and procedures.	**12.6.2** Verify that the security awareness program requires employees to acknowledge (for example, in writing or electronically) at least annually that they have read and understand the company's information security policy.			
12.7 Screen potential employees (see definition of "employee" at 9.2 above) prior to hire to minimize the risk of attacks from internal sources. *For those employees such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.*	**12.7** Inquire with Human Resource department management and verify that background checks are conducted (within the constraints of local laws) on employees prior to hire who will have access to cardholder data or the cardholder data environment. (Examples of background checks include previous employment history, criminal record, credit history, and reference checks.)			
12.8 If cardholder data is shared with service providers, maintain and implement policies and procedures to manage service providers, to include the following:	**12.8** If the entity being assessed shares cardholder data with service providers (for example, back-up tape storage facilities, managed service providers such as Web hosting companies or security service providers, or those that receive data for fraud modeling purposes), through observation, review of policies and procedures, and review of supporting documentation, perform the following:			
12.8.1 Maintain a list of service providers.	**12.8.1** Verify that a list of service providers is maintained.			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
12.8.2 Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess.	**12.8.2** Verify that the written agreement includes an acknowledgement by the service providers of their responsibility for securing cardholder data.			
12.8.3 Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.	**12.8.3** Verify that policies and procedures are documented and were followed including proper due diligence prior to engaging any service provider.			
12.8.4 Maintain a program to monitor service providers' PCI DSS compliance status.	**12.8.4** Verify that the entity assessed maintains a program to monitor its service providers' PCI DSS compliance status.			
12.9 Implement an incident response plan. Be prepared to respond immediately to a system breach.	**12.9** Obtain and examine the Incident Response Plan and related procedures and perform the following:			

(12.9 continued on next page)

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
12.9.1 Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum: ▪ Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum ▪ Specific incident response procedures ▪ Business recovery and continuity procedures ▪ Data back-up processes ▪ Analysis of legal requirements for reporting compromises ▪ Coverage and responses of all critical system components ▪ Reference or inclusion of incident response procedures from the payment brands	**12.9.1** Verify that the Incident Response Plan includes: ▪ Roles, responsibilities, and communication strategies in the event of a compromise including notification of the payment brands, at a minimum ▪ Specific incident response procedures, ▪ Business recovery and continuity procedures, ▪ Data back-up processes ▪ Analysis of legal requirements for reporting compromises (for example, California Bill 1386 which requires notification of affected consumers in the event of an actual or suspected compromise for any business with California residents in their database) ▪ Coverage and responses for all critical system components ▪ Reference or inclusion of incident response procedures from the payment brands			
12.9.2 Test the plan at least annually.	**12.9.2** Verify that the plan is tested at least annually.			
12.9.3 Designate specific personnel to be available on a 24/7 basis to respond to alerts.	**12.9.3** Verify through observation and review of policies, that there is 24/7 incident response and monitoring coverage for any evidence of unauthorized activity, detection of unauthorized wireless access points, critical IDS alerts, and/or reports of unauthorized critical system or content file changes.			
12.9.4 Provide appropriate training to staff with security breach response responsibilities.	**12.9.4** Verify through observation and review of policies that staff with security breach responsibilities are periodically trained.			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
12.9.5 Include alerts from intrusion-detection, intrusion-prevention, and file-integrity monitoring systems.	**12.9.5** Verify through observation and review of processes that monitoring and responding to alerts from security systems including detection of unauthorized wireless access points are covered in the Incident Response Plan.			
12.9.6 Develop process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.	**12.9.6** Verify through observation and review of policies that there is a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.			

Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers

Requirement A.1: Shared hosting providers must protect the cardholder data environment

As referenced in Requirement 12.8, all service providers with access to cardholder data (including shared hosting providers) must adhere to the PCI DSS. In addition, Requirement 2.4 states that shared hosting providers must protect each entity's hosted environment and data. Therefore, shared hosting providers must additionally comply with the requirements in this Appendix.

Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
A.1 Protect each entity's (that is merchant, service provider, or other entity) hosted environment and data, per A.1.1 through A.1.4: A hosting provider must fulfill these requirements as well as all other relevant sections of the PCI DSS. *Note: Even though a hosting provider may meet these requirements, the compliance of the entity that uses the hosting provider is not guaranteed. Each entity* must *comply with the PCI DSS and validate compliance as applicable.*	**A.1** Specifically for a PCI DSS assessment of a shared hosting provider, to verify that shared hosting providers protect entities' (merchants and service providers) hosted environment and data, select a sample of servers (Microsoft Windows and Unix/Linux) across a representative sample of hosted merchants and service providers, and perform A.1.1 through A.1.4 below.			
A.1.1 Ensure that each entity only runs processes that have access to that entity's cardholder data environment.	**A.1.1** If a shared hosting provider allows entities (for example, merchants or service providers) to run their own applications, verify these application processes run using the unique ID of the entity. For example: ▪ No entity on the system can use a shared web server user ID. ▪ All CGI scripts used by an entity must be created and run as the entity's unique user ID.			

Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
A.1.2 Restrict each entity's access and privileges to own cardholder data environment only.	**A.1.2.a** Verify the user ID of any application process is not a privileged user (root/admin).			
	A.1.2.b Verify each entity (merchant, service provider) has read, write, or execute permissions only for files and directories it owns or for necessary system files (restricted via file system permissions, access control lists, chroot, jailshell, etc.). IMPORTANT: An entity's files may not be shared by group.			
	A.1.2.c Verify an entity's users do not have write access to shared system binaries.			
	A.1.2.d Verify that viewing of log entries is restricted to the owning entity.			
	A.1.2.e To ensure each entity cannot monopolize server resources to exploit vulnerabilities (for example, error, race, and restart conditions, resulting in, for example, buffer overflows), verify restrictions are in place for the use of these system resources: ▪ Disk space ▪ Bandwidth ▪ Memory ▪ CPU			
A.1.3 Ensure logging and audit trails are enabled and unique to each entity's cardholder data environment and consistent with PCI DSS Requirement 10.	**A.1.3.a** Verify the shared hosting provider has enabled logging as follows, for each merchant and service provider environment: ▪ Logs are enabled for common third-party applications. ▪ Logs are active by default. ▪ Logs are available for review by the owning entity. ▪ Log locations are clearly communicated to the owning entity.			
A.1.4 Enable processes to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider.	**A.1.4** Verify the shared hosting provider has written policies that provide for a timely forensics investigation of related servers in the event of a compromise.			

Appendix B: Compensating Controls

Compensating controls may be considered for most PCI DSS requirements when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of other, or compensating, controls.

Compensating controls must satisfy the following criteria:

1. Meet the intent and rigor of the original PCI DSS requirement.
2. Provide a similar level of defense as the original PCI DSS requirement, such that the compensating control sufficiently offsets the risk that the original PCI DSS requirement was designed to defend against. (See *Navigating PCI DSS* for the intent of each PCI DSS requirement.)
3. Be "above and beyond" other PCI DSS requirements. (Simply being in compliance with other PCI DSS requirements is not a compensating control.)

   When evaluating "above and beyond" for compensating controls, consider the following:

   Note: The items at a) through c) below are intended as examples only. All compensating controls must be reviewed and validated for sufficiency by the assessor who conducts the PCI DSS review. The effectiveness of a compensating control is dependent on the specifics of the environment in which the control is implemented, the surrounding security controls, and the configuration of the control. Companies should be aware that a particular compensating control will not be effective in all environments.

   a) Existing PCI DSS requirements CANNOT be considered as compensating controls if they are already required for the item under review. For example, passwords for non-console administrative access must be sent encrypted to mitigate the risk of intercepting clear-text administrative passwords. An entity cannot use other PCI DSS password requirements (intruder lockout, complex passwords, etc.) to compensate for lack of encrypted passwords, since those other password requirements do not mitigate the risk of interception of clear-text passwords. Also, the other password controls are already PCI DSS requirements for the item under review (passwords).

   b) Existing PCI DSS requirements MAY be considered as compensating controls if they are required for another area, but are not required for the item under review. For example, two-factor authentication is a PCI DSS requirement for remote access. Two-factor authentication *from within the internal network* can also be considered as a compensating control for non-console administrative access when transmission of encrypted passwords cannot be supported. Two-factor authentication may be an acceptable compensating control if; (1) it meets the intent of the original requirement by addressing the risk of intercepting clear-text administrative passwords; and (2) it is set up properly and in a secure environment.

   c) Existing PCI DSS requirements may be combined with new controls to become a compensating control. For example, if a company is unable to render cardholder data unreadable per requirement 3.4 (for example, by encryption), a compensating control could consist of a device or combination of devices, applications, and controls that address all of the following: (1) internal network segmentation; (2) IP address or MAC address filtering; and (3) two-factor authentication from within the internal network.

4. Be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement

The assessor is required to thoroughly evaluate compensating controls during each annual PCI DSS assessment to validate that each compensating control adequately addresses the risk the original PCI DSS requirement was designed to address, per items 1-4 above. To maintain compliance, processes and controls must be in place to ensure compensating controls remain effective after the assessment is complete.

Appendix C: Compensating Controls Worksheet

Use this worksheet to define compensating controls for any requirement where compensating controls are used to meet a PCI DSS requirement. Note that compensating controls should also be documented in the Report on Compliance in the corresponding PCI DSS requirement section.

***Note:** Only companies that have undertaken a risk analysis and have legitimate technological or documented business constraints can consider the use of compensating controls to achieve compliance.*

Requirement Number and Definition:

	Information Required	Explanation
1. Constraints	List constraints precluding compliance with the original requirement.	
2. Objective	Define the objective of the original control; identify the objective met by the compensating control.	
3. Identified Risk	Identify any additional risk posed by the lack of the original control.	
4. Definition of Compensating Controls	Define the compensating controls and explain how they address the objectives of the original control and the increased risk, if any.	
5. Validation of Compensating Controls	Define how the compensating controls were validated and tested.	
6. Maintenance	Define process and controls in place to maintain compensating controls.	

Compensating Controls Worksheet – Completed Example

Use this worksheet to define compensating controls for any requirement where "YES" was checked and compensating controls were mentioned in the "Special" column.

Requirement Number: *8.1—Are all users identified with a unique user name before allowing them to access system components or cardholder data?*

	Information Required	Explanation
1. Constraints	List constraints precluding compliance with the original requirement.	*Company XYZ employs stand-alone Unix Servers without LDAP. As such, they each require a "root" login. It is not possible for Company XYZ to manage the "root" login nor is it feasible to log all "root" activity by each user.*
2. Objective	Define the objective of the original control; identify the objective met by the compensating control.	*The objective of requiring unique logins is twofold. First, it is not considered acceptable from a security perspective to share login credentials. Secondly, having shared logins makes it impossible to state definitively that a person is responsible for a particular action.*
3. Identified Risk	Identify any additional risk posed by the lack of the original control.	*Additional risk is introduced to the access control system by not ensuring all users have a unique ID and are able to be tracked.*
4. Definition of Compensating Controls	Define the compensating controls and explain how they address the objectives of the original control and the increased risk, if any.	*Company XYZ is going to require all users to log into the servers from their desktops using the SU command. SU allows a user to access the "root" account and perform actions under the "root" account but is able to be logged in the SU-log directory. In this way, each user's actions can be tracked through the SU account.*
5. Validation of Compensating Controls	Define how the compensating controls were validated and tested.	*Company XYZ demonstrates to assessor that the SU command being executed and that those individuals utilizing the command are logged to identify that the individual is performing actions under root privileges*
6. Maintenance	Define process and controls in place to maintain compensating controls.	*Company XYZ documents processes and procedures to ensure SU configurations are not changed, altered, or removed to allow individual users to execute root commands without being individually tracked or logged*

Appendix D: Attestation of Compliance – Merchants

Payment Card Industry (PCI)
Data Security Standard

Attestation of Compliance for Onsite Assessments – Merchants

Version 1.2

October 2008

Instructions for Submission

This document must be completed by a Qualified Security Assessor (QSA) or merchant (if merchant internal audit performs validation) as a declaration of the merchant's compliance status with the Payment Card Industry Data Security Standard (PCI DSS). Complete all applicable sections and submit to the acquirer or requesting payment brand.

Part 1. Qualified Security Assessor Company Information

Company Name:					
Lead QSA Contact Name:			Title:		
Telephone:			E-mail:		
Business Address:			City:		
State/Province:		Country:		ZIP:	
URL:					

Part 2. Merchant Organization Information

Company Name:			DBA(s):		
Contact Name:			Title:		
Telephone:			E-mail:		
Business Address:			City:		
State/Province:		Country:		ZIP:	
URL:					

Part 2a. Type of Merchant Business (check all that apply)

☐ Retailer ☐ Telecommunication ☐ Grocery and Supermarkets

☐ Petroleum ☐ E-Commerce ☐ Mail/Telephone-Order

☐ Travel & Entertainment ☐ Others (please specify):

List facilities and locations included in PCI DSS review:

Part 2b. Relationships

Does your company have a relationship with one or more third-party agents (for example, gateways, web-hosting companies, airline booking agents, loyalty program agents, etc)? ☐ Yes ☐ No

Does your company have a relationship with more than one acquirer? ☐ Yes ☐ No

Part 2c. Transaction Processing

Payment Application in use: Payment Application Version:

Part 3. PCI DSS Validation

Based on the results noted in the Report on Compliance ("ROC") dated *(date of ROC)*, *(QSA Name/Merchant Name)* asserts the following compliance status for the entity identified in Part 2 of this document as of *(date)* (check one):

☐ **Compliant:** All requirements in the ROC are marked "in place[4]," and a passing scan has been completed by the PCI SSC Approved Scanning Vendor *(ASV Name)* thereby *(Merchant Company Name)* has demonstrated full compliance with the PCI DSS *(insert version number).*

☐ **Non-Compliant:** Some requirements in the ROC are marked "not in place," resulting in an overall **NON-COMPLIANT** rating, **or** a passing scan has not been completed by a PCI SSC Approved Scanning Vendor, thereby *(Merchant Company Name)* has not demonstrated full compliance with the PCI DSS.

Target Date for Compliance:

An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. *Check with your acquirer or the payment brand(s) before completing Part 4, since not all payment brands require this section.*

Part 3a. Confirmation of Compliant Status

QSA/Merchant confirms:

☐	The ROC was completed according to the *PCI DSS Requirements and Security Assessment Procedures*, Version *(insert version number)*, and was completed according to the instructions therein.
☐	All information within the above-referenced ROC and in this attestation fairly represents the results of the assessment in all material respects.
☐	The merchant has confirmed with the payment application vendor that their payment application does not store sensitive authentication data after authorization.
☐	The merchant has read the PCI DSS and recognizes that they must maintain full PCI DSS compliance at all times.
☐	No evidence of magnetic stripe (i.e., track) data[5], CAV2, CVC2, CID, or CVV2 data[6], or PIN data[7] storage after transaction authorization was found on ANY systems reviewed during this assessment.

Part 3b. QSA and Merchant Acknowledgments

Signature of Lead QSA ↑	***Date:***
Lead QSA Name:	***Title:***

Signature of Merchant Executive Officer ↑	***Date:***
Merchant Executive Officer Name:	***Title:***

[4] "In place" results should include compensating controls reviewed by the QSA/merchant Internal Audit. If compensating controls are determined to sufficiently mitigate the risk associated with the requirement, the QSA should mark the requirement as "in place".

[5] Data encoded in the magnetic stripe used for authorization during a card-present transaction. Entities may not retain full magnetic stripe data after transaction authorization. The only elements of track data that may be retained are account number, expiration date, and name.

[6] The three- or four-digit value printed on the signature panel or face of a payment card used to verify card-not-present transactions.

[7] Personal Identification Number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.

Part 4. Action Plan for Non-Compliant Status

Please select the appropriate "Compliance Status" for each requirement. If you answer "No" to any of the requirements, you are required to provide the date Company will be compliant with the requirement and a brief description of the actions being taken to meet the requirement. *Check with your acquirer or the payment brand(s) before completing Part 4 since not all payment brands require this section.*

PCI Requirement	Description	Compliance Status (Select One)	Remediation Date and Actions (if Compliance Status is "No")
1	Install and maintain a firewall configuration to protect cardholder data.	☐ Yes ☐ No	
2	Do not use vendor-supplied defaults for system passwords and other security parameters.	☐ Yes ☐ No	
3	Protect stored cardholder data.	☐ Yes ☐ No	
4	Encrypt transmission of cardholder data across open, public networks.	☐ Yes ☐ No	
5	Use and regularly update anti-virus software.	☐ Yes ☐ No	
6	Develop and maintain secure systems and applications.	☐ Yes ☐ No	
7	Restrict access to cardholder data by business need to know.	☐ Yes ☐ No	
8	Assign a unique ID to each person with computer access.	☐ Yes ☐ No	
9	Restrict physical access to cardholder data.	☐ Yes ☐ No	
10	Track and monitor all access to network resources and cardholder data.	☐ Yes ☐ No	
11	Regularly test security systems and processes.	☐ Yes ☐ No	
12	Maintain a policy that addresses information security.	☐ Yes ☐ No	

Appendix E: Attestation of Compliance – Service Providers

Payment Card Industry (PCI)
Data Security Standard

Attestation of Compliance for Onsite Assessments – Service Providers

Version 1.2

October 2008

Instructions for Submission

The Qualified Security Assessor (QSA) and Service Provider must complete this document as a declaration of the Service Provider's compliance status with the Payment Card Industry Data Security Standard (PCI DSS). Complete all applicable sections and submit to the requesting payment brand.

Part 1. Qualified Security Assessor Company Information					
Company Name:					
Lead QSA Contact Name:			Title:		
Telephone:			E-mail:		
Business Address:			City:		
State/Province:		Country:		ZIP:	
URL:					

Part 2. Service Provider Organization Information					
Company Name:			DBA(s):		
Contact Name:			Title:		
Telephone:			E-mail:		
Business Address:			City:		
State/Province:		Country:		ZIP:	
URL:					

Part 2a. Services Provided (check all that apply)

☐ Authorization	☐ Loyalty Programs	☐ 3-D Secure Access Control Server
☐ Switching	☐ IPSP (E-commerce)	☐ Process Magnetic-Stripe Transactions
☐ Payment Gateway	☐ Clearing & Settlement	☐ Process MO/TO Transactions
☐ Hosting	☐ Issuing Processing	☐ Others (please specify):

List facilities and locations included in PCI DSS review:

Part 2b. Relationships

Does your company have a relationship with one or more third-party service providers (for example, gateways, web-hosting companies, airline booking agents, loyalty program agents, etc)? ☐ Yes ☐ No

Part 2c. Transaction Processing

How and in what capacity does your business store, process and/or transmit cardholder data?

Payment Application in use: *Payment Application Version:*

Part 3. PCI DSS Validation

Based on the results noted in the Report on Compliance ("ROC") dated *(date of ROC)*, *(QSA Name)* asserts the following compliance status for the entity identified in Part 2 of this document as of *(date)* (check one):

☐ **Compliant:** All requirements in the ROC are marked "in place[8]," and a passing scan has been completed by the PCI SSC Approved Scanning Vendor *(ASV Name)* thereby *(Service Provider Name)* has demonstrated full compliance with the PCI DSS *(insert version number).*

☐ **Non-Compliant:** Some requirements in the ROC are marked "not in place," resulting in an overall **NON-COMPLIANT** rating, **or** a passing scan has not been completed by a PCI SSC Approved Scanning Vendor, thereby *(Service Provider Name)* has not demonstrated full compliance with the PCI DSS.

Target Date for Compliance:

An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. *Check with the payment brand(s) before completing Part 4, since not all payment brands require this section.*

Part 3a. Confirmation of Compliant Status

QSA and Service Provider confirm:

☐	The ROC was completed according to the *PCI DSS Requirements and Security Assessment Procedures*, Version *(insert version number)*, and was completed according to the instructions therein.
☐	All information within the above-referenced ROC and in this attestation fairly represents the results of the assessment in all material respects.
☐	The Service Provider has read the PCI DSS and recognizes that they must maintain full PCI DSS compliance at all times.
☐	No evidence of magnetic stripe (i.e., track) data[9], CAV2, CVC2, CID, or CVV2 data[10], or PIN data[11] storage after transaction authorization was found on ANY systems reviewed during this assessment.

Part 3b. QSA and Service Provider Acknowledgments

Signature of Lead QSA ↑	***Date:***
Lead QSA Name:	***Title:***

Signature of Service Provider Executive Officer ↑	***Date:***
Service Provider Executive Officer Name:	***Title:***

[8] "In place" results should include compensating controls reviewed by the QSA. If compensating controls are determined to sufficiently mitigate the risk associated with the requirement, the QSA should mark the requirement as "in place".

[9] Data encoded in the magnetic stripe used for authorization during a card-present transaction. Entities may not retain full magnetic stripe data after transaction authorization. The only elements of track data that may be retained are account number, expiration date, and name.

[10] The three- or four-digit value printed on the signature panel or face of a payment card used to verify card-not-present transactions.

[11] Personal Identification Number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.

Part 4. Action Plan for Non-Compliant Status

Please select the appropriate "Compliance Status" for each requirement. If you answer "No" to any of the requirements, you are required to provide the date Company will be compliant with the requirement and a brief description of the actions being taken to meet the requirement. *Check with the payment brand(s) before completing Part 4 since not all payment brands require this section.*

PCI Requirement	Description	Compliance Status (Select One)	Remediation Date and Actions (if Compliance Status is "No")
1	Install and maintain a firewall configuration to protect cardholder data.	☐ Yes ☐ No	
2	Do not use vendor-supplied defaults for system passwords and other security parameters.	☐ Yes ☐ No	
3	Protect stored cardholder data.	☐ Yes ☐ No	
4	Encrypt transmission of cardholder data across open, public networks.	☐ Yes ☐ No	
5	Use and regularly update anti-virus software.	☐ Yes ☐ No	
6	Develop and maintain secure systems and applications.	☐ Yes ☐ No	
7	Restrict access to cardholder data by business need to know.	☐ Yes ☐ No	
8	Assign a unique ID to each person with computer access.	☐ Yes ☐ No	
9	Restrict physical access to cardholder data.	☐ Yes ☐ No	
10	Track and monitor all access to network resources and cardholder data.	☐ Yes ☐ No	
11	Regularly test security systems and processes.	☐ Yes ☐ No	
12	Maintain a policy that addresses information security.	☐ Yes ☐ No	

Appendix F: PCI DSS Reviews — Scoping and Selecting Samples