PCI Questionnaire Report

Summary

Company Name: FLAGSTAFF CHILD AND FAM

DBA:

Self-Assessment Questionnaire: PCI SAQ C 3.2

Questionnaire Date: 2017-04-18

PCI Questionnaire Compliance: COMPLIANT

(PCI Annual Self-Assessment Questionnaire ONLY)

Question(s) Compliant: 173

Question(s) Non-Compliant: 0

By signing below, the client attests that this questionnaire was completed accurately and completely, reflecting all systems, processes and facilities considered in-scope for the PCI DSS.

Signature

Date

Printed Name

Title

Eligibility

Status	Item	Question	Your Response	Remediation
	Merchant certifies eligibility to complete this shortened version of the Self-Assessment Questionnaire because, for this payment channel:			
	E.15	Merchant does not store cardholder data in electronic format; and	Yes	
	E.16	If Merchant does store cardholder data, such data is only paper reports or copies of paper receipts and is not received electronically.	Yes	
	E.30	Merchant has a payment application system and an Internet connection on the same device and/or same local area network (LAN);	Yes	
	E.31	The payment application system/Internet device is not connected to any other system within the merchant environment;	Yes	
	E.32	The physical location of the POS environment is not connected to other premises or locations, and any LAN is for a single location only;	Yes	

Firewall Configuration

Status	Item	Question	Your Response	Remediation
	Do firewall and router configurations restrict connections between untrusted networks and any system 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 (a)	Is inbound and outbound traffic restricted to that which is necessary for the cardholder data environment?	Yes	
	1.2.1 (b)	Is all other inbound and outbound traffic specifically denied (for example by using an explicit "deny all" or an implicit deny after allow statement)?	Yes	
	1.2.3	Are perimeter firewalls installed between all wireless networks and the cardholder data environment, and are these firewalls configured to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment?	Yes	
	Is direct public access prohibited between the Internet and any system component in the cardholder data environment, as follows:			
	1.3.4	Is outbound traffic from the cardholder data environment to the Internet explicitly authorized?	Yes	
	1.3.5	Are only established connections permitted into the network?	Yes	

System Settings				
Status	**Item**	**Question**	**Your Response**	**Remediation**
	2.1 (a)	Are vendor-supplied defaults always changed before installing a system on the network? *This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, Simple Network Management Protocol (SNMP) community strings, etc.).*	Yes	
	2.1 (b)	Are unnecessary default accounts removed or disabled before installing a system on the network?	Yes	
	For wireless environments connected to the cardholder data environment or transmitting cardholder data, are ALL wireless vendor defaults changed at installations, as follows:			
	2.1.1 (a)	Are encryption keys changed from default at installation, and changed anytime anyone with knowledge of the keys leaves the company or changes positions?	Yes	
	2.1.1 (b)	Are default SNMP community strings on wireless devices changed at installation?	Yes	
	2.1.1 (c)	Are default passwords/passphrases on access points changed at installation?	Yes	
	2.1.1 (d)	Is firmware on wireless devices updated to support strong encryption for authentication and transmission over wireless networks?	Yes	
	2.1.1 (e)	Are other security-related wireless vendor defaults changed, if applicable?	Yes	

Status	Item	Question	Your Response	Remediation
	2.2 (a)	Are configuration standards developed for all system components and are they consistent with industry-accepted system hardening standards? *Sources of industry-accepted system hardening standards may include, but are not limited to, SysAdmin Audit Network Security (SANS) Institute, National Institute of Standards Technology (NIST), International Organization for Standardization (ISO), and Center for Internet Security (CIS).*	Yes	
	2.2 (b)	Are system configuration standards updated as new vulnerability issues are identified, as defined in Requirement 6.1?	Yes	
	2.2 (c)	Are system configuration standards applied when new systems are configured?	Yes	
	2.2 (d)	Do system configuration standards include all of the following: • Changing of all vendor-supplied defaults and elimination of unnecessary default accounts? • Implementing only one primary function per server to prevent functions that require different security levels from co -existing on the same server? • Enabling only necessary services, protocols, daemons, etc., as required for the function of the system? • Implementing additional security features for any required services, protocols or daemons that are considered to be insecure? • Configuring system security parameters to prevent misuse? • Removing all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers?	Yes	
	2.2.1 (a)	Is only one primary function implemented per server, to prevent functions that require different security levels from co-existing on the same server? *For example, web servers, database servers, and DNS should be implemented on separate servers.*	Yes	

Status	Item	Question	Your Response	Remediation
	2.2.1 (b)	If virtualization technologies are used, is only one primary function implemented per virtual system component or device?	Yes	
	2.2.2 (a)	Are only necessary services, protocols, daemons, etc. enabled as required for the function of the system (services and protocols not directly needed to perform the device's specified function are disabled)?	Yes	
	2.2.2 (b)	Are all enabled insecure services, daemons, or protocols justified per documented configuration standards?	Yes	
	2.2.3	Are additional security features documented and implemented for any required services, protocols or daemons that are considered to be insecure? *NOTE: Where SSL/early TLS is used, the requiements in Appendix A2 must be completed.*	Yes	
	2.2.4 (a)	Are system administrators and/or personnel that configure system components knowledgeable about common security parameter settings for those system components?	Yes	
	2.2.4 (b)	Are common system security parameters settings included in the system configuration standards?	Yes	
	2.2.4 (c)	Are security parameter settings set appropriately on system components?	Yes	
	2.2.5 (a)	Has all unnecessary functionality--such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers--been removed?	Yes	

Status	Item	Question	Your Response	Remediation
	2.2.5 (b)	Are enabled functions documented and do they support secure configuration?	Yes	
	2.2.5 (c)	Is only documented functionality present on system components?	Yes	
	Is non-console administrative access encrypted as follows: ***Note:*** *Where SSL/early TLS is used, the requirements in Appendix A2 must be completed*			
	2.3 (a)	Is all non-console administrative access encrypted with strong cryptography, and is a strong encryption method invoked before the administrator's password is requested?	Yes	
	2.3 (b)	Are system services and parameter files configured to prevent the use of Telnet and other insecure remote login commands?	Yes	
	2.3 (c)	Is administrator access to web-based management interfaces encrypted with strong cryptography?	Yes	
	2.3 (d)	For the technology in use, is strong cryptography implemented according to industry best practice and/or vendor recommendations?	Yes	
	2.5	Are security policies and operational procedures for managing vendor defaults and other security parameters: • Documented • In use • Known to all affected parties?	Yes	

Stored Data Protection				
Status	**Item**	**Question**	**Your Response**	**Remediation**
	3.2 (c)	Is sensitive authentication data deleted or rendered unrecoverable upon completion of the authorization process?	Yes	
	Do all systems adhere to the following requirements regarding non-storage of sensitive authentication data after authorization (even if encrypted):			
	3.2.1	The full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere) are not stored after authorization? *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.*	Yes	
	3.2.2	The card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) is not stored after authorization?	Yes	
	3.2.3	The personal identification number (PIN) or the encrypted PIN block is not stored after authorization?	Yes	
	3.3	Is the PAN masked when displayed (the first six and last four digits are the maximum number of digits to be displayed) such that only personnel with a legitimate business need can see the more than the first six/last four digits of the PAN? *Note: This requirement does not supersede stricter requirements in place for displays of cardholder data--for example, legal or payment card brand requirements for point-of-sale (POS) receipts.*	Yes	

Transmitted Data Protection

Status	Item	Question	Your Response	Remediation
	4.1 (a)	Are strong cryptography and security protocols, such as TLS, SSH or IPSEC, used to safeguard sensitive cardholder data during transmission over open, public networks? **Note:** Where SSL/early TLS is used, the requirements in Appendix A2 must be completed. *Examples of open, public networks include but are not limited to the Internet; wireless technologies, including 802.11 and Bluetooth; cellular technologies, for example, Global System for Mobile communications (GSM), Code division multiple access (CDMA); and General Packet Radio Service (GPRS).*	Yes	
	4.1 (b)	Are only trusted keys and/or certificates accepted?	Yes	
	4.1 (c)	Are security protocols implemented to use only secure configurations, and to not support insecure versions or configurations?	Yes	
	4.1 (d)	Is the proper encryption strength implemented for the encryption methodology in use (check vendor recommendations/best practices)?	Yes	
	4.1 (e)	For SSL/TLS implementations, is SSL/TLS enabled whenever cardholder data is transmitted or received? For example, for browser-based implementations: • "HTTPS" appears as the browser Universal Record Locator (URL) protocol, and • Cardholder data is only requested if "HTTPS" appears as part of the URL.	Yes	
	4.1.1	Are industry best practices used to implement strong encryption for authentication and transmission for wireless networks transmitting cardholder data or connected to the cardholder data environment?	Yes	

Questionnaire Date: 2017-04-18

Status	Item	Question	Your Response	Remediation
	4.2 (b)	Are policies in place that state that unprotected PANs are not to be sent via end-user messaging technologies?	Yes	

Anti-Virus Protection

Status	Item	Question	Your Response	Remediation
	5.1	Is anti-virus software deployed on all systems commonly affected by malicious software?	Yes	
	5.1.1	Are anti-virus programs capable of detecting, removing, and protecting against all known types of malicious software (for example, viruses, Trojans, worms, spyware, adware, and rootkits)?	Yes	
	5.1.2	Are periodic evaluations performed to identify and evaluate evolving malware threats in order to confirm whether those systems considered to not be commonly affected by malicious software continue as such?	Yes	
	Are all anti-virus mechanisms maintained as follows:			
	5.2 (a)	Are all anti-virus software and definitions kept current?	Yes	
	5.2 (b)	Are automatic updates and periodic scans enabled and being performed?	Yes	
	5.2 (c)	Are all anti-virus mechanisms generating audit logs, and are logs retained in accordance with PCI DSS Requirement 10.7?	Yes	
	5.3	Are all anti-virus mechanisms: • Actively running? • Unable to be disabled or altered by users? *Note: Anti-virus solutions may be temporarily disabled only if there is legitimate technical need, as authorized by management on a case-by-case basis. If anti-virus protection needs to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period of time during which anti-virus protection is not active.*	Yes	

Application and Systems Security				
Status	**Item**	**Question**	**Your Response**	**Remediation**
	6.1	Is there a process to identify security vulnerabilities, including the following: • Using reputable outside sources for vulnerability information ? • Assigning a risk ranking to vulnerabilities that includes identification of all "high" risk and "critical" vulnerabilities? *Note: Risk rankings should be based on industry best practices as well as consideration of potential impact. For example, criteria for ranking vulnerabilities may include consideration of the CVSS base score and/or the classification by the vendor, and/or type of systems affected.* *Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization's environment and risk assessment strategy. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a "high risk" to the environment. In addition to the risk ranking, vulnerabilities may be considered "critical" if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed. Examples of critical systems may include security systems, public-facing devices and systems, databases, and other systems that store, process or transmit cardholder data.*	Yes	
	6.2 (a)	Are all system components and software protected from known vulnerabilities by installing applicable vendor-supplied security patches?	Yes	
	6.2 (b)	Are critical security patches installed within one month of release? *Note: Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1.*	Yes	
	Are change control processes and procedures followed for all changes to system components to include the following:			
	6.4.6	Upon completion of a significant change, are all relevant PCI DSS requirements implemented on all new or changed systems and networks, and documentation updated as applicable ***Note:****This requirement is a best practice until January 31, 2018, after which it becomes a requirement.*	Yes	

Access Restrictions				
Status	**Item**	**Question**	**Your Response**	**Remediation**
	Is access to system components and cardholder data limited to only those individuals whose jobs require such access, as follows:			
	7.1.2	Is access to privileged user IDs restricted as follows: • To least privileges necessary to perform job responsibilities? • Assigned only to roles that specifically require that privileged access?	Yes	
	7.1.3	Is access assigned based on individual personnel's job classification and function?	Yes	

Account Security

Status	Item	Question	Your Response	Remediation
	Are policies and procedures for user identification management controls defined and in place for non-consumer users and administrators on all system components, as follows:			
	8.1.1	Are all users assigned a unique ID before allowing them to access system components or cardholder data?	Yes	
	8.1.5 (a)	Are accounts used by third parties to access, support, or maintain system components via remote access enabled only during the time period needed and disabled when not in use?	Yes	
	8.1.5 (b)	Are third party remote access accounts monitored when in use?	Yes	
	8.1.6 (a)	Are repeated access attempts limited by locking out the user ID after no more than six attempts?	Yes	
	8.1.7	Once a user account is locked out, is the lockout duration set to a minimum of 30 minutes or until an administrator enables the user ID?	Yes	
	8.1.8	If a session has been idle for more than 15 minutes, are users required to re-authenticate (for example, re-enter the password) to re-activate the terminal or session?	Yes	
	8.2	In addition to assigning a unique ID, is one or more of the following methods employed to authenticate all users? • Something you know, such as a password or passphrase • Something you have, such as a token device or smart card • Something you are, such as a biometric	Yes	

Status	Item	Question	Your Response	Remediation
	8.2.3 (a)	Are user password parameters configured to require passwords/ passphrases meet the following? • A minimum password length of at least seven characters • Contain both numeric and alphabetic characters Alternatively, the passwords/passphrases must have complexity and strength at least equivalent to the parameters specified above.	Yes	
	8.2.4 (a)	Are user passwords/passphrases changed at least once every 90 days?	Yes	
	8.2.5 (a)	Must an individual submit a new password/passphrase that is different from any of the last four passwords/passphrases he or she has used?	Yes	
	8.2.6	Are passwords/passphrases set to a unique value for each user for first-time use and upon reset, and must each user change their password immediately after the first use?	Yes	
	Is all individual non-console administrative access and all remote access to the CDE secured using multi-factor authentication as follows: ***Note:*** *Multi-factor authentication requires that a minimum of two of the three authentication methods (see PCI DSS Requiremetn 8.2 for descriptions of authentication methods) be used for authentiction. Using one factor twice (for example, using two separate passwords) is not considered multi-factor authentication*			
	8.3.1	Is multi-factor authentication incorporated for all non-console access into the CDE for personnel with administrative access? *Note: This requirement is a best practice until January 31, 2018 after which it becomes a requirement.*	Yes	
	8.3.2	Is multi-factor authentication incorporated for all remote network access (both user and administrator, and including third party access for support or maintenance) originating from outside the entity's network?	Yes	
	8.4 (a)	Are authentication procedures and policies documented and communicated to all users?	Yes	

Questionnaire Date: 2017-04-18

Status	Item	Question	Your Response	Remediation
	8.4 (b)	Do authentication procedures and policies include the following? • Guidance on selecting strong authentication credentials • Guidance for how users should protect their authentication credentials • Instructions not to reuse previously used passwords • Instructions that users should change passwords if there is any suspicion the password could be compromised	Yes	
	8.5	Are group, shared, or generic accounts, passwords, or other authentication methods prohibited as follows: • Generic user IDs and accounts are disabled or removed; • Shared user IDs for system administration activities and other critical functions do not exist; and • Shared and generic user IDs are not used to administer any system components?	Yes	
	8.8	Are security policies and operational procedures for identification and authentication: • Documented • In use • Known to all affected parties?	Yes	

Physical Access Controls

Status	Item	Question	Your Response	Remediation
	9.1	Are appropriate facility entry controls in place to limit and monitor physical access to systems in the cardholder data environment?	Yes	
	9.1.1 (a)	Are either video cameras or access-control mechanisms (or both) in place to monitor individual physical access to sensitive areas? *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 public-facing areas where only point-of-sale terminals are present such as the cashier areas in a retail store.*	Yes	
	9.1.1 (b)	Are either video cameras or access-control mechanisms (or both) protected from tampering or disabling?	Yes	
	9.1.1 (c)	Is data collected from video cameras and/or access control mechanisms reviewed and correlated with other entries?	Yes	
	9.1.1 (d)	Is data collected from video cameras and/or access control mechanisms stored for at least three months unless otherwise restricted by law?	Yes	
	9.1.2	Are physical and/or logical controls in place to restrict access to publicly accessible network jacks? *For example, network jacks located in public areas and areas accessible to visitors could be disabled and only enabled when network access is explicitly authorized. Alternatively, processes could be implemented to ensure that visitors are escorted at all times in areas with active network jacks.*	Yes	

Status	Item	Question	Your Response	Remediation
	9.5	Are all media physically secured (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes)? *For purposes of Requirement 9, "media" refers to all paper and electronic media containing cardholder data.*	Yes	
	9.6 (a)	Is strict control maintained over the internal or external distribution of any kind of media?	Yes	
	Do controls include the following:			
	9.6.1	Is media classified so the sensitivity of the data can be determined ?	Yes	
	9.6.2	Is media sent by secured courier or other delivery method that can be accurately tracked?	Yes	
	9.6.3	Is management approval obtained prior to moving the media (especially when media is distributed to individuals)?	Yes	
	9.7	Is strict control maintained over the storage and accessibility of media?	Yes	
	9.8 (a)	Is all media destroyed when it is no longer needed for business or legal reasons?	Not Applicable Comment : My business does not store credit card data in any form, either electronic or paper documents or receipts.	

Status	Item	Question	Your Response	Remediation
	Is media destruction performed as follows:			
✓	9.8.1 (a)	Are hardcopy materials cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed?	Not Applicable Comment : My business does not store credit card data in any form, either electronic or paper documents or receipts.	
✓	9.8.1 (b)	Are storage containers used for materials that contain information to be destroyed secured to prevent access to the contents?	Not Applicable Comment : My business does not store credit card data in any form, either electronic or paper documents or receipts.	
	Are devices that capture payment card data via direct physical interaction with the card protected against tampering and substitution as follows? *Note: This requirement applies to card-reading devices used in card-present transactions (that is, card swipe or dip) at the point of sale. This requirement is not intended to apply to manual key-entry components such as computer keyboards and POS keypads.* *Note: Requirement 9.9 is a best practice until June 30, 2015, after which it becomes a requirement.*			
✓	9.9 (a)	Do policies and procedures require that a list of such devices be maintained?	Yes	
✓	9.9 (b)	Do policies and procedures require that devices are periodically inspected to look for tampering or substitution?	Yes	
✓	9.9 (c)	Do policies and procedures require that personnel are trained to be aware of suspicious behavior and to report tampering or substitution of devices?	Yes	
✓	9.9.1 (a)	Does the list of devices include the following? • Make, model of device • Location of device (for example, the address of the site or facility where the device is located) • Device serial number or other method of unique identification	Yes	

Status	Item	Question	Your Response	Remediation
	9.9.1 (b)	Is the list accurate and up to date?	Yes	
	9.9.1 (c)	Is the list of devices updated when devices are added, relocated, decommissioned, etc.?	Yes	
	9.9.2 (a)	Are device surfaces periodically inspected to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device) as follows? *Note: Examples of signs that a device might have been tampered with or substituted include unexpected attachments or cables plugged into the device, missing or changed security labels, broken or differently colored casing, or changes to the serial number or other external markings.*	Yes	
	9.9.2 (b)	Are personnel aware of procedures for inspecting devices?	Yes	
	Are personnel trained to be aware of attempted tampering or replacement of devices, to include the following?			
	9.9.3 (a)	Do training materials for personnel at point-of-sale locations include the following? • Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. • Do not install, replace, or return devices without verification. • Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). • Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).	Yes	

Questionnaire Date: 2017-04-18

Status	Item	Question	Your Response	Remediation
	9.9.3 (b)	Have personnel at point-of-sale locations received training, and are they aware of procedures to detect and report attempted tampering or replacement of devices?	Yes	

Access Tracking

Status	Item	Question	Your Response	Remediation
	Are automated audit trails implemented for all system components to reconstruct the following events:			
✓	10.2.2	All actions taken by any individual with root or administrative privileges?	Yes	
✓	10.2.4	Invalid logical access attempts?	Yes	
✓	10.2.5	Use of and changes to identification and authentication mechanisms-including but not limited to creation of new accounts and elevation of privileges - and all changes, additions, or deletions to accounts with root or administrative privileges?	Yes	
	Are the following audit trail entries recorded for all system components for each event:			
✓	10.3.1	User identification?	Yes	
✓	10.3.2	Type of event?	Yes	
✓	10.3.3	Date and time?	Yes	
✓	10.3.4	Success or failure indication?	Yes	

Status	Item	Question	Your Response	Remediation
	10.3.5	Origination of event?	Yes	
	10.3.6	Identity or name of affected data, system component, or resource?	Yes	
	Are logs and security events for all system components reviewed to identify anomalies or suspicious activity as follows? Note: Log harvesting, parsing, and alerting tools may be used to achieve compliance with Requirement 10.6.			
	10.6.1 (b)	Are the above logs and security events reviewed at least daily?	Yes	
	10.6.2 (b)	Are reviews of all other system components performed in accordance with organization's policies and risk management strategy?	Yes	
	10.6.3 (b)	Is follow up to exceptions and anomalies identified during the review process performed?	Yes	
	10.7 (b)	Are audit logs retained for at least one year?	Yes	
	10.7 (c)	Are at least the last three months' logs immediately available for analysis?	Yes	

Monitoring and Testing

Status	Item	Question	Your Response	Remediation
	11.1 (a)	Are processes implemented for detection and identification of both authorized and unauthorized wireless access points on a quarterly basis? *Note: Methods that may be used in the process include, but are not limited to, wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS.* *Whichever methods are used, they must be sufficient to detect and identify any unauthorized devices.*	Yes	
	11.1 (b)	Does the methodology detect and identify any unauthorized wireless access points, including at least the following? • WLAN cards inserted into system components; • Portable or mobile devices attached to system components to create a wireless access point (for example, by USB, etc.); and • Wireless devices attached to a network port or network device.	Yes	
	11.1 (c)	Is the scan to identify authorized and unauthorized wireless access points performed at least quarterly for all system components and facilities?	Yes	
	11.1 (d)	If automated monitoring is utilized (for example, wireless IDS/ IPS, NAC, etc.), is monitoring configured to generate alerts to notify personnel?	Yes	
	11.1.1	Is an inventory of authorized wireless access points maintained and a business justification documented for all authorized wireless access points?	Yes	
	11.1.2 (a)	Does the incident response plan define and require a response in the event that an unauthorized wireless access point is detected?	Yes	

Status	Item	Question	Your Response	Remediation
	11.1.2 (b)	Is action taken when unauthorized wireless access points are found ?	Yes	
	Are internal and external network vulnerability scans run 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), as follows? *Note: Multiple scan reports can be combined for the quarterly scan process to show that all systems were scanned and all applicable vulnerabilities have been addressed. Additional documentation may be required to verify non-remediated vulnerabilities are in the process of being addressed.* *For initial PCI DSS compliance, it is not required that four quarters of passing scans be completed 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, and 3) vulnerabilities noted in the scan results have been corrected as shown in a re-scan(s). For subsequent years after the initial PCI DSS review, four quarters of passing scans must have occurred.*		
	11.2.1 (a)	Are quarterly internal vulnerability scans performed?	Yes	
	11.2.1 (b)	Does the quarterly internal scan process address all "high-risk" vulnerabilities and include rescans to verify all "high-risk" volunerabilities (as defined in PCI DSS Requirement 6.1) are resolved?	Yes	
	11.2.1 (c)	Are quarterly internal scans performed by a qualified internal resource(s) or qualified external third party, and if applicable, does organizational independence of the tester exist (not required to be a QSA or ASV)?	Yes	
	11.2.2 (a)	Are quarterly external vulnerability scans performed? *Note: Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC).* *Refer to the ASV Program Guide published on the PCI SSC website for scan customer responsibilities, scan preparation, etc.*	Yes	
	11.2.2 (b)	Do external quarterly scan and rescan results satisfy the ASV Program Guide requirements for a passing scan (for example, no vulnerabilities rated 4.0 or higher by the CVSS, and no automatic failures)?	Yes	

Status	Item	Question	Your Response	Remediation
	11.2.2 (c)	Are quarterly external vulnerability scans performed by a PCI SSC Approved Scanning Vendor (ASV)?	Yes	
	11.2.3 (a)	Are internal and external scans, and rescans as needed, performed after any significant change? *Note: Scans must be performed by qualified personnel.*	Yes	
	11.2.3 (b)	Does the scan process include rescans until: • For external scans, no vulnerabilities exist that are scored 4.0 or higher by the CVSS, • For internal scans, a passing result is obtained or all "high-risk" vulnerabilities as defined in PCI DSS Requirement 6.1 are resolved?	Yes	
	11.2.3 (c)	Are scans performed by a qualified internal resource(s) or qualified external third party, and if applicable, does organizational independence of the tester exist (not required to be a QSA or ASV)?	Yes	
	If segmentation is used to isolate the CDE from other networks:			
	11.3.4 (a)	Are penetration-testing procedures defined to test all segmentation methods, to confirm they are operational and effective, and isolate all out-of-scope systems from in-scope systems?	Yes	
	11.3.4 (b)	Does penetration testing to verify segmentation controls meet the following? • Performed at least annually and after any changes to segmentation controls/methods • Covers all segmentation controls/methods in use • Verifies that segmentation methods are operational and effective, and isolate all out-of-scope systems from in-scope systems.	Yes	
	11.3.4 (c)	Are tests performed by a qualified internal resource or qualified external third party, and if applicable, does organizational independence of the tester exist (not required to be a QSA or ASV)?	Yes	

Status	Item	Question	Your Response	Remediation
	11.5 (a)	Is a change-detection mechanism (for example, file-integrity monitoring tools) deployed to detect unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files? *Examples of files that should be monitored include:* • *System executables* • *Application executables* • *Configuration and parameter files* • *Centrally stored, historical or archived, log, and audit files* • *Additional critical files determined by entity (for example, through risk assessment or other means)*	Yes	
	11.5 (b)	Is the change-detection mechanism configured to alert personnel to unauthorized modification of critical system files, configuration files or content files, and do the tools perform critical file comparisons at least weekly? *Note: For change detection 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. Change detection mechanisms such as 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).*	Yes	
	11.5.1	Is a process in place to respond to any alerts generated by the change-detection solution?	Yes	

Security Policies and Procedures				
Status	**Item**	**Question**	**Your Response**	**Remediation**
	12.1	Is a security policy established, published, maintained, and disseminated to all relevant personnel? *Note: For the purposes of Requirement 12, "personnel" refers to full-time and part-time employees, temporary employees and personnel, and contractors and consultants who are "resident" on the entity's site or otherwise have access to the company's site cardholder data environment.*	Yes	
	12.1.1	Is the security policy reviewed at least annually and updated when the environment changes?	Yes	
	Are usage policies for critical technologies developed to define proper use of these technologies and require the following: *Note: Examples of critical technologies include, but are not limited to, remote access and wireless technologies, laptops, tablets, removable electronic media, e-mail usage and Internet usage.*			
	12.3.1	Explicit approval by authorized parties to use the technologies?	Yes	
	12.3.2	Authentication for use of the technology?	Yes	
	12.3.3	A list of all such devices and personnel with access?	Yes	
	12.3.5	Acceptable uses of the technologies?	Yes	

Status	Item	Question	Your Response	Remediation
✓	12.3.6	Acceptable network locations for the technologies?	Yes	
✓	12.3.8	Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity?	Yes	
✓	12.3.9	Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use?	Yes	
✓	12.4	Do security policy and procedures clearly define information security responsibilities for all personnel?	Yes	
	Are the following information security management responsibilities formally assigned to an individual or team:			
✓	12.5.3	Establishing, documenting, and distributing security incident response and escalation procedures to ensure timely and effective handling of all situations?	Yes	
✓	12.6 (a)	Is a formal security awareness program in place to make all personnel aware of the cardholder data security policy and procedures?	Yes	
	Are policies and procedures maintained and implemented to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows:			
✓	12.8.1	Is a list of service providers maintained, including a description of the services(s) provided?	Not Applicable Comment : My organization does not have any relationships with third-party companies where credit card data is shared or who could affect the security of the credit card environment.	

Status	Item	Question	Your Response	Remediation
✓	12.8.2	Is a written agreement maintained that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process, or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment? *Note: The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.*	Not Applicable Comment : My organization does not have any relationships with third-party companies where credit card data is shared or who could affect the security of the credit card environment.	
✓	12.8.3	Is there an established process for engaging service providers, including proper due diligence prior to engagement?	Not Applicable Comment : My organization does not have any relationships with third-party companies where credit card data is shared or who could affect the security of the credit card environment.	
✓	12.8.4	Is a program maintained to monitor service providers' PCI DSS compliance status at least annually?	Not Applicable Comment : My organization does not have any relationships with third-party companies where credit card data is shared or who could affect the security of the credit card environment.	
✓	12.8.5	Is information maintained about which PCI DSS requirements are managed by each service provider, and which are managed by the entity?	Not Applicable Comment : My organization does not have any relationships with third-party companies where credit card data is shared or who could affect the security of the credit card environment.	
	Has an incident response plan been implemented in preparation to respond immediately to a system breach, as follows:			
✓	12.10.1 (a)	Has an incident response plan been created to be implemented in the event of system breach?	Yes	
	Does the plan address the following, at a minimum:			
✓	12.10.1 (b-1)	Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum?	Yes	

Questionnaire Date: 2017-04-18

Status	Item	Question	Your Response	Remediation
	12.10.1 (b-2)	Specific incident response procedures?	Yes	
	12.10.1 (b-3)	Business recovery and continuity procedures?	Yes	
	12.10.1 (b-4)	Data backup processes?	Yes	
	12.10.1 (b-5)	Analysis of legal requirements for reporting compromises?	Yes	
	12.10.1 (b-6)	Coverage and responses of all critical system components?	Yes	
	12.10.1 (b-7)	Reference or inclusion of incident response procedures from the payment brands?	Yes	

Hosting Providers				
Status	**Item**	**Question**	**Your Response**	**Remediation**
	A2.1	For POS POI terminals (and the SSL/TLS termination points to which they connect) using SSL and/or early TLS: • Are the devices confirmed to not be susceptible to an known exploits for SSL/early TLS • Or: • Is there a formal Risk Mitigation and Migration Plan in place per Requirement A2.2?	Yes	
	A2.2	Is there a formal Risk Mitigation and Migration Plan in place for all implementations that use SSL and/or early TLS (other than as allowed in A2.1) that includes: • Description of usage, including; what data is being transmitted, types and number of systems that use and/or support SSL/early TLS, type of environment; • Risk assessment results and risk reduction controls in place; • Description of processes to monitor for new vulnerabilities associated with SSL/early TLS; • Description of change control processes that are implemented to ensure SSL/early TLS is not implemented into new environments; • Overview of migration project plan including target migration completion date no later than 30th June 2016.	Yes	

Confirmation and Acknowledgement

Status	Item	Question	Your Response	Remediation
	CA.C	PCI DSS Self-Assessment Questionnaire C, Version 3.2, was completed according to the instructions therein.	Yes	
	CA.2	All information within the above-referenced SAQ and in this attestation fairly represents the results of my assessment in all material respects.	Yes	
	CA.3	I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.	Yes	
	CA.4	I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.	Yes	
	CA.5	If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.	Yes	
	CA.6	No evidence of full track data[1], CAV2, CVC2, CID, or CVV2 data[2], or PIN data[3] storage after transaction authorization was found on ANY system reviewed during this assessment. 1. Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full track data after transaction authorization. The only elements of track data that may be retained are primary account number (PAN), expiration date, and cardholder name. 2. The three- or four-digit value printed by the signature panel or on the face of a payment card used to verify card-not-present transactions. 3. Personal identification number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.	Yes	

Compensating Controls

The following questionnaire issues were identified as being addressed with Compensating Controls....

Compensating Controls			
#	Item	Question	Details