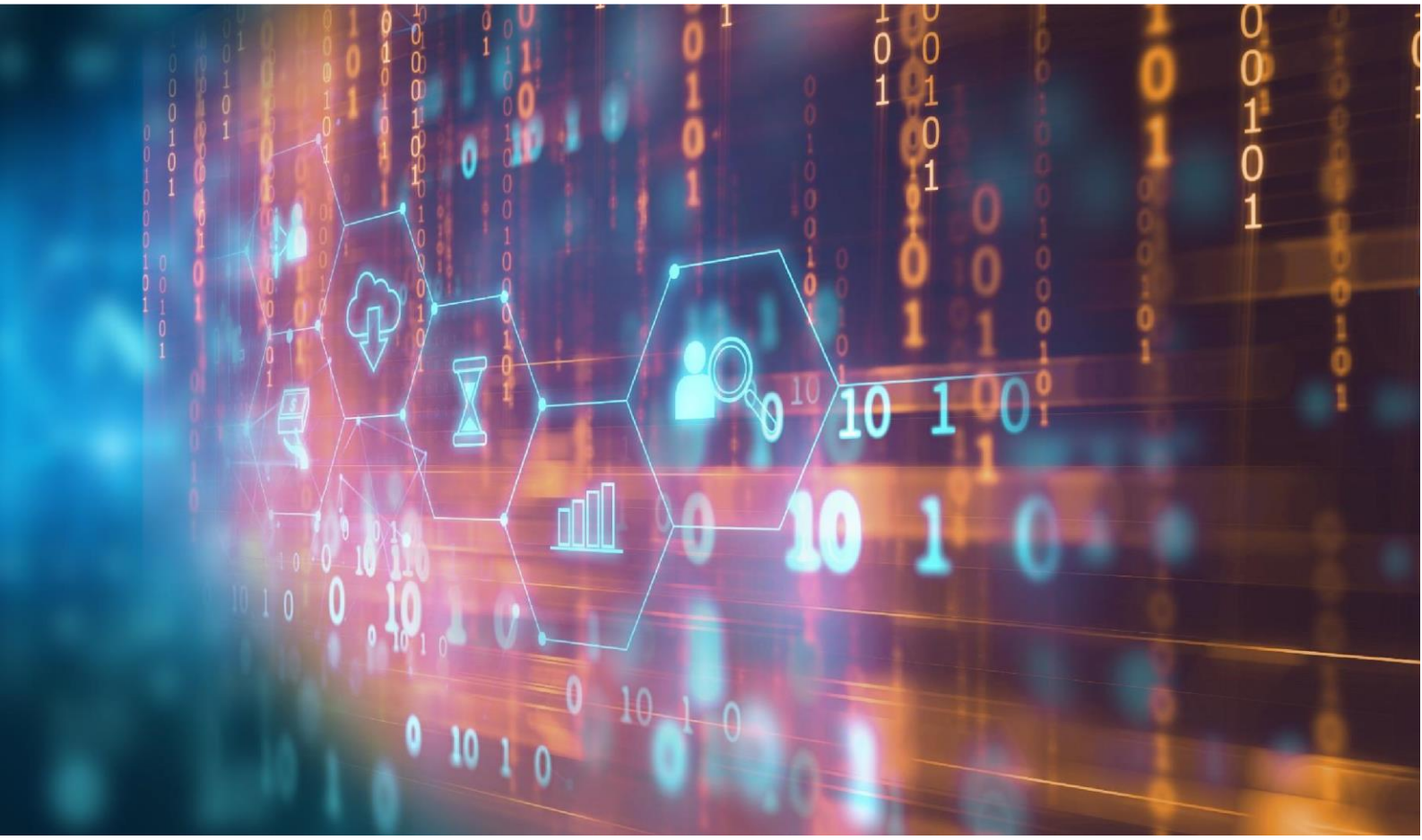
access PaySuite

Mobile SDK



PCI Compliance Statement

October 2023

Introduction

One of the security issues with integrating your app with our payments platforms is the handling of large amounts of cardholder data. When integrating with Access PaySuite, you are completely in control of the collection, transmission and optional storage of cardholder data.

Important - You must comply with all eligible PCI DSS requirements, any functions related to cardholder data are not the responsibility of Access PaySuite.

To mitigate the risks associated with your integration, please review this document to assess your compliance.

PCI Responsibilities

Requirements	Control Description	Managed by Customer	Responsiblity of the service provider	Shared Responsibility	Justification
Requirement 1: Install and Maintain a Firewall Configuration					
1.1	Establish firewall and router configuration standards that include the following:				
1.1.1	A formal process for approving and testing all network connections and changes to the firewall and router configurations.	NO	YES	NO	
1.1.2	Current diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks.	NO	YES	NO	
1.1.3	Current diagram that shows all cardholder data flows across systems and networks.	NO	NO	YES	
1.1.4	Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone.	NO	YES	NO	

Requirements	Control Description	Managed by Customer	Responsiblity of the service provider	Shared Responsibility	Justification
1.1.5	Description of groups, roles, and responsibilities for management of network components.	NO	YES	NO	
1.1.6	Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented.	NO	YES	NO	
1.1.7	Requirement to review firewall and router rule sets at least every six months.	NO	YES	NO	
1.2	Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data.	NO	YES	NO	
1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	NO	YES	NO	
1.2.2	Secure and synchronize router configuration files.	NO	YES	NO	
1.2.3	Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.	NO	YES	NO	
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.	NO	YES	NO	

Requirements	Control Description	Managed by Customer	Responsiblity of the service provider	Shared Responsibility	Justification
1.3.1	Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	NO	YES	NO	
1.3.2	Limit inbound Internet traffic to IP addresses within the DMZ.	NO	YES	NO	
1.3.3	Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment.	NO	YES	NO	
1.3.4	Do not allow internal addresses to pass from the Internet into the DMZ.	NO	YES	NO	
1.3.5	Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	NO	YES	NO	
1.3.6	Implement stateful inspection, also known as dynamic packet filtering. (That is, only “established” connections are allowed into the network.)	NO	YES	NO	
1.3.7	Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.	NO	YES	NO	
1.3.8	Do not disclose private IP addresses and routing information to unauthorized parties.	NO	YES	NO	
1.4	Install personal firewall software on any mobile and/or employee-owned devices that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the network.	NO	YES	NO	

Requirements	Control Description	Managed by Customer	Responsiblity of the service provider	Shared Responsibility	Justification
1.5	Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties.	NO	YES	NO	

Requirements	Control Description	Managed by Customer	Responsiblity of the service provider	Shared Responsiblity	Justification
Requirement 2: Do not Use Vendor Supplied Defaults					
2.1	Always change vendorsupplied defaults and remove or disable unnecessary default accounts before installing a system on the network.	NO	YES	NO	Not applicable - no wireless networks connected to the cardholder environment
2.1.1	For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.	NO	NO	NO	
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.	NO	YES	NO	
2.2.1	Implement only one primary function per server to prevent functions that require different security levels from coexisting on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.)	NO	YES	NO	

Requirements	Control Description	Managed by Customer	Responsiblity of the service provider	Shared Responsiblity	Justification
2.2.2	Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	NO	YES	NO	Not applicable - no insecure services, daemons or protocols are enabled
2.2.3	Implement additional security features for any required services, protocols, or daemons that are considered to be insecure — for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.	NO	NO	NO	
2.2.4	Configure system security parameters to prevent misuse.	NO	YES	NO	
2.2.5	Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	NO	YES	NO	
2.3	Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for webbased management and other non-console administrative access.	NO	YES	NO	

2.4	Maintain an inventory of system components that are in scope for PCI DSS.	NO	YES	NO	
Requirements	**Control Description**	**Managed by Customer**	**Responsiblity of the service provider**	**Shared Responsiblity**	**Justification**
2.5	Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties.	NO	YES	NO	
2.6	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.	NO	NO	NO	Not applicable - entitiy is not a shared hosting provider

Requirements	**Control Description**	**Managed by Customer**	**Responsiblity of the service provider**	**Shared Responsiblity**	**Justification**
Requirement 3: Protect Stored Cardholder Data					
3.1	Keep cardholder data storage to a minimum by implementing data-retention and disposal policies, procedures and processes.	NO	YES	NO	

3.2	Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process.	NO	YES	NO	
3.2.1	Do not store 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). This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.	NO	YES	NO	No track or equivelant chip data is captured
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-notpresent transactions.	NO	YES	NO	

Requirements	Control Description	Managed by Customer	Responsiblity of the service provider	Shared Responsiblity	Justification
3.2.3	Do not store the personal identification number (PIN) or the encrypted PIN block.	NO	YES	NO	No PIN data is captured

3.3	Mask PAN 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 more than the first six/last four digits of the PAN.	NO	YES	NO	
3.4	Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs).	NO	YES	NO	
3.4.1	If disk encryption is used (rather than file- or columnlevel database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.	NO	YES	NO	
3.5	Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse.	NO	YES	NO	

Requirements	Control Description	Managed by Customer	Responsiblity of the service provider	Shared Responsiblity	Justification

3.5.1	**Additional requirement for service providers only:** Maintain a documented description of the cryptographic architecture.	NO	YES	NO	
3.5.2	Restrict access to cryptographic keys to the fewest number of custodians necessary.	NO	YES	NO	
3.5.3	Store secret and private keys used to encrypt/decrypt cardholder data.	NO	YES	NO	
3.5.4	Store cryptographic keys in the fewest possible locations.	NO	YES	NO	
3.6	Fully document and implement all keymanagement processes and procedures for cryptographic keys used for encryption of cardholder data, including the following:	NO	YES	NO	
3.6.1	Generation of strong cryptographic keys.	NO	YES	NO	
3.6.2	Secure cryptographic key distribution.	NO	YES	NO	
3.6.3	Secure cryptographic key storage.	NO	YES	NO	

Requirements	Control Description	Managed by Customer	Responsiblity of the service provider	Shared Responsiblity	Justification

3.6.4	Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines.	NO	YES	NO	
3.6.5	Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a cleartext key component), or keys are suspected of being compromised.	NO	YES	NO	
3.6.6	If manual clear-text cryptographic keymanagement operations are used, these operations must be managed using split knowledge and dual control.	NO	YES	NO	
3.6.7	Prevention of unauthorized substitution of cryptographic keys	NO	YES	NO	
Requirements	**Control Description**	**Managed by Customer**	**Responsiblity of the service provider**	**Shared Responsiblity**	**Justification**

3.6.8	Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities.	NO	YES	NO	
3.7	Ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties.	NO	YES	NO	

Requirements	Control Description	Managed by Customer	Responsiblity of the service provider	Shared Responsiblity	Justification
Requirement 4: Encrypt Transmission of Cardholder Data across Open, Public Networks					
4.1	Use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks.	NO	YES	NO	
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.	NO	NO	NO	Not applicable - no wireless networks used within the cardholder data environment
4.2	Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat, etc.).	NO	YES	NO	
4.3	Ensure that security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use, and known to all affected parties.	NO	YES	NO	

Requirements	Control Description	Managed by Customer	Responsiblity of the service provider	Shared R esponsibility	Justification
Requirement 5: Protect all Systems Against Malware and Update Anti-Virus Software					
5.1	Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	NO	YES	NO	
5.1.1	Ensure that all anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.	NO	YES	NO	
5.1.2	For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software.	NO	NO	NO	Not applicable - all servers in scope have anti malware software installed
5.2	Ensure that all anti-virus mechanisms are maintained.	NO	YES	NO	

5.3	Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a caseby-case basis for a limited time period.	NO	YES	NO	
Requirements	**Control Description**	**Managed by Customer**	**Responsiblity of the service provider**	**Shared R esponsibility**	**Justification**
5.4	Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties.	NO	YES	NO	

Requirements	Control Description	Managed by Customer	Responsiblity of the service provider	Shared Responsiblity	Justification
Requirement 6: Develop and Maintain Secure Systems and Applications					
6.1	Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as “high,” “medium,” or “low”) to newly discovered security vulnerabilities.	NO	NO	YES	
6.2	Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.	NO	NO	YES	
6.3	Develop internal and external software applications (including webbased administrative access to applications) securely.	NO	NO	YES	
6.3.1	Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers.	NO	NO	YES	

6.3.2	Review custom code prior to release to production or customers in order to identify any potential coding vulnerability (using either	NO	NO	YES	

Requirements	Control Description	Managed by Customer	Responsiblity of the service provider	Shared Responsiblity	Justification
	manual or automated processes).				
6.4	Follow change control processes and procedures for all changes to system components. The processes must include the following:	NO	NO	YES	
6.4.1	Separate development/test environments from production environments, and enforce the separation with access controls.	NO	NO	YES	
6.4.2	Separation of duties between development/test and production environments.	NO	NO	YES	
6.4.3	Production data (live PANs) are not used for testing or development.	NO	NO	YES	
6.4.4	Removal of test data and accounts before production systems become active.	NO	NO	YES	
6.4.5	Change control procedures for the implementation of security patches and software modifications must include the following:	NO	NO	YES	
6.4.5.1	Documentation of impact.	NO	NO	YES	

6.4.5.2	Documented change approval by authorized parties.	NO	NO	YES	
6.4.5.3	Functionality testing to verify that the change does not adversely impact the security of the system.	NO	NO	YES	

Requirements	Control Description	Managed by Customer	Responsiblity of the service provider	Shared Responsiblity	Justification
6.4.5.4	Back-out procedures.	NO	NO	YES	
6.4.6	Upon completion of a significant change, all relevant PCI DSS requirements must be implemented on all new or changed systems and networks, and documentation updated as applicable.	NO	NO	YES	

6.5	Address common coding vulnerabilities in softwaredevelopment processes as follows:Train developers in secure coding techniques, including how to avoid common coding vulnerabilities, and understanding how sensitive data is handled in memory. Train developers in secure coding techniques, including how to avoid common coding vulnerabilities, and understanding how sensitive data is handled in memory. Develop applications based on secure coding guidelines.	NO	NO	YES	
6.5.1	Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.	NO	NO	YES	

Requirements	Control Description	Managed by Customer	Responsiblity of the service provider	Shared Responsiblity	Justification
6.5.2	Buffer overflow.	NO	NO	YES	
6.5.3	Insecure cryptographic storage.	NO	NO	YES	
6.5.4	Insecure communications.	NO	NO	YES	
6.5.5	Improper error handling	NO	NO	YES	
6.5.6	All “high risk” vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1).	NO	NO	YES	
6.5.7	Cross-site scripting (XSS).	NO	NO	YES	

6.5.8	Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions).	NO	NO	YES	
6.5.9	Cross-site request forgery (CSRF)	NO	NO	YES	
6.5.10	Broken authentication and session management.	NO	NO	YES	
Requirements	**Control Description**	**Managed by Customer**	**Responsiblity of the service provider**	**Shared Responsiblity**	**Justification**
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 an automated technical solution that detects and prevents webbased attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic..	NO	NO	YES	

6.7	Ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties.	NO	NO	YES	

Requirements	Control Description	Managed by Customer	Responsiblity of the service provider	Shared Responsiblity	Justification
Requirement 7: Restrict Access to Cardholder Data by Business Need to Know					
7.1	Limit access to system components and cardholder data to only those individuals whose job requires such access.	NO	YES	NO	
7.1.1	Define access needs for each role, including: System components and data resources that each role needs to access for their job function. Level of privilege required (for example, user, administrator, etc.) for accessing resources.	NO	YES	NO	
7.1.2	Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.	NO	YES	NO	

7.1.3	Assign access based on individual personnel's job classification and function.	NO	YES	NO	
7.1.4	Require documented approval by authorized parties specifying required privileges.	NO	YES	NO	
Requirements	**Control Description**	**Managed by Customer**	**Responsiblity of the service provider**	**Shared Responsiblity**	**Justification**
7.2	Establish an access control system for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.	NO	YES	NO	
7.2.1	Coverage of all system components	NO	YES	NO	
7.2.2	Assignment of privileges to individuals based on job classification and function	NO	YES	NO	
7.2.3	Default "deny-all" setting	NO	YES	NO	
7.3	Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties.	NO	YES	NO	

Requirements	Control Description	Managed by Customer	Responsiblity of the service provider	Shared Responsiblity	Justification
Requirement 8: Identify and Authenticate Access to System Components					
8.1	Define and implement policies and procedures to ensure proper user identification management for nonconsumer users and administrators on all system components as follows:	NO	YES	NO	
8.1.1	Assign all users a unique ID before allowing them to access system components or cardholder data.	NO	YES	NO	
8.1.2	Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	NO	YES	NO	
8.1.3	Immediately revoke access for any terminated users.	NO	YES	NO	
8.1.4	Remove/disable inactive user accounts at least every 90 days.	NO	YES	NO	
8.1.5	Manage IDs used by vendors to access, support, or maintain system components via remote access.	NO	NO	NO	Not applicable - third parties are no granted remote access

8.1.6	Limit repeated access attempts by locking out the user ID after not more than six attempts.	NO	YES	NO	

Requirements	Control Description	Managed by Customer	Responsiblity of the service provider	Shared Responsiblity	Justification
8.1.7	Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.	NO	YES	NO	
8.1.8	If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.	NO	YES	NO	
8.2	In addition to assigning a unique ID, ensure proper userauthentication management for nonconsumer users and administrators on all system components by employing at least one of the following methods 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.	NO	YES	NO	

8.2.1	Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.	NO	YES	NO	

Requirements	Control Description	Managed by Customer	Responsiblity of the service provider	Shared Responsiblity	Justification
8.2.2	Verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens, or generating new keys.	NO	YES	NO	
8.2.3	Passwords/phrases must meet the following: Require a minimum length of at least seven characters. Contain both numeric and alphabetic characters.	NO	YES	NO	
8.2.4	Change user passwords/passphrases at least every 90 days.	NO	YES	NO	
8.2.5	Do not allow an individual to submit a new password/phrase that is the same as any of the last four passwords/phrases he or she has used.	NO	YES	NO	

8.2.6	Set passwords/phrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use.	NO	YES	NO	
8.3	Secure all individual non-console administrative access and all remote access	NO	YES	NO	

Requirements	Control Description	Managed by Customer	Responsiblity of the service provider	Shared Responsiblity	Justification
	to the CDE using multifactor authentication.				
8.3.1	Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access.	NO	YES	NO	
8.3.2	Incorporate multi-factor authentication 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.	NO	YES	NO	
8.4	Document and communicate authentication procedures and policies to all users.	NO	YES	NO	

8.5	Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows: Generic user IDs are disabled or removed. Shared user IDs do not exist for system administration and other critical functions. Shared and generic user IDs are not used to administer any system components	NO	NO	YES	

Requirements	Control Description	Managed by Customer	Responsiblity of the service provider	Shared Responsiblity	Justification
8.5.1	Additional requirement for service providers: Service providers with remote access to customer premises (for example, for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer.	NO	NO	NO	Not applicable - Access PaySuite does not have remote access to customer premises.
8.6	Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.) use of these mechanisms must be assigned.	NO	YES	NO	

8.7	All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows: All user access to, user queries of, and user actions on databases are through programmatic methods. Only database administrators have the ability to directly access or query databases. Application IDs for database applications	NO	YES	NO	
Requirements	**Control Description**	**Managed by Customer**	**Responsiblity of the service provider**	**Shared Responsiblity**	**Justification**
	can only be used by the applications (and not by individual users or other non-application processes).				
8.8	Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties.	NO	YES	NO	

Requirements	Control Description	Managed by Customer	Responsiblity of the service provider	Shared Responsiblity	Justification
Requirement 9: Restrict Physical Access to Cardholder Data					
9.1	Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.	NO	YES	NO	
9.1.1	Use video cameras and/or 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.	NO	YES	NO	
9.1.2	Implement physical and/or logical controls to restrict access to publicly accessible network jacks.	NO	YES	NO	
9.1.3	Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.	NO	YES	NO	

9.2	Develop procedures to easily distinguish between onsite personnel and visitors, to include: Identifying new onsite personnel or visitors (for example, assigning badges). Changes to access requirements. Revoking or terminating onsite personnel and	NO	YES	NO	

Requirements	Control Description	Managed by Customer	Responsiblity of the service provider	Shared Responsiblity	Justification
	expired visitor identification (such as ID badges).				
9.3	Control physical access for onsite personnel to the sensitive areas as follows: Access must be authorized and based on individual job function. Access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc., are returned or disabled.	NO	YES	NO	

9.4	Implement procedures to identify and authorize visitors. Procedures should include the following:	NO	YES	NO	
9.4.1	Visitors are authorized before entering, and escorted at all times within, areas where cardholder data is processed or maintained.	NO	YES	NO	
9.4.2	Visitors are identified and given a badge or other identification that expires and that visibly	NO	YES	NO	

Requirements	Control Description	Managed by Customer	Responsiblity of the service provider	Shared Responsiblity	Justification
	distinguishes the visitors from onsite personnel.				
9.4.3	Visitors are asked to surrender the badge or identification before leaving the facility or at the date of expiration.	NO	YES	NO	
9.4.4	A visitor log is used to maintain a physical audit trail of visitor activity to the facility as well as for computer rooms and data centers where cardholder data is stored or transmitted.	NO	YES	NO	
9.5	Physically secure all media.	NO	YES	YES	

9.5.1	Store media backups 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.	NO	NO	NO	Not applicable - Access PaySuite do not have any media backups
9.6	Maintain strict control over the internal or external distribution of any kind of media, including the following:	NO	YES	NO	
9.6.1	Classify media so the sensitivity of the data can be determined.	NO	YES	NO	
9.6.2	Send the media by secured courier or other delivery method that can be accurately tracked.	NO	YES	NO	

Requirements	Control Description	Managed by Customer	Responsiblity of the service provider	Shared Responsiblity	Justification
9.6.3	Ensure management approves any and all media that is moved from a secured area (including when media is distributed to individuals).	NO	YES	NO	
9.7	Maintain strict control over the storage and accessibility of media.	NO	YES	NO	
9.8	Destroy media when it is no longer needed for business or legal reasons as follows:	NO	NO	NO	Not applicable - All damaged or inoperable PED devices are securely shipped by secured courier (or other delivery method that can be accurately tracked), to VeriFone.

9.8.1	Shred, incinerate, or pulp hard-copy materials so that cardholder data cannot be reconstructed. Secure storage containers used for materials that are to be destroyed.	NO	NO	NO	Not applicable to - All damaged or inoperable PED devices are securely shipped by secured courier (or other delivery method that can be accurately tracked), to VeriFone.
9.8.2	Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.	NO	NO	NO	Not applicable - All damaged or inoperable PED devices are securely shipped by secured courier (or other delivery method that can be accurately tracked), to VeriFone.
9.9	Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution.	NO	YES	NO	
Requirements	**Control Description**	**Managed by Customer**	**Responsiblity of the service provider**	**Shared Responsiblity**	**Justification**
9.9.1	Maintain an up-to-date list of devices. The list should 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.	NO	YES	NO	

9.9.2	Periodically inspect device surfaces 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).	NO	NO	NO	Not applicable - All damaged or inoperable PED devices are securely shipped by secured courier (or other delivery method that can be accurately tracked), to VeriFone.
9.9.3	Provide training for personnel to be aware of attempted tampering or replacement of devices.	NO	NO	NO	Not applicable - All damaged or inoperable PED devices are securely shipped by secured courier (or other delivery method that can be accurately tracked), to VeriFone.
9.10	Ensure that security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all affected parties.	NO	YES	YES	

Requirements	Control Description	Managed by Customer	Responsiblity of the service provider	Shared Responsiblity	Justification
Requirement 10: Track and Monitor All Access To Network Resources					
10.1	Implement audit trails to link all access to system components to each individual user.	NO	YES	NO	
10.2	Implement automated audit trails for all system components to reconstruct the following events:	NO	YES	NO	

10.2.1	All individual user accesses to cardholder data.	NO	YES	NO	
10.2.2	All actions taken by any individual with root or administrative privileges	NO	YES	NO	
10.2.3	Access to all audit trails	NO	YES	NO	
10.2.4	Invalid logical access attempts	NO	YES	NO	
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.	NO	YES	NO	
10.2.6	Initialization, stopping, or pausing of the audit logs.	NO	YES	NO	
10.2.7	Creation and deletion of system-level objects	NO	YES	NO	
10.3	Record at least the following audit trail entries for all system components for each event:	NO	YES	NO	

Requirements	Control Description	Managed by Customer	Responsiblity of the service provider	Shared Responsiblity	Justification
10.3.1	User identification	NO	YES	NO	
10.3.2	Type of event	NO	YES	NO	
10.3.3	Date and time	NO	YES	NO	
10.3.4	Success or failure indication	NO	YES	NO	

10.3.5	Origination of event	NO	YES	NO	
10.3.6	Identity or name of affected data, system component, or resource	NO	YES	NO	
10.4	Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time.	NO	YES	NO	
10.4.1	Critical systems have the correct and consistent time.	NO	YES	NO	
10.4.2	Time data is protected.	NO	YES	NO	
10.4.3	Time settings are received from industry-accepted time sources.	NO	YES	NO	
10.5	Secure audit trails so they cannot be altered.	NO	YES	NO	
10.5.1	Limit viewing of audit trails to those with a job-related need	NO	YES	NO	
10.5.2	Protect audit trail files from unauthorized modifications	NO	YES	NO	
10.5.3	Promptly back-up audit trail files to a centralized log server or media that is difficult to alter	NO	YES	NO	

Requirements	Control Description	Managed by Customer	Responsiblity of the service provider	Shared Responsiblity	Justification
10.5.4	Write logs for externalfacing technologies onto a secure, centralized, internal log server or media device.	NO	YES	NO	

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).	NO	YES	NO	
10.6	Review logs and security events for all system components to identify anomalies or suspicious activity.	NO	YES	NO	
10.6.1	Review the following at least daily: Logs of all system components that store, process, or transmit CHD and/or SAD, or that could impact the security of CHD and/or SAD. Logs of all critical system components. Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusionprevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).	NO	YES	NO	

Requirements	Control Description	Managed by Customer	Responsiblity of the service provider	Shared Responsiblity	Justification

10.6.2	Review logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment.	NO	YES	NO	
10.6.3	Follow up exceptions and anomalies identified during the review process.	NO	YES	NO	
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 backup).	NO	YES	NO	
10.8	**Additional requirement for service providers only**: Implement a process for the timely detection and reporting of failures of critical security control systems.	NO	YES	NO	
10.8.1	**Additional requirement for service providers only:** Respond to failures of any critical security controls in a timely manner.	NO	YES	NO	
10.9	Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties.	NO	YES	NO	

Requirements	Control Description	Managed by Customer	Responsiblity of the service provider	Shared Responsiblity	Justification
Requirement 11: Regularly Test Security Systems and Processes					
11.1	Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis.	NO	YES	NO	
11.1.1	Maintain an inventory of authorized wireless access points including a documented business justification.	NO	NO	NO	Not applicable - no wireless access points are allowed
11.1.2	Implement incident response procedures in the event unauthorized wireless access points are detected.	NO	YES	NO	
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).	NO	YES	NO	

11.2.1	Perform quarterly internal vulnerability scans, and rescans as needed, until all “high-risk” vulnerabilities (as identified in Requirement 6.1) are resolved. Scans must be performed by qualified personnel.	NO	YES	NO	

Requirements	Control Description	Managed by Customer	Responsiblity of the service provider	Shared Responsiblity	Justification
11.2.2	Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved.	NO	YES	NO	
11.2.3	Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel.	NO	YES	NO	

11.3	Implement a methodology for penetration testing that includes at least the following: Is based on industryaccepted penetration testing approaches (for example, NIST SP800115). Includes coverage for the entire CDE perimeter and critical systems. Includes testing from both inside and outside of the network. Includes testing to validate any segmentation and scope reduction controls. Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5. Includes review and	NO	NO	YES	

Requirements	Control Description	Managed by Customer	Responsiblity of the service provider	Shared Responsiblity	Justification

	consideration of threats and vulnerabilities experienced in the last 12 months. Defines network-layer penetration tests to include components that support network functions as well as operating systems. Specifies retention of penetration testing results and remediation activities results.				
11.3.1	Perform external penetration testing at least annually 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).	NO	NO	YES	
11.3.2	Perform internal penetration testing at least annually 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	NO	NO	YES	

Requirements	Control Description	Managed by Customer	Responsiblity of the service provider	Shared Responsiblity	Justification
	server added to the environment).				
11.3.3	Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections.	NO	NO	YES	
11.3.4	If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from in-scope systems.	NO	YES	NO	
11.3.4.1	**Additional requirement for service providers only:** If segmentation is used, confirm PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after any changes to segmentation controls/methods.	NO	YES	NO	

Requirements	Control Description	Managed by Customer	Responsiblity of the service provider	Shared Responsiblity	Justification
11.4	Use intrusion-detection systems and/or intrusionprevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises.	NO	YES	NO	
11.5	Deploy a change-detection mechanism (for example, file-integrity monitoring tools) 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.	NO	YES	NO	
11.5.1	Implement a process to respond to any alerts generated by the changedetection solution.	NO	YES	NO	
11.6	Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties.	NO	NO	YES	

Requirements	Control Description	Managed by Customer	Responsiblity of the service provider	Shared Responsiblity	Justification
Requirement 12: Information Security Policy					
12.1	Establish, publish, maintain, and disseminate a security policy.	NO	YES	NO	
12.1.1	Review the security policy at least annually and update the policy when business objectives or the risk environment change.	NO	YES	NO	
12.2	Implement a risk assessment process, that: Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.), Identifies critical assets, threats, and vulnerabilities, and Results in a formal risk assessment.	NO	NO	YES	
12.3	Develop usage policies for critical technologies and define proper use of these technologies.	NO	YES	NO	
12.3.1	Explicit approval by authorized parties.	NO	YES	NO	
12.3.2	Authentication for use of the technology	NO	YES	NO	

Requirements	Control Description	Managed by Customer	Responsiblity of the service provider	Shared Responsiblity	Justification
12.3.3	A list of all such devices and personnel with access.	NO	YES	NO	
12.3.4	A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices).	NO	YES	NO	
12.3.5	Acceptable uses of the technologies	NO	YES	NO	
12.3.6	Acceptable network locations for the technologies.	NO	YES	NO	
12.3.7	List of company-approved products	NO	YES	NO	
12.3.8	Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity.	NO	YES	NO	
12.3.9	Activation of remoteaccess technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use.	NO	NO	NO	Not applicable - Vendors/Partners are not granted remote access to CDE

12.3.10	For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need. Where	NO	YES	NO	

Requirements	Control Description	Managed by Customer	Responsiblity of the service provider	Shared Responsiblity	Justification
	there is an authorized business need, the usage policies must require the data be protected in accordance with all applicable PCI DSS Requirements.				
12.4	Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.	NO	NO	YES	
12.4.1	**Additional requirement for service providers only**: Executive management shall establish responsibility for the protection of cardholder data.	NO	YES	NO	
12.5	Assign to an individual or team the following information security management responsibilities:	NO	YES	NO	

12.5.1	Establish, document, and distribute security policies and procedures.	NO	YES	NO	
12.5.2	Monitor and analyze security alerts and information, and distribute to appropriate personnel	NO	YES	NO	
12.5.3	Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.	NO	YES	NO	

Requirements	Control Description	Managed by Customer	Responsiblity of the service provider	Shared Responsiblity	Justification
12.5.4	Administer user accounts, including additions, deletions, and modifications	NO	YES	NO	
12.5.5	Monitor and control all access to data.	NO	YES	NO	
12.6	Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security.	NO	YES	NO	
12.6.1	Educate personnel upon hire and at least annually.	NO	YES	NO	
12.6.2	Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures.	NO	YES	NO	

12.7	Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. (Examples of background checks include previous employment history, criminal record, credit history, and reference checks.)	NO	NO	YES	
12.8	Maintain and implement policies and procedures to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows:	NO	NO	YES	
12.8.1	Maintain a list of service providers.	NO	NO	YES	

Requirements	Control Description	Managed by Customer	Responsiblity of the service provider	Shared Responsiblity	Justification
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 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 CDE.	NO	NO	YES	
12.8.3	Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.	NO	NO	YES	

12.8.4	Maintain a program to monitor service providers' PCI DSS compliance status at least annually.	NO	NO	YES	
12.8.5	Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.	NO	NO	YES	
12.9	Additional requirement for service providers: Service providers acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent	NO	YES	NO	

Requirements	Control Description	Managed by Customer	Responsiblity of the service provider	Shared Responsiblity	Justification
	that they could impact the security of the customer's cardholder data environment.				
12.10	Implement an incident response plan. Be prepared to respond immediately to a system breach.	NO	YES	NO	

12.10.1	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.	NO	NO	YES	
Requirements	**Control Description**	**Managed by Customer**	**Responsiblity of the service provider**	**Shared Responsiblity**	**Justification**
12.10.2	Test the plan at least annually.	NO	YES	NO	
12.10.3	Designate specific personnel to be available on a 24/7 basis to respond to alerts.	NO	YES	NO	
12.10.4	Provide appropriate training to staff with security breach response responsibilities.	NO	YES	NO	

12.10.5	Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems.	NO	YES	NO	
12.10.6	Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.	NO	YES	NO	
12.11	**Additional requirement for service providers only:** Perform reviews at least quarterly to confirm personnel are following security policies and operational procedures.	NO	YES	NO	
12.11.1	**Additional requirement for service providers only:** Maintain documentation of quarterly review process.				