Payment Card Industry (PCI)
Data Security Standard
Self-Assessment Questionnaire B

Merchants with Only Imprint Machines or Only Standalone, Dial-out Terminals – No Electronic Cardholder Data Storage

For use with PCI DSS Version 4.0
Merchant #: 4228997700829331
Merchant Name: Informationr.us

December 2022

Section 2: Self-Assessment Questionnaire B

Note: *The following questions are numbered according to PCI DSS requirements and testing procedures, as defined in the PCI DSS Requirements and Security Assessment Procedures document.*

Self-assessment completion date: 3/22/2024

Protect Cardholder Data

Requirement 3: Protect Stored Account Data

Note: *For SAQ B, Requirement 3 applies only to merchants with paper records that include account data (for example, receipts or printed reports).*

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			In Place	**In Place with CCW**	**Not Applicable**	**Not in Place**
3.1.1	All security policies and operational procedures that are identified in Requirement 3 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	• Examine documentation. • Interview personnel.	☑	□	□	□
3.3.1	SAD is not retained after authorization, even if encrypted. All sensitive authentication data received is rendered unrecoverable upon completion of the authorization process.	• Examine documented policies and procedures. • Examine system configurations. • Observe the secure data deletion processes.	☑	□	□	□
3.3.1.1	The full contents of any track are not retained upon completion of the authorization process.	• Examine data sources.	☑	□	□	□
3.3.1.2	The card verification code is not retained upon completion of the authorization process.	• Examine data sources.	☑	□	□	□

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			In Place	In Place with CCW	Not Applicable	Not in Place
3.3.1.3	The personal identification number (PIN) and the PIN block are not retained upon completion of the authorization process.	• Examine data sources.	☑	□	□	□
3.4.1	PAN is masked when displayed (the BIN 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 BIN and last four digits of the PAN.	• Examine documented policies and procedures. • Examine system configurations. • Examine the documented list of roles that need access to more than the BIN and last four digits of the PAN (includes full PAN). • Examine displays of PAN (for example, on screen, on paper receipts).	☑	□	□	□

Implement Strong Access Control Measures

Requirement 7: Restrict Access to System Components and Cardholder Data by Business Need to Know

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			In Place	In Place with CCW	Not Applicable	Not in Place
7.2.2	Access is assigned to users, including privileged users, based on: • Job classification and function. • Least privileges necessary to perform job responsibilities.	• Examine policies and procedures. • Examine user access settings, including for privileged users. • Interview responsible management personnel. • Interview personnel responsible for assigning access.	☑	□	□	□

Requirement 9: Restrict Physical Access to Cardholder Data

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			In Place	**In Place with CCW**	**Not Applicable**	**Not in Place**
9.4.1	All media with cardholder data is physically secured.	• Examine documentation.	☑	□	□	□
9.4.1.1	Offline media backups with cardholder data are stored in a secure location.	• Examine documented procedures. • Examine logs or other documentation. • Interview responsible personnel at the storge location(s).	☑	□	□	□
9.4.2	All media with cardholder data is classified in accordance with the sensitivity of the data.	• Examine documented procedures. • Examine media logs or other documentation.	☑	□	□	□
9.4.3	Media with cardholder data sent outside the facility is secured as follows: • Media is sent by secured courier or other delivery method that can be accurately tracked.	• Examine documented procedures. • Interview personnel. • Examine records. • Examine offsite tracking logs for all media.	☑	□	□	□
9.4.4	Management approves all media with cardholder data that is moved outside the facility (including when media is distributed to individuals).	• Examine documented procedures. • Examine offsite media tracking logs. • Interview responsible personnel.	☑	□	□	□

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			In Place	In Place with CCW	Not Applicable	Not in Place
9.4.6	Hard-copy materials with cardholder data are destroyed when no longer needed for business or legal reasons, as follows: • Materials are cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed. • Materials are stored in secure storage containers prior to destruction.	• Examine the periodic media destruction policy. • Observe processes. • Interview personnel. • Observe storage containers.	☑	□	□	□
9.5.1	POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following: • Maintaining a list of POI devices. • Periodically inspecting POI devices to look for tampering or unauthorized substitution. • Training personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of devices.	• Examine documented policies and procedures.	☑	□	□	□
9.5.1.1	An up-to-date list of POI devices is maintained, including: • Make and model of the device. • Location of device. • Device serial number or other methods of unique identification.	• Examine the list of POI devices. • Observe POI devices and device locations. • Interview personnel.	☑	□	□	□

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			In Place	In Place with CCW	Not Applicable	Not in Place
9.5.1.2	POI device surfaces are periodically inspected to detect tampering and unauthorized substitution.	• Examine documented procedures. • Interview responsible personnel. • Observe inspection processes.	☑	□	□	□
9.5.1.3	Training is provided for personnel in POI environments to be aware of attempted tampering or replacement of POI devices, and includes: • Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, before granting them access to modify or troubleshoot devices. • Procedures to ensure devices are not installed, replaced, or returned without verification. • Being aware of suspicious behavior around devices. • Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel.	• Review training materials for personnel in POI environments. • Interview responsible personnel.	☑	□	□	□

Maintain an Information Security Policy

Requirement 12: Support Information Security with Organizational Policies and Programs

Note: *Requirement 12 specifies that merchants have information security policies for their personnel, but these policies can be as simple or complex as needed for the size and complexity of the merchant's operations. The policy document must be provided to all personnel, so they are aware of their responsibilities for protecting payment terminals, any paper documents with account data, etc. If a merchant has no employees, then it is expected that the merchant understands and acknowledges their responsibility for security within their store(s).*

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			In Place	**In Place with CCW**	**Not Applicable**	**Not in Place**
12.1.1	An overall information security policy is: • Established. • Published. • Maintained. • Disseminated to all relevant personnel, as well as to relevant vendors and business partners.	• Examine the information security policy. • Interview personnel.	☑	□	□	□
12.1.2	The information security policy is: • Reviewed at least once every 12 months. • Updated as needed to reflect changes to business objectives or risks to the environment.	• Examine the information security policy. • Interview responsible personnel.	☑	□	□	□
12.1.3	The security policy clearly defines information security roles and responsibilities for all personnel, and all personnel are aware of and acknowledge their information security responsibilities.	• Examine the information security policy. • Interview responsible personnel. • Examine documented evidence.	☑	□	□	□

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			In Place	In Place with CCW	Not Applicable	Not in Place
12.6.1	A formal security awareness program is implemented to make all personnel aware of the entity's information security policy and procedures, and their role in protecting the cardholder data.	• Examine the security awareness program.	☑	□	□	□
12.8.1	A list of all third-party service providers (TPSPs) with which account data is shared or that could affect the security of account data is maintained, including a description for each of the services provided.	• Examine policies and procedures. • Examine list of TPSPs.	☑	□	□	□
12.8.2	Written agreements with TPSPs are maintained as follows: • Written agreements are maintained with all TPSPs with which account data is shared or that could affect the security of the CDE. • Written agreements include acknowledgments from TPSPs that they are responsible for the security of account data the TPSPs possess or otherwise store, process, or transmit on behalf of the entity, or to the extent that they could impact the security of the entity's CDE.	• Examine policies and procedures. • Examine written agreements with TPSPs.	☑	□	□	□
12.8.3	An established process is implemented for engaging TPSPs, including proper due diligence prior to engagement.	• Examine policies and procedures. • Examine evidence. • Interview responsible personnel.	☑	□	□	□

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			In Place	In Place with CCW	Not Applicable	Not in Place
12.8.4	A program is implemented to monitor TPSPs' PCI DSS compliance status at least once every 12 months.	• Examine policies and procedures. • Examine documentation. • Interview responsible personnel.	☑	□	□	□
12.8.5	Information is maintained about which PCI DSS requirements are managed by each TPSP, which are managed by the entity, and any that are shared between the TPSP and the entity.	• Examine policies and procedures. • Examine documentation. • Interview responsible personnel.	☑	□	□	□
12.10.1	An incident response plan exists and is ready to be activated in the event of a suspected or confirmed security incident.	• Examine the incident response plan. • Interview personnel. • Examine documentation from previously reported incidents.	☑	□	□	□

Appendix A: Additional PCI DSS Requirements

Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers

This appendix is not used for merchant assessments.

Appendix A2: Additional PCI DSS Requirements for Entities using SSL/early TLS

This appendix is not used for SAQ B merchant assessments.

Appendix A3: Designated Entities Supplemental Validation (DESV)

This Appendix applies only to entities designated by a payment brand(s) or acquirer as requiring additional validation of existing PCI DSS requirements. Entities required to validate to this Appendix should use the DESV Supplemental Reporting Template and Supplemental Attestation of Compliance for reporting, and consult with the applicable payment brand and/or acquirer for submission procedures.

Appendix B: Compensating Controls Worksheet

Use this worksheet to define compensating controls for any requirement where "YES with CCW" was checked.

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

Refer to Appendices B, C, and D of PCI DSS for information about compensating controls and guidance on how to complete this worksheet.

Requirement Number and Definition:

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

Appendix C: Explanation of Non-Applicability

If the "N/A" (Not Applicable) column was checked in the questionnaire, use this worksheet to explain why the related requirement is not applicable to your organization.

Requirement	**Reason Requirement is Not Applicable**
Example:	
3.4	Cardholder data is never stored electronically