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 3.2.1
Merchant #: 4228993800031357
Merchant Name: Rosie Taxi Cab

June 2018

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: 1/28/2024

Protect Cardholder Data

Requirement 3: Protect stored cardholder data

Note: *For the purposes of Requirement 12, "personnel" refers to full-time 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.*

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
3.2	(c) Is sensitive authentication data deleted or rendered unrecoverable upon completion of the authorization process?	- Review policies and procedures - Examine system configurations - Examine deletion processes	☑	☐	☐	☐
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?	- Examine data sources including: • Incoming transaction data • All logs • History files • Trace files • Database schema • Database contents	☑	☐	☐	☐
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?	- Examine data sources including: • Incoming transaction data • All logs • History files • Trace files • Database schema • Database contents	☑	☐	☐	☐

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
3.2.3	The personal identification number (PIN) or the encrypted PIN block is not stored after authorization?	- Examine data sources including: • Incoming transaction data • All logs • History files • Trace files • Database schema • Database contents	☑	☐	☐	☐
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 full 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.*	- Review policies and procedures - Review roles that need access to displays of full PAN - Examine system configurations - Observe displays of PAN	☑	☐	☐	☐

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

Note: *For the purposes of Requirement 12, "personnel" refers to full-time 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.*

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
4.2	(b) Are policies in place that state that unprotected PANs are not to be sent via end-user messaging technologies?	- Review policies and procedures	☑	☐	☐	☐

Implement Strong Access Control Measures

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

Note: *For the purposes of Requirement 12, "personnel" refers to full-time 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.*

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
7.1	Is access to system components and cardholder data limited to only those individuals whose jobs require such access, as follows: • Is there a written policy for access control that incorporates the following? • Defining access needs and privilege assignments for each role • Restriction of access to privileged user IDs to least privileges necessary to perform job responsibilities, • Assignment of access based on individual personnel's job classification and function • Documented approval (electronically or in writing) by authorized parties for all access, including listing of specific privileges approved	- Examine written access control policy	☑	☐	☐	☐
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?	- Interview personnel - Interview management - Review privileged user IDs	☑	☐	☐	☐
7.1.3	Are access assigned based on individual personnel's job classification and function?	- Interview management - Review user IDs	☑	☐	☐	☐

Requirement 9: Restrict physical access to cardholder data

Note: *For the purposes of Requirement 12, "personnel" refers to full-time 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.*

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
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.	- Review policies and procedures for physically securing media - Interview personnel	☑	☐	☐	☐
9.6	(a) Is strict control maintained over the internal or external distribution of any kind of media?	- Review policies and proceduresfor distribution of media	☑	☐	☐	☐
9.6.1	Is media classified so the sensitivity of the data can be determined?	- Review policies and procedures for media classification - Interview security personnel	☑	☐	☐	☐
9.6.2	Is media sent by secured courier or other delivery method that can be accurately tracked?	- Interview personnel - Examine media distribution tracking logs and documentation	☑	☐	☐	☐
9.6.3	Is management approval obtained prior to moving the media (especially when media is distributed to individuals)?	- Interview personnel - Examine media distribution tracking logs and documentation	☑	☐	☐	☐
9.7	Is strict control maintained over the storage and accessibility of media?	- Review policies and procedures	☑	☐	☐	☐
9.8	(a) Is all media destroyed when it is no longer needed for business or legal reasons?	- Review periodic media destruction policies and procedures	☑	☐	☐	☐
9.8.1	(a) Are hardcopy materials cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed?	- Interview personnel - Examine procedures - Observe processes	☑	☐	☐	☐
	(b) Are storage containers used for materials that contain information to be destroyed secured to prevent access to the contents?	- Examine security of storage containers	☑	☐	☐	☐

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
9.9	Are devices that capture payment card data via direct physical interaction with the card protected against tampering and substitution as follows?					
	(a) Do policies and procedures require that a list of such devices maintained?	- Review policies and procedures	☑	☐	☐	☐
	(b) Do policies and procedures require that devices are periodically inspected to look for tampering or substitution?	- Review policies and procedures	☑	☐	☐	☐
	(c) Do policies and procedures require that personnel are trained to be aware of suspicious behavior and to report tampering or substitution of devices?	- Review policies and procedures	☑	☐	☐	☐
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	- Examine the list of devices	☑	☐	☐	☐
	(b) Is the list accurate and up to date?	- Observe devices and device locations and compare to list	☑	☐	☐	☐
	(c) Is the list of devices updated when devices are added, relocated, decommissioned, etc.?	- Interview personnel	☑	☐	☐	☐

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
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.*	- Interview personnel - Observe inspection processes and compare to defined processes	☑	☐	☐	☐
	(b) Are personnel aware of procedures for inspecting devices?	- Interview personnel	☑	☐	☐	☐
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).	- Review training materials	☑	☐	☐	☐
	(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?	- Interview personnel at POS locations	☑	☐	☐	☐

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security for all personnel

Note: *For the purposes of Requirement 12, "personnel" refers to full-time 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.*

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
12.1	Is a security policy established, published, maintained, and disseminated to all relevant personnel?	- Review the information security policy	☑	☐	☐	☐
12.1.1	Is the security policy reviewed at least annually and updated when the environment changes?	- Review the information security policy - Interview responsible personnel	☑	☐	☐	☐
12.3	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?	- Review usage policies - Interview responsible personnel	☑	☐	☐	☐
12.3.3	A list of all such devices and personnel with access?	- Review usage policies - Interview responsible personnel	☑	☐	☐	☐
12.3.5	Acceptable uses of the technologies?	- Review usage policies - Interview responsible personnel	☑	☐	☐	☐
12.4	Do security policy and procedures clearly define information security responsibilities for all personnel?	- Review information security policy and procedures - Interview a sample of responsible personnel	☑	☐	☐	☐

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
12.5	(b) 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?	- Review information security policy and procedures	☑	☐	☐	☐
12.6	(a) Is a formal security awareness program in place to make all personnel aware of the cardholder data security policy and procedures?	- Review security awareness program	☑	☐	☐	☐
12.8	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 service(s) provided?	- Review policies and procedures - Observe processes - Review list of service providers	☑	☐	☐	☐
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.	- Observe written agreements - Review policies and procedures	☑	☐	☐	☐

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
12.8.3	Is there an established process for engaging service providers, including proper due diligence prior to engagement?	- Observe processes - Review policies and procedures and supporting documentation	☑	☐	☐	☐
12.8.4	Is a program maintained to monitor service providers' PCI DSS compliance status at least annually?	- Observe processes - Review policies and procedures and supporting documentation	☑	☐	☐	☐
12.8.5	Is information maintained about which PCI DSS requirements are managed by each service provider, and which are managed by the entity?	- Observe processes - Review policies and procedures and supporting documentation	☑	☐	☐	☐
12.10.1	(a) Has an incident response plan been created to be implemented in the event of system breach?	- Review the incident response plan - Review incident response plan procedures	☑	☐	☐	☐

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