Payment Card Industry (PCI)
Data Security Standard
Self-Assessment Questionnaire P2PE
and Attestation of Compliance

Merchants using Hardware Payment Terminals in a PCI SSC-Listed P2PE Solution Only – No Electronic Cardholder Data Storage

For use with PCI DSS Version 3.2

Revision 1.1

January 2017

Document Changes

Date	PCI DSS Version	SAQ Revision	Description
N/A	1.0		Not used.
May 2012	2.0		To create SAQ P2PE-HW for merchants using only hardware terminals as part of a validated P2PE solution listed by PCI SSC. This SAQ is for use with PCI DSS v2.0.
February 2014	3.0		To align content with PCI DSS v3.0 requirements and testing procedures and incorporate additional response options.

Table of Contents

Document Changes i

Before you Begin iii

Merchant Eligibility Criteria for SAQ P2PE iii

PCI DSS Self-Assessment Completion Steps iii

Understanding the Self-Assessment Questionnaire iv

Expected Testing .... *iv*

Completing the Self-Assessment Questionnaire v

Guidance for Non-Applicability of Certain, Specific Requirements ....

Before you Begin

Merchant Eligibility Criteria for SAQ P2PE

SAQ P2PE has been developed to address requirements applicable to merchants who process cardholder data only via hardware payment terminals included in a validated and PCI-listed Point-to-Point Encryption (P2PE) solution.

SAQ P2PE merchants do not have access to clear-text cardholder data on any computer system and only enter account data via hardware payment terminals from a PCI SSC-approved P2PE solution. SAQ P2PE merchants may be either brick-and-mortar (card-present) or mail/telephone-order (card-not-present) merchants. For example, a mail/telephone-order merchant could be eligible for SAQ P2PE if they receive cardholder data on paper or over a telephone, and key it directly and only into a validated P2PE hardware device.

SAQ P2PE merchants confirm that, for this payment channel:

- All payment processing is via a validated PCI P2PE solution approved and listed by the PCI SSC;
- The only systems in the merchant environment that store, process or transmit account data are the

Understanding the Self-Assessment Questionnaire

The questions contained in the “PCI DSS Question” column in this self-assessment questionnaire are based on the requirements in the PCI DSS.

Additional resources that provide guidance on PCI DSS requirements and how to complete the self-assessment questionnaire have been provided to assist with the assessment process. An overview of some of these resources is provided below:

Document	**Includes:**
PCI DSS *(PCI Data Security Standard Requirements and Security Assessment Procedures)*	x Guidance on Scoping x Guidance on the intent of all PCI DSS Requirements x Details of testing procedures x Guidance on Compensating Controls
SAQ Instructions and Guidelines documents	x Information about all SAQs and their eligibility criteria x How to determine which SAQ is right for your organization
PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms	x Descriptions and definitions of terms used in the PCI DSS and self-assessment questionnaires

These and other resources can be found on the PCI SSC website *(www.pcisecuritystandards.org)*. Organizations are encouraged to review the PCI DSS and other supporting documents before beginning an assessment,

Expected Testing

T

Completing the Self-Assessment Questionnaire

)RU HDFK TXHVWLRQ WKHUH LV D FKRLFH RI UHVSRQVHV WR LQGLFDWH requirement. Only one response should be selected for each question.

A description of the meaning for each response is provided in the table below:

Response	When to use this response:
Yes	The expected testing has been performed, and all elements of the requirement have been met as stated.
Yes with CCW (Compensating Control Worksheet)	The expected testing has been performed, and the requirement has been met with the assistance of a compensating control. All responses in this column require completion of a Compensating Control Worksheet (CCW) in Appendix B of the SAQ. Information on the use of compensating controls and guidance on how to complete the worksheet is provided in the PCI DSS.
No	Some or all elements of the requirement have not been met, or are in the process of being implemented, or require further testing before it will be known if they are in place.
N/A (Not Applicable)	The requirement does not apply to the RUJDQL]DWLRQ¶V (See Guidance for Non-Applicability of Certain, Specific Requirements below for examples.) All responses in this column require a supporting explanation in Appendix C of the SAQ.

Guidance for Non-Applicability of Certain, Specific Requirements

If any requirements are deemed not applicable to your environment, select the ³1 $´ RSWLRQ IRU WKDW specific requirement, and FRPSOHWH WKH ³([SODQDWLRQ RI 1RQ-$SSOLFDELOLW\´ ZRUNVKHHW LQ $SS HDFK ³1 $.´ HQWU\

Legal Exception

If your organization is subject to a legal restriction that prevents the organization from meeting a PCI DSS UHTXLUHPHQW FKHFN WKH ³1R´ FROXPQ IRU WKDW UHTXLUHPHQW DQG

Part 2b. Description of Payment Card Business	
How and in what capacity does your business store, process and/or transmit cardholder data?	

Part 2c. Locations

List types of facilities (for example, retail outlets, corporate offices, data centers, call centers, etc.) and a summary of locations included in the PCI DSS review.

Type of facility	Number of facilities of this type	Location(s) of facility (city, country)

Part 2f. Third-Party Service Providers	
Does your company use a Qualified Integrator & Reseller (QIR)? If Yes: Name of QIR Company: QIR Individual Name: Description of services provided by QIR:	☐ Yes ☐ No

Does your company

☐

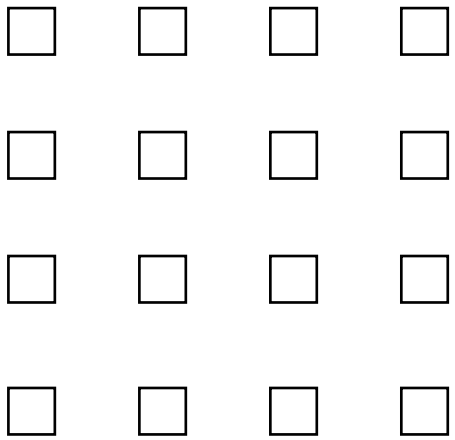
☐

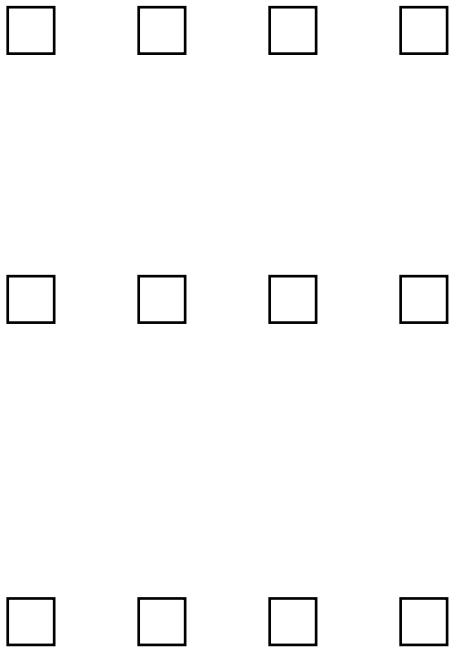
☐

☐

☐

☐





Implement Strong Access Control Measures

Requirement 9: Restrict physical access to cardholder data

Note: *Requirements 9.5 and 9.8 apply only to SAQ P2PE merchants that have paper records (for example, receipts, printed reports, etc.) with account data, including primary account numbers (PANs).*

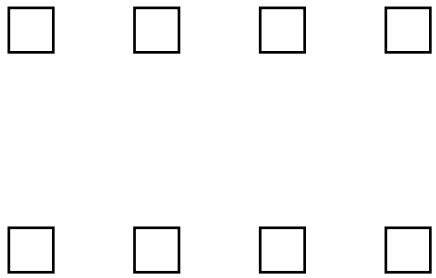
PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
9.5	Are all media physically secured (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes)? *)RU SXUSRVHV RI 5HTXLUHPHQW paper and electronic media containing cardholder data.*	ƒ Review policies and procedures for physically securing media ƒ Interview personnel	☐	☐	☐	☐
9.8	(a) Is all media destroyed when it is no longer needed for business or legal reasons?	ƒ Review periodic media destruction policies and procedures	☐	☐	☐	☐
	(c) 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?	ƒ Review periodic media destruction policies and procedures ƒ Interview personnel ƒ Observe processes	☐	☐	☐	☐
	(b) Are storage containers used for materials that contain information to be destroyed secured to prevent access to the contents?	ƒ Review periodic media destruction policies and procedures ƒ Examine security of storage containers	☐	☐	☐	☐

Guidance: *³<HV´ DQVZHU UHTXLUHPHQWV at 9.5 and 9.8 mean that the merchant securely stores any paper with account data, for example by storing them in a locked drawer, cabinet, or safe, and that the merchant destroys such paper when no longer needed for business purposes. This includes a written document or policy for employees so they know how to secure paper with account data and how to destroy the paper when no longer needed.*

If the merchant never stores any paper with account data, the merchant should mark the ³1 $FFRXQW DQG FRPSOHWH Worksheet, and sign the Attestation of Compliance in Part 3b and complete the worksheet in Appendix C.

PCI DSS Question	Expected Testing	Response			
		☐	☐	☐	☐
		☐	☐	☐	☐
		☐	☐	☐	☐
		☐	☐	☐	☐
		☐	☐	☐	☐
		☐	☐	☐	☐

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.*	ƒ Interview personnel ƒ Observe inspection processes and compare to defined processes	☐	☐	☐	☐
	(b) Are personnel aware of procedures for inspecting devices?	ƒ Interview personnel	☐	☐	☐	☐
9.9.3	Are personnel trained to be aware of attempted tampering or replacement of devices, to include the following?					
	(a) Do training materials for personnel at point-of-sale locations include the following? x 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. x Do not install, replace, or return devices without verification. x Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). x Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).	ƒ Review training materials	☐	☐	☐	☐



Maintain an Information Security Policy

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

Note: Requirement 12 specifies that merchants must have information security policies for their personnel, but these policies can be as simple or F R P S O H [D V Q H H G H G I R U W K H V L] H D Q G F R P S O H [L W \ R I W K H P H U F K D Q W ¶ V R S H U D W L R Q V *aware of their responsibilities for protecting the, payment terminals, any paper documents with cardholder 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)			
			Yes	Yes with CCW	No	N/A
12.1	Is a security policy established, published, maintained, and disseminated to all relevant personnel?	ƒ Review the information security policy	☐	☐	☐	☐
12.1.1	Is the security policy reviewed at least annually and updated when the environment changes?	ƒ Review the information security policy ƒ Interview responsible personnel	☐	☐	☐	☐
Guidance: ³ < H V ´ D Q V Z H U V I R U U H T X L U H P H Q W V D W P H D Q W K D W W K H P H U F K D Q W						
how to protect the store and payment devices in accordance with the P2PE Instruction Manual (PIM), *and who to call in an emergency.*						
12.4	Do security policy and procedures clearly define information security responsibilities for all personnel?	ƒ Review information security policy and procedures ƒ Interview a sample of responsible personnel	☐	☐	☐	☐
Guidance: $ ³ < H V ´ D Q V Z H U V I R U P H D Q V W K D W W K H P H U F K D Q W ¶ V V H F X U L W \ S R O L F \ G H I L Q H V E D						
consistent with the size and complexity of the m H U F K D Q W ¶ V R S H U D W L R Q V) R U H [D P S O H V H F X U L W \ U H V S R Q V L E I						
responsibilities by employee levels, such as the responsibilities expected of a manager/owner and those expected of clerks.						
12.5	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?	ƒ Review information security policy and procedures	☐	☐	☐	☐
Guidance: $ ³ < H V ´ D Q V Z H U P H D Q V W K D W W K H P H U F K D Q W ¶ V V H F X U L W \ S R O L F \ G H I L Q H V E D						
escalation plan required at 12.9.						

PCI DSS Question			Expected Testing	Response (Check one response for each question)			
				Yes	Yes with CCW	No	N/A
12.6	(a)	Is a formal security awareness program in place to make all personnel aware of the cardholder data security policy and procedures?	ƒ Review security awareness program	☐	☐	☐	☐
				☐	☐	☐	☐
				☐	☐	☐	☐

	PCI DSS Question

Appendix C: Explanation of Non-Applicability

If the ³1 $(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:	
12.8	Cardholder data is never shared with service providers.

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in SAQ P2PE (Section 2), dated (SAQ completion date) .

Based on the results documented in the SAQ P2PE noted above, the signatories

☐

☐

☐

☐

☐

☐

Part 3a. Acknowledgement of Status

☐

☐

Part 4. Action Plan for Non-Compliant Status

Select the appropriate response for ³ & R P S to LPCQDSS Requirements ´ I R U H D F K U H T X L U H P H Q

☐ ☐

☐ ☐

☐ ☐