Airwallex

Appendix B - How to Complete the SAQ - A-EP

Part 1. Merchant and Qualified Security Assessor Information					
Part 1a. Merchant Organization Information					
Company Name:			DBA (doing business as):		
Contact Name:			Title:		
Telephone:			E-mail:		
Business Address:			City:		
State/Province:		Country:		Zip:	
URL:					
Part 1b. Qualified Security Assessor Company Information (if applicable)					
Company Name:					
Lead QSA Contact Name:			Title:		
Telephone:			E-mail:		
Business Address:			City:		
State/Province:		Country:		Zip:	
URL:					

Part 1a. Company Name: Should be consistent with the entity of the merchant, unless otherwise stated in Part2b.
URL: Merchant's official website or the main transaction website.

Part 1b. Company Name: If applicable, can be found here:
https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_security_assessors
Note that Level 1 Merchants must use a Qualified Security Assessor.

Part 2. Executive Summary		
Part 2a. Type of Merchant Business (check all that apply)		
☐ Retailer	☐ Telecommunication	☐ Grocery and Supermarkets
☐ Petroleum	☐ E-Commerce	☐ Mail order/telephone order (MOTO)
☐ Others (please specify):		
What types of payment channels does your business serve? ☐ Mail order/telephone order (MOTO) ☐ E-Commerce ☐ Card-present (face-to-face)		Which payment channels are covered by this SAQ? ☐ Mail order/telephone order (MOTO) ☐ E-Commerce ☐ Card-present (face-to-face)
Note: *If your organization has a payment channel or process that is not covered by this SAQ, consult your acquirer or payment brand about validation for the other channels.*		

In the above section, check what is most relevant to your business. In most cases for the SAQ A-EP form, 'E-Commerce' is the most relevant checkbox.

Part 2. Executive Summary *(continued)*

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)
Example: Retail outlets	*3*	*Boston, MA, USA*

Part 2(b) The specific process and treatment method of the following links should be clearly described: How to collect, transfer, store and reuse card information: If you are using HostedPaymentPage, Drop-in and Element, it can be described as: "We do not store, process or transmit cardholder data. The cardholder data is collected, stored, and processed via Airwallex hosted payment page/Airwallexdrop-in/Airwallex element."

**If you are collecting the first six and last four memory card numbers you can mentioned this here.*

Describe in detail the payment card environment. This may include the goods and services consumers purchase, how card payments are processed and service providers and how they interact with the payment card environment.

Part 2(c) Relates to the facilities for your company. When completing the SAQ A-EP form it will most often be a corporate office, data centre etc as companies filling in this form will typically have e-commerce sales.

Part 2d. Payment Applications

Does the organization use one or more Payment Applications? ☐ Yes ☐ No

Provide the following information regarding the Payment Applications your organization uses:

Payment Application Name	Version Number	Application Vendor	Is application PA-DSS Listed?	PA-DSS Listing Expiry date (if applicable)
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	

If applicable, can be found here:
https://www.pcisecuritystandards.org/assessors_and_solutions/payment_applications?agree=true
If not, check NO on the first line above.

Part 2e. Description of Environment	
Provide a ***high-level*** description of the environment covered by this assessment. *For example:* • *Connections into and out of the cardholder data environment (CDE).* • *Critical system components within the CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.*	
Does your business use network segmentation to affect the scope of your PCI DSS environment? *(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation.)*	☐ Yes ☐ No

Part 2. Executive Summary *(continued)*		
Part 2f. Third-Party Service Providers		
Does your company use a Qualified Integrator & Reseller (QIR)?		☐ Yes ☐ No
If Yes:		
Name of QIR Company:		
QIR Individual Name:		
Description of services provided by QIR:		
Does your company share cardholder data with any third-party service providers (for example, Qualified Integrator & Resellers (QIR), gateways, payment processors, payment service providers (PSP), web-hosting companies, airline booking agents, loyalty program agents, etc.)?		☐ Yes ☐ No
If Yes:		
Name of service provider:	**Description of services provided:**	
Note: *Requirement 12.8 applies to all entities in this list.*		

Name of QIR Company: It can be found here:
https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_integrators_and_resellers

Note that you do not need to fill this part unless you collect cardholder data and share to third-party. If you collect cardholder data from Airwallex and shares to other PSP then the PSP should be listed in below form; If the client collects cardholder data from other acquirer and shares to us then we need to be listed.

Part 2g. Eligibility to Complete SAQ A-EP	
Merchant certifies eligibility to complete this shortened version of the Self-Assessment Questionnaire because, for this payment channel:	
☐	Merchant accepts only e-commerce transactions;
☐	All processing of cardholder data, with the exception of the payment page, is entirely outsourced to a PCI DSS validated third-party payment processor;
☐	Merchant's e-commerce website does not receive cardholder data but controls how consumers, or their cardholder data, are redirected to a PCI DSS validated third-party payment processor;
☐	If merchant website is hosted by a third-party provider, the provider is validated to all applicable PCI DSS requirements (e.g., including PCI DSS Appendix A if the provider is a shared hosting provider);
☐	Each element of the payment page(s) delivered to the consumer's browser originates from either the merchant's website or a PCI DSS compliant service provider(s);
☐	Merchant does not electronically store, process, or transmit any cardholder data on merchant systems or premises, but relies entirely on a third party(s) to handle all these functions;
☐	Merchant has confirmed that all third party(s) handling storage, processing, and/or transmission of cardholder data are PCI DSS compliant; **and**
☐	Any cardholder data the merchant retains is on paper (for example, printed reports or receipts), and these documents are not received electronically.

Check all.

Section 2: Self-Assessment Questionnaire A-EP

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:

For Section 2 Merchant needs to complete the questionnaire. There are 12 sections. Where a merchant can respond to the question in the affirmative check 'yes'.
If there are compensating controls please check 'CCW' and add additional information in Appendix B.
If there is any question which is not applicable then check 'N/A' and provide details in Appendix C.

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in SAQ A-EP (Section 2), dated *(SAQ completion date)*.

Based on the results documented in the SAQ A-EP noted above, the signatories identified in Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document: (***check one):***

☐	**Compliant:** All sections of the PCI DSS SAQ are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby *(Merchant Company Name)* has demonstrated full compliance with the PCI DSS.
☐	**Non-Compliant:** Not all sections of the PCI DSS SAQ are complete, or not all questions are answered affirmatively, resulting in an overall **NON-COMPLIANT** rating, thereby *(Merchant Company Name)* has not demonstrated full compliance with the PCI DSS. **Target Date** for Compliance: An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. *Check with your acquirer or the payment brand(s) before completing Part 4.*
☐	**Compliant but with Legal exception:** One or more requirements are marked "No" due to a legal restriction that prevents the requirement from being met. This option requires additional review from acquirer or payment brand. *If checked, complete the following:*

Affected Requirement	Details of how legal constraint prevents requirement being met

(SAQ completion date) replace this with the relevant date.
Replace (Merchant Company Name) with your Company name.

Part 3a. Acknowledgement of Status

Signatory(s) confirms:

(Check all that apply)

☐	PCI DSS Self-Assessment Questionnaire A-EP, Version *(version of SAQ)*, was completed according to the instructions therein.
☐	All information within the above-referenced SAQ and in this attestation fairly represents the results of my assessment in all material respects.
☐	I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
☐	I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
☐	If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.

Check all boxes. In the first checkbox replace (version of SAQ) with A-EP.

Part 3b. Merchant Attestation	
Signature of Merchant Executive Officer ↑	*Date:*
Merchant Executive Officer Name:	*Title:*

Part 3c. Qualified Security Assessor (QSA) Acknowledgement (if applicable)	
If a QSA was involved or assisted with this assessment, describe the role performed:	

Signature of Duly Authorized Officer of QSA Company ↑	*Date:*
Duly Authorized Officer Name:	*QSA Company:*

Part 3d. Internal Security Assessor (ISA) Involvement (if applicable)	
If an ISA(s) was involved or assisted with this assessment, identify the ISA personnel and describe the role performed:	

Part 3(b): *Physical or digital signature is acceptable.*
Part 3(b): Align with Part1b. If applicable, can be found here:
https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_security_assessors

Part 4. Action Plan for Non-Compliant Requirements

Select the appropriate response for "Compliant to PCI DSS Requirements" for each requirement. If you answer "No" to any of the requirements, you may be required to provide the date your Company expects to be compliant with the requirement and a brief description of the actions being taken to meet the requirement.

Check with your acquirer or the payment brand(s) before completing Part 4.

PCI DSS Requirement*	Description of Requirement	Compliant to PCI DSS Requirements (Select One)		Remediation Date and Actions (If "NO" selected for any Requirement)
		YES	NO	
1	Install and maintain a firewall configuration to protect cardholder data.	☐	☐	
2	Do not use vendor-supplied defaults for system passwords and other security parameters.	☐	☐	
3	Protect stored cardholder data.	☐	☐	
4	Encrypt transmission of cardholder data across open, public networks.	☐	☐	
5	Protect all systems against malware and regularly update anti-virus software or programs.	☐	☐	
6	Develop and maintain secure systems and applications.	☐	☐	
7	Restrict access to cardholder data by business need to know.	☐	☐	
8	Identify and authenticate access to system components.	☐	☐	
9	Restrict physical access to cardholder data.	☐	☐	
10	Track and monitor all access to network resources and cardholder data.	☐	☐	
11	Regularly test security systems and processes.	☐	☐	
12	Maintain a policy that addresses information security for all personnel.	☐	☐	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/Early TLS for Card-Present POS POI Terminal Connections.	☐	☐	

This part if you selected 'NO' in Section 2. Please ensure that you inform AWX if you answer no to any of the above.