Payment Card Industry

Data Security Standard

Self-Assessment Questionnaire A and Attestation of Compliance

For use with PCI DSS Version 4.0

Revision 2

Publication Date: July 2023

Document changes

Date	PCI DSS Version	SAQ Revision	Description
October 2008	1.2		To align content with new PCI DSS v1.2 and to implement minor changes noted since original v1.1.
October 2010	2.0		To align content with new PCI DSS v2.0 requirements and testing procedures.
February 2014	3.0		To align content with PCI DSS v3.0 requirements and testing procedures and incorporate additional response options.
April 2015	3.1		Updated to align with PCI DSS v3.1. For details of PCI DSS changes, see PCI DSS - Summary of Changes from PCI DSS Version 3.0 to 3.1.
July 2015	3.1	1.1	Updated version numbering to align with other SAQs.
April 2016	3.2	1.0	Updated to align with PCI DSS v3.2. For details of PCI DSS changes, see PCI DSS - Summary of Changes from PCI DSS Version 3.1 to 3.2. Requirements added from PCI DSS v3.2 Requirements 2, 8, and 12.
January 2017	3.2	1.1	Updated Document Changes to clarify requirements added in the April 2016 update. Added note to Before You Begin section to clarify intent of inclusion of PCI DSS Requirements 2 and 8.
June 2018	3.2.1	1.0	Updated to align with PCI DSS v3.2.1. For details of PCI DSS changes, see PCI DSS - Summary of Changes from PCI DSS Version 3.2 to 3.2.1. Added Requirement 6.2 from PCI DSS v3.2.1.
April 2022	4.0		Updated to align with PCI DSS v4.0. For details of PCI DSS changes, see PCI DSS - Summary of Changes from PCI DSS Version 3.2.1 to 4.0. Rearranged, retitled, and expanded information in the "Completing the Self-Assessment Questionnaire" section (previously titled "Before You Begin"). Aligned content in Sections 1 and 3 of Attestation of Compliance (AOC) with PCI DSS v4.0 Report on Compliance AOC. Added PCI DSS v4.0 requirements. Added appendices to support new reporting responses.
December 2022	4.0	1	Removed "In Place with Remediation" as a reporting option from Requirement Responses table, Attestation of Compliance (AOC) Part 2g, SAQ Section 2 Response column, and AOC Section 3. Also removed former Appendix C. Added "In Place with CCW" to AOC Section 3. Added guidance for responding to future-dated requirements. Clarified note under Eligibility Criteria on page iv that addresses applicability of Requirements 2, 6, 8, and 11 to e-commerce merchants. Clarified notes that address applicability to e-commerce merchants for Requirements 6.4.3, 8, 11, and 11.6.1. Added minor clarifications and addressed typographical errors.
July 2023	4.0	2	Address typographical error in Requirement 11.6.1 SAQ Completion Guidance - changed "merchant's payment page/form" to "TPSP's/payment processor's payment page/form".

Contents

© 2006-2023 PCI Security Standards Council, LLC. All Rights Reserved.

Completing the Self-Assessment Questionnaire

Merchant Eligibility Criteria for Self-Assessment Questionnaire A

Self-Assessment Questionnaire (SAQ) A includes only those PCI DSS requirements applicable to merchants with account data functions completely outsourced to PCI DSS validated and compliant third parties, where the merchant retains only paper reports or receipts with account data.

SAQ A merchants may be either e-commerce or mail/telephone-order merchants (card-not-present) and do not store, process, or transmit any account data in electronic format on their systems or premises.

This SAQ is not applicable to face-to-face channels.

This SAQ is not applicable to service providers.

SAQ A merchants confirm that, for this payment channel:

- The merchant accepts only card-not-present (e-commerce or mail/telephone-order) transactions;
- All processing of account data is entirely outsourced to PCI DSS compliant third-party service provider (TPSP) /payment processor;
- The merchant does not electronically store, process, or transmit any account data on merchant systems or premises, but relies entirely on a TPSP(s) to handle all these functions;
- The merchant has reviewed the PCI DSS Attestation of Compliance form(s) for its TPSP(s) and confirmed that TPSP(s) are PCI DSS compliant for the services being used by the merchant; and
- Any account data the merchant might retain is on paper (for example, printed reports or receipts), and these documents are not received electronically.

Additionally, for e-commerce channels:

- All elements of the payment page(s)/form(s) delivered to the customer's browser originate only and directly from a PCI DSS compliant TPSP/payment processor.

This SAQ includes only those requirements that apply to a specific type of merchant environment, as defined in the above eligibility criteria. If there are PCI DSS requirements applicable to the cardholder data environment that are not covered in this SAQ, it may be an indication that this SAQ is not suitable for the merchant's environment.

Note: For this SAQ, PCI DSS Requirements that address the protection of computer systems (for example, Requirements 2, 6, 8, and 11) AND requirements that refer to the "cardholder data environment" apply to the following e-commerce merchants:

- Those that redirect customers from their website to a TPSP/payment processor for payment processing, and specifically to the merchant web server upon which the redirection mechanism is located.
- Those with a website(s) that includes a TPSP's/payment processor's embedded payment page/form (for example, an inline frame or iFrame), and specifically to the merchant web server that includes the embedded payment page/form.

These PCI DSS requirements are applicable because the above merchant websites impact how the account data is transmitted, even though the websites themselves do not receive account data.

Mail order/telephone order (MOTO) or e-commerce merchants that have completely outsourced all operations (where there is no redirection mechanism from the merchant to the TPSP/payment processor and no embedded payment form from a TPSP/payment processor) and therefore do not have any systems in scope for this SAQ, would consider these requirements to be "not applicable." Refer to guidance on the following pages for how to report requirements that are not applicable.

Defining Account Data, Cardholder Data, and Sensitive Authentication Data

PCI DSS is intended for all entities that store, process, or transmit cardholder data (CHD) and/or sensitive authentication data (SAD) or could impact the security of the cardholder data environment (CDE). Cardholder data and sensitive authentication data are considered account data and are defined as follows:

Account Data	
Cardholder Data includes:	**Sensitive Authentication Data includes:**
• Primary Account Number (PAN) • Cardholder Name • Expiration Date • Service Code	• Full track data (magnetic-stripe data or equivalent on a chip) • Card verification code • PINs/PIN blocks

Refer to PCI DSS Section 2, PCI DSS Applicability Information, for further details.

PCI DSS Self-Assessment Completion Steps

1. Confirm by review of the eligibility criteria in this SAQ and the Self-Assessment Questionnaire Instructions and Guidelines document on the PCI SSC website that this is the correct SAQ for the merchant's environment.
2. Confirm that the merchant environment is properly scoped.
3. Assess the environment for compliance with PCI DSS requirements.
4. Complete all sections of this document:
   - Section 1: Assessment Information (Parts 1 & 2 of the Attestation of Compliance (AOC) - Contact Information and Executive Summary).
   - Section 2 - Self-Assessment Questionnaire A .
   - Section 3: Validation and Attestation Details (Parts 3 & 4 of the AOC - PCI DSS Validation and Action Plan for Non-Compliant Requirements (if Part 4 is applicable)).
5. Submit the SAQ and AOC, along with any other requested documentation-such as ASV scan reports-to the requesting organization (those organizations that manage compliance programs such as payment brands and acquirers).

Expected Testing

The instructions provided in the "Expected Testing" column are based on the testing procedures in PCI DSS and provide a high-level description of the types of testing activities that a merchant is expected to perform to verify that a requirement has been met.

The intent behind each testing method is described as follows:

- Examine: The merchant critically evaluates data evidence. Common examples include documents (electronic or physical), screenshots, configuration files, audit logs, and data files.
- Observe: The merchant watches an action or views something in the environment. Examples of observation subjects include personnel performing a task or process, system components performing a function or responding to input, environmental conditions, and physical controls.
- Interview: The merchant converses with individual personnel. Interview objectives may include confirmation of whether an activity is performed, descriptions of how an activity is performed, and whether personnel have particular knowledge or understanding.

The testing methods are intended to allow the merchant to demonstrate how it has met a requirement. The specific items to be examined or observed and personnel to be interviewed should be appropriate for both the requirement being assessed and the merchant's particular implementation.

Full details of testing procedures for each requirement can be found in PCI DSS.

Requirement Responses

For each requirement item, there is a choice of responses to indicate the merchant's status regarding that requirement. **Only one response should be selected for each requirement item.**

A description of the meaning for each response and when to use each response is provided in the table below:

Response	When to use this response:
In Place	The expected testing has been performed, and all elements of the requirement have been met as stated.
In Place with CCW (Compensating Controls 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 Controls Worksheet (CCW) in Appendix B of this SAQ. Information on the use of compensating controls and guidance on how to complete the worksheet is provided in PCI DSS in Appendices B and C.
Not Applicable	The requirement does not apply to the merchant's environment. (See "Guidance for Not Applicable Requirements" below for examples.) All responses in this column require a supporting explanation in Appendix C of this SAQ.
Not Tested	This response is not applicable to, and not included as an option for, this SAQ. This SAQ was created for a specific type of environment based on how the merchant stores, processes, and/or transmits account data and defines the specific PCI DSS requirements that apply for this environment. Consequently, all requirements in this SAQ must be tested.
Not in Place	Some or all elements of the requirement have not been met, or are in the process of being implemented, or require further testing before the merchant can confirm they are in place. Responses in this column may require the completion of Part 4, if requested by the entity to which this SAQ will be submitted. This response is also used if a requirement cannot be met due to a legal restriction. (See "Legal Exception" below for more guidance).

© 2006-2023 PCI Security Standards Council, LLC. All Rights Reserved.

Guidance for Not Applicable Requirements

If any requirements do not apply to the merchant's environment, select the Not Applicable option for that specific requirement. For example, in this SAQ, requirements for securing all media with cardholder data (Requirements 9.4.1 - 9.4.6) only apply if a merchant stores paper media with cardholder data; if paper media is not stored, the merchant can select Not Applicable for those requirements.

For each response where Not Applicable is selected in this SAQ, complete Appendix C: Explanation of Requirements Noted as Not Applicable.

Guidance for Responding to Future Dated Requirements

In Section 2 below, each new PCI DSS v4.0 requirement or bullet with an extended implementation period includes the following note: "This requirement [or bullet] is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment."

These new requirements are not required to be included in a PCI DSS assessment until the future date has passed. Prior to that future date, any new requirements with an extended implementation date that have not been implemented by the merchant may be marked as Not Applicable and documented in Appendix C: Explanation of Requirements Noted as Not Applicable.

Legal Exception

If your organization is subject to a legal restriction that prevents the organization from meeting a PCI DSS requirement, select Not in Place for that requirement and complete the relevant attestation in Section 3, Part 3 of this SAQ.

> **Note:** A legal restriction is one where meeting the PCI DSS requirement would violate a local or regional law or regulation.
>
> Contractual obligations or legal advice are not legal restrictions.

Use of the Customized Approach

SAQs cannot be used to document use of the Customized Approach to meet PCI DSS requirements. For this reason, the Customized Approach Objectives are not included in SAQs. Entities wishing to validate using the Customized Approach may be able to use the PCI DSS Report on Compliance (ROC) Template to document the results of their assessment.

> Use of the Customized Approach is not supported in SAQs.

The use of the customized approach may be regulated by organizations that manage compliance programs, such as payment brands and acquirers. Questions about use of a customized approach should always be referred to those organizations. This includes whether an entity that is eligible for an SAQ may instead complete a ROC to use a customized approach, and whether an entity is required to use a QSA, or may use an ISA, to complete an assessment using the customized approach. Information about the use of the Customized Approach can be found in Appendices D and E of PCI DSS.

Additional PCI SSC Resources

Additional resources that provide guidance on PCI DSS requirements and how to complete the self-assessment questionnaire have been provided below to assist with the assessment process.

Resource	Includes:
PCI Data Security Standard Requirements and Testing Procedures (PCI DSS)	• Guidance on Scoping • Guidance on the intent of all PCI DSS Requirements • Details of testing procedures • Guidance on Compensating Controls • Appendix G: Glossary of Terms, Abbreviations, and Acronyms
SAQ Instructions and Guidelines	• Information about all SAQs and their eligibility criteria • How to determine which SAQ is right for your organization
Frequently Asked Questions (FAQs)	• Guidance and information about SAQs.
Online PCI DSS Glossary	• PCI DSS Terms, Abbreviations, and Acronyms
Information Supplements and Guidelines	• Guidance on a variety of PCI DSS topics including • Understanding PCI DSS Scoping and Network Segmentation • Third-Party Security Assurance • Multi-Factor Authentication Guidance • Best Practices for Maintaining PCI DSS Compliance
Getting Started with PCI	• Resources for smaller merchants including: • Guide to Safe Payments • Common Payment Systems • Questions to Ask Your Vendors • Glossary of Payment and Information Security Terms • PCI Firewall Basics

These and other resources can be found on the PCI SSC website (www.pcisecuritystandards.org).

Organizations are encouraged to review PCI DSS and other supporting documents before beginning an assessment.

© 2006-2023 PCI Security Standards Council, LLC. All Rights Reserved.

Section 1: Assessment Information

Instructions for Submission

This document must be completed as a declaration of the results of the merchant's self-assessment against the *Payment Card Industry Data Security Standard (PCI DSS) Requirements and Testing Procedures*. Complete all sections. The merchant is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the entity(ies) to which the Attestation of Compliance (AOC) will be submitted for reporting and submission procedures.

Part 1. Contact Information	
Part 1a. Assessed Merchant	
Company Name:	Gracesoft
DBA (doing business as):	
Company mailing address:	Not provided USA
Company main website:	https://apps.gracesoft.com/PMS/EasyWebRez/roomdetails/1798|https://apps, gracesoft.com/pmsui
Company contact name:	Gideon Stanley
Company contact title:	CEO
Contact phone number:	7134932551
Contact e-mail address:	gideon@gracesoft.com
Part 1b. Assessor	
Provide the following information for all assessors involved in the assessment. If there was no assessor for a given assessor type, enter Not Applicable.	
PCI SSC Internal Security Assessor(s)	
ISA name(s):	
Qualified Security Assessor	
Company name:	
Company mailing address:	
Company website:	
Lead Assessor Name:	
Assessor phone number:	
Assessor e-mail address:	
Assessor certificate number:	

Part 2. Executive Summary

Part 2a. Merchant Business Payment Channels (select all that apply):

Indicate all payment channels used by the business that are included in this assessment.

☐ Mail order/telephone order (MOTO)

☒ E-Commerce

☐ Card-present

Are any payment channels not included in this assessment? If yes, indicate which channel(s) is not included in the assessment and provide a brief explanation about why the channel was excluded.	☐ Yes ☐ No

Note: If the organization has a payment channel that is not covered by this SAQ, consult with the entity(ies) to which this AOC will be submitted about validation for the other channels.

Part 2b. Description of Role with Payment Cards

For each payment channel included in this assessment as selected in Part 2a above, describe how the business stores, processes, and/or transmits account data.

Channel	How Business Stores, Processes, and/or Transmits Account Data
E-commerce,	Customer do not enter any credit card information on our website. The credit card information is directly entered on Token Ex - IFrame - our 3rd party data security company, headquartered in Tulsa, Oklahoma

Part 2c. Description of Payment Card 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 POI devices, databases, web servers, etc., and any other necessary payment components, as applicable. • System components that could impact the security of account data.	Our servers are hosted on Microsoft Corporation's Azure Services, and card holder data is directly entered on TokenEx servers. TokenEx sends the data directly to the credit card processing providers such as Authorize.net and stripe.com etc. If there is an error with the Card data, Token Ex send us back the message. And we display to the customer. We do not process any card data on our servers.
Indicate whether the environment includes segmentation to reduce the scope of the assessment. *(Refer to "Segmentation" section of PCI DSS for guidance on segmentation.)*	☒ Yes ☐ No

Part 2. Executive Summary *(continued)*		
Part 2d. In-Scope Locations/Facilities		
List all types of physical locations/facilities (for example, retail locations, corporate offices, data centers, call centers, and mail rooms) in scope for the PCI DSS assessment.		
Facility Type	**Total number of locations (How many locations of this type are in scope)**	**Location(s) of facility (city, country)**
Example: Data centers	*3*	*Boston, MA, USA*
Our software application is hosted on Microsoft Corporation's Azure Services. They are our hosting provider. We do not have any store or outlets. Customers use our booking engine to make online reservations.		

Part 2e. PCI SSC Validated Products and Solutions

Does the merchant use any item identified on any PCI SSC Lists of Validated Products and Solutions *?

□ Yes □ No

Provide the following information regarding each item the merchant uses from PCI SSC's Lists of Validated Products and Solutions.

Name of PCI SSC-validated Product or Solution	Version of Product or Solution	PCI SSC Standard to which product or solution was validated	PCI SSC listing reference number	Expiry date of listing (YYYY-MM-DD)

* For purposes of this document, "Lists of Validated Products and Solutions" means the lists of validated products, solutions, and/or components appearing on the PCI SSC website (www.pcisecuritystandards.org) for example, 3DS Software Development Kits, Approved PTS Devices, Validated Payment Software, Payment Applications (PA-DSS), Point to Point Encryption (P2PE) solutions, Software-Based PIN Entry on COTS (SPoC) solutions, and Contactless Payments on COTS (CPoC) solutions.

Part 2. Executive Summary *(continued)*

Part 2f. Third-Party Service Providers

Does the merchant have relationships with one or more third-party service providers that:	
Store, process, or transmit account data on the merchant's behalf (for example, payment gateways, payment processors, payment service providers (PSPs), and off-site storage)	□ Yes ☒ No
Manage system components included in the scope of the merchant's PCI DSS assessment for example, via network security control services, anti-malware services, security incident and event management (SIEM), contact and call centers, web-hosting services, and IaaS, PaaS, SaaS, and FaaS cloud providers.	□ Yes ☒ No
Could impact the security of the merchant's CDE (for example, vendors providing support via remote access, and/or bespoke software developers)	□ Yes ☒ No

If Yes:

Name of service provider:	**Description of service(s) provided:**
Microsoft Corp	Hosting
Stripe Inc|Moneris Solutions Corporation / Moneris Solutions Inc.|PayPal|CyberSource (including Authorize.Net Managed Hosting and K.K.)	Payment Processing
GraceSoft	Shopping Cart

Note: Requirement 12.8 applies to all entities in this list.

Part 2. Executive Summary *(continued)*

Part 2g. Summary of Assessment (SAQ Section 2 and related appendices)

Indicate below all responses that were selected for each PCI DSS requirement.

PCI DSS Requirement *	Requirement Responses More than one response may be selected for a given requirement. Indicate all responses that apply.			
	In Place	In Place with CCW	Not Applicable	Not in Place
Requirement 2:	☑	□	□	□
Requirement 3:	☑	□	□	□
Requirement 6:	☑	□	☑	□
Requirement 8:	☑	□	□	□
Requirement 9:	☑	□	□	□
Requirement 11:	☑	□	☑	□
Requirement 12:	☑	□	□	□

* PCI DSS Requirements indicated above refer to the requirements in Section 2 of this SAQ.

Part 2h. Eligibility to Complete SAQ A

Merchant certifies eligibility to complete this Self-Assessment Questionnaire because, for this payment channel:

x	The merchant accepts only card-not-present (e-commerce or mail/telephone-order) transaction.
x	All processing of account data is entirely outsourced to a PCI DSS compliant third-party service provider (TPSP)/payment processor.
x	The merchant does not electronically store, process, or transmit any account data on merchant systems or premises, but relies entirely on a TPSP(s) to handle all these functions.
x	The merchant has reviewed the PCI DSS Attestation of Compliance form(s) for its TPSP(s) and confirmed that TPSP(s) are PCI DSS compliant for the services being used by the merchant.
x	Any account data the merchant might retain is on paper (for example, printed reports or receipts), and these documents are not received electronically.
x	Additionally, for e-commerce channels: All elements of the payment page(s)/form(s) delivered to the customer's browser originate only and directly from a PCI DSS compliant TPSP/payment processor.

Section 2: Self-Assessment Questionnaire A

Note: The following requirements mirror the requirements in the PCI DSS Requirements and Testing Procedures document.

Self-assessment completion date: 06/12/2024

Build and Maintain a Secure Network and Systems

Requirement 2: Apply Secure Configurations to All System Components

PCI DSS Requirement		Expected Testing	Response: (Check one response for each requirement)			
			In Place	In Place with CCW	Not Applicable	Not in Place
2.2 System components are configured and managed securely						
Note: For SAQ A, Requirement 2.2.2 applies to e-commerce merchants' vendor default accounts on webservers.						
2.2.2	Vendor default accounts are managed as follows: • If the vendor default account(s) will be used, the default password is changed per Requirement 8.3.6. • If the vendor default account(s) will not be used, the account is removed or disabled.	• Examine system configuration standards. • Examine vendor documentation. • Observe a system administrator logging on using vendor default accounts. • Examine configuration files. • Interview personnel.	☑	☐	☐	☐
	Applicability Notes					
	This applies to ALL vendor default accounts and passwords, including, but not limited to, those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, and Simple Network Management Protocol (SNMP)					

	defaults. This requirement also applies where a system component is not installed within an entity's environment, for example, software and applications that are part of the CDE and are accessed via a cloud subscription service.				

** Refer to the "Requirement Responses" section (page v) for information about these response options.*

© 2006-2023 PCI Security Standards Council, LLC. All Rights Reserved.

Protect Account Data

Requirement 3: Protect Stored Account Data

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

PCI DSS Requirement		Expected Testing	Response: (Check one response for each requirement)			
			In Place	In Place with CCW	Not Applicable	Not in Place
3.1 Processes and mechanisms for protecting stored account data are defined and understood						
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.	☑	□	□	□
SAQ Completion Guidance: *Selection of any of the In Place responses for Requirement 3.1.1 means that, if the merchant has paper storage of account data, the merchant has policies and procedures in place that govern merchant activities for Requirement 3. This helps to ensure personnel are aware of and following security policies and documented operational procedures for managing the secure storage of any paper records with account data. If merchant does not store paper records with account data, mark this requirement as Not Applicable and complete Appendix C: Explanation of Requirements Noted as Not Applicable.*						
3.2 Storage of account data is kept to a minimum.						
3.2.1	Account data storage is kept to a minimum through implementation of data retention and disposal policies, procedures, and processes that include at least the following:	• Examine the data retention and disposal policies, procedures, and processes. • Interview personnel. • Examine files and system records on system components where account data is stored.	☑	□	□	□

© 2006-2023 PCI Security Standards Council, LLC. All Rights Reserved.

	• Coverage for all locations of stored account data. • Coverage for any sensitive authentication data (SAD) stored prior to completion of authorization. This bullet is a best practice until its effective date; refer to Applicability Notes below for details. • Limiting data storage amount and retention time to that which is required for legal or regulatory, and/or business requirements. • Specific retention requirements for stored account data that defines length of retention period and includes a documented business justification. • Processes for secure deletion or rendering account data unrecoverable when no longer needed per the retention policy. A process for verifying, at least once every three months, that stored account data exceeding the defined retention period has been securely deleted or rendered unrecoverable.	• Observe the mechanisms used to render account data unrecoverable.				
	Applicability Notes					
	Where account data is stored by a TPSP (for example, in a cloud environment), entities are responsible for working with their service providers to understand how the TPSP meets this requirement for the entity. Considerations include ensuring that all geographic instances of a data element are securely					

	deleted. The bullet above (for coverage of SAD stored prior to completion of authorization) is a best practice until 31 March 2025, after which it will be required as part of Requirement 3.2.1 and must be fully considered during a PCI DSS assessment.				
SAQ Completion Guidance: *Selection of any of the In Place responses for Requirement 3.2.1 means that if a merchant stores any paper (for example, receipts or paper reports) that contain account data, the merchant only stores the paper as long as it is needed for business, legal, and/or regulatory reasons and destroys the paper once it is no longer needed. If a merchant never prints or stores any paper containing account data, mark this requirement as Not Applicable and complete Appendix C: Explanation of Requirements Noted as Not Applicable.*					

** Refer to the "Requirement Responses" section (page v) for information about these response options.*

Maintain a Vulnerability Management Program

Requirement 6: Develop and Maintain Secure Systems and Software

Note: For SAQ A, Requirement 6 applies to web servers that host the page(s) on the merchant's website(s) that provide the address (the URL) of the TPSP's payment page /form to the merchant's customers.

PCI DSS Requirement		Expected Testing	Response: (Check one response for each requirement)			
			In Place	In Place with CCW	Not Applicable	Not in Place
6.3 Security vulnerabilities are identified and addressed.						
6.3.1	Security vulnerabilities are identified and managed as follows: • New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). • Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. • Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment. • Bullet intentionally left blank for this SAQ.	• Examine policies and procedures. • Interview responsible personnel. • Examine documentation. • Observe processes.	☑	□	□	□

© 2006-2023 PCI Security Standards Council, LLC. All Rights Reserved.

	Applicability Notes					
	This requirement is not achieved by, nor is it the same as, vulnerability scans performed for Requirements 11.3.1 and 11.3.2. This requirement is for a process to actively monitor industry sources for vulnerability information and for the entity to determine the risk ranking to be associated with each vulnerability.					
6.3.3	All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows: • Critical or high-security patches /updates are installed within one month of release. • Bullet intentionally left blank for this SAQ.	• Examine policies and procedures. • Examine system components and related software. • Compare list of security patches installed to recent vendor patch lists.	☑	□	□	□
6.4 Public-facing web applications are protected against attacks.						
Note: For SAQ A, Requirement 6.4.3 applies to a merchant's website(s) that includes a TPSP's/payment processor's embedded payment page/form (for example, an inline frame or iFrame).						
6.4.3	All payment page scripts that are loaded and executed in the consumer's browser are managed as follows					
	A method is implemented to confirm that each script is authorized.	• Examine policies and procedures. • Interview responsible personnel. • Examine inventory records. • Examine system configurations.	□	□	☑	□
	A method is implemented to assure the integrity of each script.		□	□	☑	□
	An inventory of all scripts is maintained with written justification as to why each is necessary.		□	□	☑	□
	Applicability Notes					

	This requirement applies to all scripts loaded from the entity's environment and scripts loaded from third and fourth parties. This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.				

** Refer to the "Requirement Responses" section (page v) for information about these response options.*

© 2006-2023 PCI Security Standards Council, LLC. All Rights Reserved.

Implement Strong Access Control Measures

Requirement 8: Identify Users and Authenticate Access to System Components

Note: For SAQ A, Requirement 8 applies to merchant webservers that host the page(s) that either 1) redirects customers from the merchant website to a TPSP/payment processor for payment processing (for example, with a URL redirect) or 2) includes a TPSP's/payment processor's embedded payment page/form (for example, an inline frame or iFrame).

PCI DSS Requirement		Expected Testing	Response: (Check one response for each requirement)			
			In Place	In Place with CCW	Not Applicable	Not in Place
8.2 User identification and related accounts for users and administrators are strictly managed throughout an account's lifecycle.						
8.2.1	All users are assigned a unique ID before access to system components or cardholder data is allowed.	• Interview responsible personnel. • Examine audit logs and other evidence.	☑	□	□	□
	Applicability Notes					
	This requirement is not intended to apply to user accounts within point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals).					
8.2.2	Group, shared, or generic accounts, or other shared authentication credentials are only used when necessary on an exception basis, and are managed as follows: • Account use is prevented unless needed for an exceptional circumstance. • Use is limited to the time needed for the exceptional circumstance. • Business justification for use is documented.	• Examine user account lists on system components and applicable documentation. • Examine authentication policies and procedures. • Interview system administrators.	☑	□	□	□

© 2006-2023 PCI Security Standards Council, LLC. All Rights Reserved.

	• Use is explicitly approved by management. • Individual user identity is confirmed before access to an account is granted. • Every action taken is attributable to an individual user.					
	Applicability Notes					
	This requirement is not intended to apply to user accounts within point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals).					
8.2.5	Access for terminated users is immediately revoked.	• Examine information sources for terminated users. • Review current user access lists. • Interview responsible personnel.	☑	□	□	□
8.3 Strong authentication for users and administrators is established and managed						
8.3.1	All user access to system components for users and administrators is authenticated via at least one of the following authentication factors: • 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 element.	• Examine documentation describing the authentication factor(s) used. • For each type of authentication factor used with each type of system component, observe the authentication process.	☑	□	□	□

	Applicability Notes This requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals). This requirement does not supersede multi-factor authentication (MFA) requirements but applies to those in-scope systems not otherwise subject to MFA requirements. A digital certificate is a valid option for "something you have" if it is unique for a particular user					
8.3.5	If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they are set and reset for each user as follows: • Set to a unique value for first-time use and upon reset. • Forced to be changed immediately after the first use.	• Examine procedures for setting and resetting passwords/passphrases. • Observe security personnel.	☑	□	□	□
8.3.6	If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they meet the following minimum level of complexity: • A minimum length of 12 characters (or IF the system does not support 12 characters, a minimum length of eight characters). • Contain both numeric and alphabetic characters.	• Examine system configuration settings.	☑	□	□	□

	Applicability Notes					
	This requirement is not intended to apply to: • User accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals). • Application or system accounts, which are governed by requirements in section 8.6. This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment. Until 31 March 2025, passwords must be a minimum length of seven characters in accordance with PCI DSS v3.2.1 Requirement 8.2.3.					
8.3.7	Individuals are not allowed to submit a new password/passphrase that is the same as any of the last four passwords/passphrases used.	• Examine system configuration settings.	☑	□	□	□
	Applicability Notes					
	This requirement is not intended to apply to user accounts within point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals).					
8.3.9	If passwords/passphrases are used as the only authentication factor for user access (i. e., in any singlefactor authentication implementation) then either: • Passwords/passphrases are changed at least once every 90 days, OR • The security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly.	• Inspect system configuration settings.	☑	□	□	□

© 2006-2023 PCI Security Standards Council, LLC. All Rights Reserved.

	Applicability Notes					
	This requirement applies to in-scope system components that are not in the CDE because these components are not subject to MFA requirements. This requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals). This requirement does not apply to service providers' customer accounts but does apply to accounts for service provider personnel.					

** Refer to the "Requirement Responses" section (page v) for information about these response options.*

Requirement 9: Restrict Physical Access to Cardholder Data

PCI DSS Requirement		Expected Testing	Response: (Check one response for each requirement)			
			In Place	In Place with CCW	Not Applicable	Not in Place
9.4 Media with cardholder data is securely stored, accessed, distributed, and destroyed.						
Note: For SAQ A, Requirements at 9.4 only apply to merchants with paper records (for example, receipts or printed reports) with account data, including primary account numbers (PANs).						
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: - Bullet intentionally left blank for this SAQ. - Media is sent by secured courier or other delivery method that can be accurately tracked. - Bullet intentionally left blank for this SAQ.	- 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). Applicability Notes Individuals approving media movements should have the appropriate level of management authority to grant this approval. However, it is not specifically required that such individuals have "manager" as part of their title.	- Examine documented procedures. - Examine offsite media tracking logs. - Interview responsible personnel.	☑	□	□	□
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.	- Examine the periodic media destruction policy. - Observe processes. - Interview personnel. - Observe storage containers.	☑	□	□	□

	- Materials are stored in secure storage containers prior to destruction.					
	Applicability Notes					
	These requirements for media destruction when that media is no longer needed for business or legal reasons are separate and distinct from PCI DSS Requirement 3.2.1, which is for securely deleting cardholder data when no longer needed per the entity's cardholder data retention policies.					

SAQ Completion Guidance:
Selection of any of the In Place responses for Requirements at 9.4 means that the merchant securely stores any paper media with account data, for example by storing the paper 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, mark this requirement as Not Applicable and complete Appendix C: Explanation of Requirements Noted as Not Applicable.

** Refer to the "Requirement Responses" section (page v) for information about these response options.*

Requirement 11: Test Security of Systems and Networks Regularly

Note: For SAQ A, Requirement 11 applies to merchant webservers that host the page(s) that either 1) redirects customers from the merchant website to a TPSP/payment processor for payment processing (for example, with a URL redirect) or 2) includes a TPSP's/payment processor's embedded payment page/form (for example, an inline frame or iFrame).

PCI DSS Requirement		Expected Testing	Response: (Check one response for each requirement)			
			In Place	In Place with CCW	Not Applicable	Not in Place
11.3 External and internal vulnerabilities are regularly identified, prioritized, and addressed.						
11.3.2	External vulnerability scans are performed as follows: - At least once every three months. - By PCI SSC Approved Scanning Vendor (ASV).	- Examine ASV scan reports.	☑	□	□	□

© 2006-2023 PCI Security Standards Council, LLC. All Rights Reserved.

	- Vulnerabilities are resolved and ASV Program Guide requirements for a passing scan are met. - Rescans are performed as needed to confirm that vulnerabilities are resolved per the ASV Program Guide requirements for a passing scan.					
	Applicability Notes					
	For initial PCI DSS compliance, it is not required that four passing scans be completed within 12 months if the assessor verifies: *1.* The most recent scan result was a passing scan, *2.* The entity has documented policies and procedures requiring scanning at least once every three months, and *3.* Vulnerabilities noted in the scan results have been corrected as shown in a rescan(s). However, for subsequent years after the initial PCI DSS assessment, passing scans at least every three months must have occurred. ASV scanning tools can scan a vast array of network types and topologies. Any specifics about the target environment (for example, load balancers, third-party providers, ISPs, specific configurations, protocols in use, scan interference) should be worked out between the ASV and scan customer. Refer to the ASV Program Guide published on the PCI SSC website for scan customer responsibilities, scan preparation, etc.					
11.3.2.1	External vulnerability scans are performed after any significant change as follows: - Vulnerabilities that are scored 4.0 or higher by the CVSS are resolved. - Rescans are conducted as needed. - Scans are performed by qualified personnel and organizational independence of the tester exists (not required to be a QSA or ASV).	- Examine change control documentation. - Interview personnel. - Examine external scan, and as applicable rescan reports.	☑	☐	☐	☐

11.6 Unauthorized changes on payment pages are detected and responded to						
Note: For SAQ A, Requirement 11.6.1 applies to a merchant's website that includes a TPSP's/payment processor's embedded payment page/form (for example, an inline frame or iFrame).						
11.6.1	A change- and tamper-detection mechanism is deployed as follows					
	To alert personnel to unauthorized modification (including indicators of compromise, changes, additions, and deletions) to the HTTP headers and the contents of payment pages as received by the consumer browser.	• Examine system settings and mechanism configuration settings. • Examine monitored payment pages. • Examine results from monitoring activities. • Examine the mechanism configuration settings. • Examine configuration settings. • Interview responsible personnel. • If applicable, examine the targeted risk analysis.	□	□	☑	□
	The mechanism is configured to evaluate the received HTTP header and payment page.		□	□	☑	□
	The mechanism functions are performed as follows: • At least once every seven days **OR** • Periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1).		□	□	☑	□
	Applicability Notes					
	The intention of this requirement is not that an entity installs software in the systems or browsers of its consumers, but rather that the entity uses techniques such as those described under Examples in the					

	PCI DSS Guidance column (of PCI DSS Requirements and Testing Procedures) to prevent and detect unexpected script activities. This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.				
SAQ Completion Guidance: *If a merchant uses URL redirects, where the merchant hosts the page(s) on their website(s) that provides the address (the URL) of the TPSP's/payment processor's payment page/form to the merchant's customers, the merchant marks this requirement as Not Applicable and completes Appendix C: Explanation of Requirements Noted as Not Applicable.*					

** Refer to the "Requirement Responses" section (page v) for information about these response options.*

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 Requirement		Expected Testing	Response: (Check one response for each requirement)			
			In Place	In Place with CCW	Not Applicable	Not in Place
12.8 Risk to information assets associated with third-party service provider (TPSP) relationships is managed						
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.	☑	□	□	□
	Applicability Notes					
	The use of a PCI DSS compliant TPSP does not make an entity PCI DSS compliant, nor does it remove the entity's responsibility for its own PCI DSS compliance.					
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	• Examine policies and procedures. • Examine written agreements with TPSPs.	☑	□	□	□

	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.					
	Applicability Notes					
	The exact wording of an acknowledgment will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgment does not have to include the exact wording provided in this requirement. Evidence that a TPSP is meeting PCI DSS requirements (for example, a PCI DSS Attestation of Compliance (AOC) or a declaration on a company's website) is not the same as a written agreement specified in this requirement.					
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.	☑	□	□	□
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.	☑	□	□	□
	Applicability Notes					
	Where an entity has an agreement with a TPSP for meeting PCI DSS requirements on behalf of the entity (for example, via a firewall service), the entity must work with the TPSP to make sure the applicable PCI DSS requirements are met. If the TPSP does not meet those applicable PCI DSS requirements, then those requirements are also "not in place" for the entity.					

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.	☑	□	□	□
SAQ Completion Guidance: *Selection of any of the In Place responses for requirements at 12.8.1 through 12.8.5 means that the merchant has a list of, and agreements with, service providers they share account data with or that could impact the security of the merchant's cardholder data environment. For example, such agreements would be applicable if a merchant uses a document-retention company to store paper documents that include account data or if a merchant's vendor accesses merchant systems remotely to perform maintenance.*						
12.10 Suspected and confirmed security incidents that could impact the CDE are responded to immediately.						
12.10.1	An incident response plan exists and is ready to be activated in the event of a suspected or confirmed security incident. The plan includes, but is not limited to: • Roles, responsibilities, and communication and contact strategies in the event of a suspected or confirmed security incident, including notification of payment brands and acquirers, at a minimum. • Incident response procedures with specific containment and mitigation activities for different types of incidents. • Business recovery and continuity procedures. • Data backup processes. • Analysis of legal requirements for reporting compromises. • Coverage and responses of all critical system components.	• Examine the incident response plan. • Interview personnel. • Examine documentation from previously reported incidents.	☑	□	□	□

© 2006-2023 PCI Security Standards Council, LLC. All Rights Reserved.

	• Reference or inclusion of incident response procedures from the payment brands.					

SAQ Completion Guidance:
Selection of any of the In Place responses for Requirement 12.10.1 means that the merchant has documented an incident response and escalation plan to be used for emergencies, consistent with the size and complexity of the merchant's operations. For example, such a plan could be a simple document posted in the back office that lists who to call in the event of various situations with an annual review to confirm it is still accurate, but could extend all the way to a full incident response plan including backup "hotsite" facilities and thorough annual testing. This plan should be readily available to all personnel as a resource in an emergency

** Refer to the "Requirement Responses" section (page v) for information about these response options.*

© 2006-2023 PCI Security Standards Council, LLC. All Rights Reserved.

Appendix A: Additional PCI DSS Requirements

Appendix A1: Additional PCI DSS Requirements for Multi-Tenant Service Providers

This Appendix is not used for merchant assessments.

Appendix A2: Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections

This Appendix is not used for SAQ A 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

This Appendix must be completed to define compensating controls for any requirement where In Place with CCW was selected.

> **Note:** Only entities that have a legitimate and documented technological or business constraint can consider the use of compensating controls to achieve compliance.
>
> Refer to Appendices B and C in PCI DSS for information about compensating controls and guidance on how to complete this worksheet.

Requirement Number and Definition:

	Information required	Explanation
1. Constraints	Document the legitimate technical or business constraints precluding compliance with the original requirement.	
2. Definition of Compensating Controls	Define the compensating controls: explain how they address the objectives of the original control and the increased risk, if any.	
3. Objective	Define the objective of the original control.	
	Identify the objective met by the compensating control. **Note:** This can be, but is not required to be, the stated Customized Approach Objective listed for this requirement in PCI DSS.	
4. Identified Risk	Identify any additional risk posed by the lack of the original control.	
5. Validation of Compensating Controls	Define how the compensating controls were validated and tested.	
6. Maintenance	Define process(es) and controls in place to maintain compensating controls.	

© 2006-2023 PCI Security Standards Council, LLC. All Rights Reserved.

Appendix C: Explanation of Requirements Noted as Not Applicable

This Appendix must be completed for each requirement where Not Applicable was selected.

Requirement	Reason Requirement is Not Applicable
Example:	
Requirement 3.5.1	Account data is never stored electronically
Requirement 6.4.3.a	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.
Requirement 6.4.3.b	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.
Requirement 6.4.3.c	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.
Requirement 11.6.1.a	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.
Requirement 11.6.1.b	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.
Requirement 11.6.1.c	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

© 2006-2023 PCI Security Standards Council, LLC. All Rights Reserved.

Appendix D: Explanation of Requirements Noted as Not Tested

This Appendix is not used for SAQ A merchant assessments.

Annotation

MIDs/ Accounts covered by this Attestation-of-Compliance

Mid / Account	Company name	Address Line 1
merchant_720107	Gracesoft	Not provided

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation:

This AOC is based on results noted in SAQ A (Section 2) dated 06/12/2024.

Based on the results documented in the SAQ A noted above, each signatory identified in any of Parts 3b-3d, as applicable, assert(s) the following compliance status for the merchant identified in Part 2 of this document.

Select one:

☒ **Compliant:** All sections of the PCI DSS SAQ are complete and all requirements are marked as being either 1) In Place, 2) In Place with CCW, or 3) Not Applicable, resulting in an overall **COMPLIANT** rating; thereby Gracesoft has demonstrated compliance with all PCI DSS requirements included in this SAQ .

☐ **Non-Compliant:**

Not all sections of the PCI DSS SAQ are complete, or one or more requirements are marked as Not in Place, resulting in an overall **NON-COMPLIANT** rating; thereby Gracesoft has not demonstrated compliance with the PCI DSS requirements included in this SAQ.

Target Date for Compliance:

A merchant submitting this form with a Non-Compliant status may be required to complete the Action Plan in Part 4 of this document. Confirm with the entity to which this AOC will be submitted before completing Part 4.

☐ **Compliant but with Legal exception:** One or more requirements in the PCI DSS SAQ are marked as Not in Place due to a legal restriction that prevents the requirement from being met and all other requirements are marked as being either 1) In Place, 2) In Place with CCW, or 3) Not Applicable, resulting in an overall **COMPLIANT BUT WITH LEGAL EXCEPTION** rating; thereby Gracesoft has demonstrated compliance with all PCI DSS requirements included in this SAQ except those noted as Not in Place due to a legal restriction.

This option requires additional review from the entity to which this AOC will be submitted. If selected, complete the following:

Affected Requirement	Details of how legal constraint prevents requirement from being met

© 2006-2023 PCI Security Standards Council, LLC. All Rights Reserved.

Part 3a. Merchant Acknowledgement

Signatory(s) confirms:
(Select all that apply)

☒	PCI DSS Self-Assessment Questionnaire A , Version 4.0, was completed according to the instructions therein.
☒	All information within the above-referenced SAQ and in this attestation fairly represents the results of the merchant's assessment in all material respects.
☒	PCI DSS controls will be maintained at all times, as applicable to the merchant's environment.

Part 3b. Merchant Attestation

Signature of Merchant Executive Officer This was electronically signed by Gracesoftware on behalf of Gracesoft Gideon Stanley	*Date:* 06/12/2024
Merchant Executive Officer Name: Gideon Stanley	*Title:* CEO

Part 3c. Qualified Security Assessor (QSA) Acknowledgement

If a QSA was involved or assisted with this assessment, indicate the role performed:	☐ QSA performed testing procedures. ☐ QSA provided other assistance. If selected, describe all role(s) performed:
Signature of Lead QSA	*Date:*
Lead QSA Name:	
Signature of Duly Authorized Officer of QSA Company	*Date:*
Duly Authorized Officer Name:	*QSA Company:*

Part 3d. PCI SSC Internal Security Assessor (ISA) Involvement

If an ISA(s) was involved or assisted with this assessment, indicate the role performed:	☐ ISA(s) performed testing procedures. ☐ ISA(s) provided other assistance. If selected, describe all role(s) performed:

Part 4. Action Plan for Non-Compliant Requirements

Only complete Part 4 upon request of the entity to which this AOC will be submitted, and only if the Assessment has a Non-Compliant status noted in Section 3.

If asked to complete this section, select the appropriate response for "Compliant to PCI DSS Requirements" for each requirement below. For any "No" responses, include the date the merchant expects to be compliant with the requirement and a brief description of the actions being taken to meet the requirement.

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	
2	Apply secure configurations to all system components	□	□	
3	Protect stored account data	□	□	
6	Develop and maintain secure systems and software	□	□	
8	Identify users and authenticate access to system components	□	□	
9	Restrict physical access to cardholder data	□	□	
11	Test security of systems and networks regularly	□	□	
12	Support information security with organizational policies and programs	□	□	

* PCI DSS Requirements indicated above refer to the requirements in Section 2 of this SAQ.