

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

Card-not-present Merchants,
All Cardholder Data Functions Fully Outsourced

For use with PCI DSS Version 3.2.1

June 2018



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.



Table of Contents

Document Changes	s	i
Before You Begin		iii
PCI DSS Self-Ass	essment Completion Steps	iv
Understanding th	e Self-Assessment Questionnaire	iv
Expected Testing	j	iv
Completing the S	elf-Assessment Questionnaire	v
Guidance for Non	-Applicability of Certain, Specific Requirements	v
Legal Exception		v
Section 1: Asses	ssment Information	1
Section 2: Self-A	Assessment Questionnaire A	4
Build and Maintai	n a Secure Network and Systems	4
	Do not use vendor-supplied defaults for system passwords and other security parameters	
Maintain a Vulner	ability Management Program	5
Requirement 6:	Develop and maintain secure systems and applications	5
Implement Strong	Access Control Measures	6
Requirement 8:	Identify and authenticate access to system components	
Requirement 9:	Restrict physical access to cardholder data	
	mation Security Policy	
•	Maintain a policy that addresses information security for all personnel	
• •	litional PCI DSS Requirements	
Appendix A1:	Additional PCI DSS Requirements for Shared Hosting Providers	
Appendix A2:	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Pi POS POI terminal connections	
Appendix A3:	Designated Entities Supplemental Validation (DESV)	
	npensating Controls Worksheet	
Appendix C: Exp	lanation of Non-Applicability	13
Section 3: Valida	ation and Attactation Datails	14



Before You Begin

SAQ A has been developed to address requirements applicable to merchants whose cardholder data functions are completely outsourced to validated third parties, where the merchant retains only paper reports or receipts with cardholder 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 cardholder data in electronic format on their systems or premises.

SAQ A merchants confirm that, for this payment channel:

- Your company accepts only card-not-present (e-commerce or mail/telephone-order) transactions;
- All processing of cardholder data is entirely outsourced to PCI DSS validated third-party service providers;
- Your company does not electronically store, process, or transmit any cardholder data on your systems or premises, but relies entirely on a third party(s) to handle all these functions;
- Your company has confirmed that all third party(s) handling storage, processing, and/or transmission of cardholder data are PCI DSS compliant; and
- Any cardholder data your company retains 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) delivered to the consumer's browser originate only and directly from a PCI DSS validated third-party service provider(s).

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

This shortened version of the SAQ includes questions that apply to a specific type of small merchant environment, as defined in the above eligibility criteria. If there are PCI DSS requirements applicable to your environment that are not covered in this SAQ, it may be an indication that this SAQ is not suitable for your environment. Additionally, you must still comply with all applicable PCI DSS requirements in order to be PCI DSS compliant.

Note: For this SAQ, PCI DSS Requirements that address the protection of computer systems (for example, Requirements 2, 6, and 8) apply to e-commerce merchants that redirect customers from their website to a third party for payment processing, and specifically to the merchant web server upon which the redirection mechanism is located. 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 third party) 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.



PCI DSS Self-Assessment Completion Steps

- 1. Identify the applicable SAQ for your environment—refer to the *Self-Assessment Questionnaire Instructions and Guidelines* document on PCI SSC website for information.
- 2. Confirm that your environment is properly scoped and meets the eligibility criteria for the SAQ you are using (as defined in Part 2g of the Attestation of Compliance).
- 3. Assess your environment for compliance with applicable PCI DSS requirements.
- 4. Complete all sections of this document:
 - Section 1 (Parts 1 & 2 of the AOC) Assessment Information and Executive Summary
 - Section 2 PCI DSS Self-Assessment Questionnaire (SAQ A)
 - Section 3 (Parts 3 & 4 of the AOC) Validation and Attestation Details and Action Plan for Non-Compliant Requirements (if applicable)
- 5. Submit the SAQ and Attestation of Compliance (AOC), along with any other requested documentation—such as ASV scan reports—to your acquirer, payment brand or other requester.

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)	 Guidance on Scoping Guidance on the intent of all PCI DSS Requirements Details of testing procedures Guidance on Compensating Controls
SAQ Instructions and Guidelines documents	 Information about all SAQs and their eligibility criteria How to determine which SAQ is right for your organization
PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms	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

The instructions provided in the "Expected Testing" column are based on the testing procedures in the PCI DSS, and provide a high-level description of the types of testing activities that should be performed in order to verify that a requirement has been met. Full details of testing procedures for each requirement can be found in the PCI DSS.



Completing the Self-Assessment Questionnaire

For each question, there is a choice of responses to indicate your company's status regarding that 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.
Control Worksheet)	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	The requirement does not apply to the organization's environment. (See
(Not Applicable)	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 "N/A" option for that specific requirement, and complete the "Explanation of Non-Applicability" worksheet in Appendix C for each "N/A" entry.

Legal Exception

If your organization is subject to a legal restriction that prevents the organization from meeting a PCI DSS requirement, check the "No" column for that requirement and complete the relevant attestation in Part 3.



Section 1: Assessment Information

Instructions for Submission

This document must be completed as a declaration of the results of the merchant's self-assessment with the *Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS).* Complete all sections: The merchant is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact acquirer (merchant bank) or the payment brands to determine reporting and submission procedures.

1a. Merchant Organi	zation Information	า				
ny Name:	HackerBay, I		DBA (doing business as):	Fyipe		
t Name:	Nawaz Dhan	dala	Title:	CEO		
one:	+1-510-775-0	208	E-mail:	nawazdhanda	ala@had	ckerbay.io
ss Address:	2711 Centerville	, STE 400	City:	Wilmingto	n	
Province:	DE	Country:	United States	}	Zip:	19808
	https://fyipe.co	om	ı			
1b. Qualified Securit	y Assessor Comp	any Inforn	nation (if applic	cable)		
ny Name:	SES A&T, S	SS, INC.				
SA Contact Name:	KAMRIN DANIE	ELLE	Title:	AUDIT OF	FICER	
one:	+1-651-697-54	30	E-mail:	audit@se	esatte	st.com
ss Address:	25 Broadway 9th	Floor	City:	New York	(
Province:	NY	Country:	United State	S	Zip:	55112
	https://sesatte	est.com				
. Executive Summ	ary					
2a. Type of Merchan	t Business (check	all that ap	ply)			
ailer	☐ Telecommur	nication	☐ Groce	ry and Supern	narkets	
roleum	☐ E-Commerce	е	☐ Mail o	rder/telephone	order	(MOTO)
ers (please specify):	Software Service					
ypes of payment channe	els does your busine	ess Whic	h payment chan	nels are cover	ed by tl	nis SAQ?
l order/telephone order	(MOTO)	м	ail order/telepho	ne order (MO	TO)	
ommerce		E	-Commerce			
d-present (face-to-face))	□ c	ard-present (face	e-to-face)		
ommerce	s a payment channe	E C	-Commerce ard-present (face s that is not cov	e-to-	-face)	-face)



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?

Users add card information when they register for an account on Fyipe. HackerBay does not store, transmit any cardholder data on it's servers. Cardholder data is sent to our third party payment partners.

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
Google Cloud Platform (Data Center)	1	United States
Amazon Web Services (Data Center)	1	United States
Microsoft Azure (Data Center)	1	United States
On Prem Data Center	2	Germany and Denmark
On Prem Data Center	1	Boston, United States
On Prem Data Center	1	Hyderabad, India
Part 2d. Payment Application		

Provide the following info	ormation regar	ding the Payment	Applications your organia	zation uses:
Payment Application Name	Version Number	Application Vendor	Is application PA-DSS Listed?	PA-DSS Listing Expiry date (if applicable)
Stripe	v3.2	Stripe, Inc.	Yes ☐ No	28 Oct 2022
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	

Part 2e. Description of Environment

Provide a <u>high-level</u> 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.
- Assessement of registration API's, upgrade account API's,
- SSL/TLS setup for database and servers.
- Encryption at rest for databases.

Does your business	use network segment	ation to affect the	scope of your PCI [oss
environment?				

(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation.)

Yes	☐ No
-	



Pa	rt 2. Executive Summary (continued)		
Par	t 2f. Third-Party Service Providers		
Doe	es your company use a Qualified Integrator &	Reseller (QIR)?	☐ Yes No
If Y	es:		
Nar	ne of QIR Company:		
QIF	R Individual Name:		
Des	cription of services provided by QIR:		
exa ser	es your company share cardholder data with mple, Qualified Integrator & Resellers (QIR) vice providers (PSP), web-hosting companie nts, etc.)?	, gateways, payment processors, payment	Yes No
If Y	es:		
Nar	ne of service provider:	Description of services provided:	
Str	ipe	Payment Processor	
Not	e: Requirement 12.8 applies to all entities in	this list.	
Р	art 2g. Eligibility to Complete SAQ A		
	chant certifies eligibility to complete this sho	rtened version of the Self-Assessment Ques	stionnaire
bec	ause, for this payment channel:		
	Merchant accepts only card-not-present (e	-commerce or mail/telephone-order) transac	tions);
	All processing of cardholder data is entirely providers;	outsourced to PCI DSS validated third-part	y service
	Merchant does not electronically store, pro or premises, but relies entirely on a third pa	cess, or transmit any cardholder data on me arty(s) to handle all these functions;	rchant systems
	Merchant has confirmed that all third partyr cardholder data are PCI DSS compliant; are	(s) handling storage, processing, and/or tran	smission of
	Any cardholder data the merchant retains i these documents are not received electron	s on paper (for example, printed reports or r ically.	eceipts), and
	Additionally, for e-commerce channels:		
	All elements of the payment page(s) delive from a PCI DSS validated third-party service	red to the consumer's browser originate only be provider(s).	y and directly



Section 2: Self-Assessment Questionnaire A

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

Self-assessment completion date:

Build and Maintain a Secure Network and Systems

10/21/2019

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

	2.1
(b) Are unnecessary default accounts removed or disabled before installing a system on the network?	(a) Are vendor-supplied defaults always changed before installing a system on the network? This applies to ALL default 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, Simple Network Management Protocol (SNMP) community strings, etc.).
Review policies and procedures. Review vendor documentation. Examine system configurations and account settings. Interview personnel.	Expected Testing Review policies and procedures. Examine vendor documentation. Observe system configurations and account settings. Interview personnel.
	Yes
	Check one response for each question. Yes with CCW No N/A
	No
	N/A



Maintain a Vulnerability Management Program

Requirement 6: Develop and maintain secure systems and applications

	PCI DSS Question		Expected Testing	(Check o	Response (Check one response for each question	ise for each qu	lestion)
				Yes	Yes with CCW	Z o	N/A
6.2	(a) Are all system components and software protected from known vulnerabilities by installing applicable vendor-supplied security patches?	•	Review policies and procedures.				
	(b) Are critical security patches installed within one month of release?		Review policies and procedures. Examine system components. Compare list of security patches installed to recent vendor patch lists.				



Implement Strong Access Control Measures

Requirement 8: Identify and authenticate access to system components

8.2.3		8.2	8.1. 3	8.1.1	
 (a) Are user password parameters configured to require passwords/passphrases meet the following? A minimum password length of at least seven characters Contain both numeric and alphabetic characters Alternatively, the passwords/passphrases must have complexity and strength at least equivalent to the parameters specified above. 	passphrase Something you have, such as a token device or smart card Something you are, such as a biometric	In addition to assigning a unique ID, is one or more of the following methods employed to authenticate all users? Something you know, such as a password or	Is access for any terminated users immediately deactivated or removed?	Are all users assigned a unique ID before allowing them to access system components or cardholder data?	PCI DSS Question
•					
Examine system configuration settings to verify password parameters.		Review password procedures. Observe authentication processes.	Review password procedures. Examine terminated users accounts. Review current access lists. Observe returned physical authentication devices.	Review password procedures. Interview personnel.	Expected Testing
					(Check o
					Check one response for each question) Yes with No N/A
					ie for each o
					question)



හ ග		
Are group, shared, or generic accounts, passwords, or other authentication methods prohibited as follows: Generic user IDs and accounts are disabled or removed; Shared user IDs for system administration activities and other critical functions do not exist; and Shared and generic user IDs are not used to administer any system components?		PCI DSS Question
 Review policies and procedures. Examine user ID lists. Interview personnel. 		Expected Testing
	Yes	(Check
	Yes with CCW	Response (Check one response for each question
	No	onse e for each q
	N/A	uestion)

Requirement 9: Restrict physical access to cardholder data

				Interview security personnel.		
				 Review policies and procedures for media classification. 	Is media classified so the sensitivity of the data can be determined?	9.6.1
					(b) Do controls include the following:	
				 Review policies and procedures for distribution of media. 	(a) Is strict control maintained over the internal or external distribution of any kind of media?	9.6
					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. 	Are all media physically secured (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes)?	9.5
N/A	No	Yes with CCW	Yes			
uestion)	onse e for each q	Response (Check one response for each question)	(Check o	Expected Testing	PCI DSS Question	



Interview personnel. Examine media distribution tracking logs and documentation. Interview personnel. Examine media distribution tracking logs and documentation. Review periodic media destruction policies and procedures. Review periodic media destruction policies and procedures. Interview personnel. Correct Ves with Yes with Yes with No N/A Yes with Yes with Yes with Yes with No N/A Interview personnel. Interview personnel. Interview personnel.
Yes
Yes with



Maintain an Information Security Policy

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

contractors and consultants who are "resident" on the entity's site or otherwise have access to the company's site cardholder data environment. Note: For the purposes of Requirement 12, "personnel" refers to full-time part-time employees, temporary employees and personnel, and

12.8.3		12.8.2	12.8.1	12.8		
Is there an established process for engaging service providers, including proper due diligence prior to engagement?	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.	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?	Is a list of service providers maintained, including a description of the service(s) provided?	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:		PCI DSS Ougstion
• • • • • • • • • • • • • • • • • • •		· ·				
Observe processes. Review policies and procedures and supporting documentation.		Observe written agreements. Review policies and procedures.	Review policies and procedures. Observe processes. Review list of service providers.			Expected Testing
					Yes	(Check c
					Yes with CCW	Response (Check one response for each question)
					N _o	onse e for each o
					N/A	question)





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 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

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.

Reason Requirement is Not Applicable
Cardholder data is never stored electronically
Cardholder data is never stored electronically with HackerBay, Inc. We use third party PCI compliant payment providers to store our customers card information



Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

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

Based on the results documented in the SAQ A 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*):

	PCI DSS SAQ are complete, all questions answered affirmatively, ANT rating; thereby (Merchant Company Name) has demonstrated full
•	ns of the PCI DSS SAQ are complete, or not all questions are answered rall NON-COMPLIANT rating, thereby (<i>Merchant Company Name</i>) has be with the PCI DSS.
Target Date for Compliance:	
,	ith a status of Non-Compliant may be required to complete the Action Check with your acquirer or the payment brand(s) before completing
	eption: One or more requirements are marked "No" due to a legal uirement from being met. This option requires additional review from
If checked, complete the following	ing:
Affected Requirement	Details of how legal constraint prevents requirement being met

Part 3a. Acknowledgement of Status

•	atory(s) confirms: ck all that apply)
	PCI DSS Self-Assessment Questionnaire A, 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.



Part 3. PCI DSS Validation (continued)

Part 3a. Acknowledgement of Status (continued)



No evidence of full track data¹, CAV2, CVC2, CID, or CVV2 data², or PIN data³ storage after transaction authorization was found on ANY system reviewed during this assessment.

ASV scans are being completed by the PCI SSC Approved Scanning Vendor (ASV Name)

Part 3b. Merchant Attestation



Signature of Merchant Executive Officer ↑ Date: 10/21/2019

Merchant Executive Officer Name: NAWAZ DHANDALA Title: CEO

Part 3c. Qualified Security Assessor (QSA) Acknowledgement (if applicable)

If a QSA was involved or assisted with this assessment, describe the role performed:

Audit of Fyipe Software, Databases, and process pertaining to PCI SAQ-A

Hamoring Conselle

Signature of Duly Authorized Officer of QSA Company ↑ Date: 10/21/2019

Duly Authorized Officer Name: KAMRIN DANIELLE QSA Company: SES A&C, SSS INC.

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:

Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full track data after transaction authorization. The only elements of track data that may be retained are primary account number (PAN), expiration date, and cardholder name.

² The three- or four-digit value printed by the signature panel or on the face of a payment card used to verify card-not-present transactions.

³ Personal identification number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.



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	requirement	
2	Do not use vendor-supplied defaults for system passwords and other security parameters.				
6	Develop and maintain secure systems and applications.				
8	Identify and authenticate access to system components.				
9	Restrict physical access to cardholder data.				
12	Maintain a policy that addresses information security for all personnel.				

^{*} PCI DSS Requirements indicated here refer to the questions in Section 2 of the SAQ.

SIGNED BY KAMRIN DANIELLE AUDIT OFFICER, SES ATTESTATION AND COMPLIANCE, SSS INC. 10/21/2019

danvin famille

SIGNED BY NAWAZ DHANDALA CEO, HACKERBAY. INC. 10/21/2019

rawayshandde









