

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.

Part 1. Merchant and Qualified Security Assessor Information

Part 1a. Merchant Organization Information

Company Name:	Growing the Faith	DBA (doing business as):	OneParish		
Contact Name:	Ryan Kreager	Title:	CEO		
Telephone:	574-265-3099	E-mail:	ryan@oneparish.com		
Business Address:	1400 E Angela Blvd	City:	South Bend		
State/Province:	IN	Country:	USA	Zip:	46617
URL:	www.oneparish.com				

Part 1b. Qualified Security Assessor Company Information (if applicable)

Company Name:					
Lead QSA Contact Name:		Title:			
Telephone:		E-mail:			
Business Address:		City:			
State/Province:		Country:		Zip:	
URL:					

Part 2. Executive Summary

Part 2a. Type of Merchant Business (check all that apply)

<input type="checkbox"/> Retailer	<input type="checkbox"/> Telecommunication	<input type="checkbox"/> Grocery and Supermarkets
<input type="checkbox"/> Petroleum	<input checked="" type="checkbox"/> E-Commerce	<input type="checkbox"/> Mail order/telephone order (MOTO)
<input type="checkbox"/> Others (please specify):		

What types of payment channels does your business serve? <input type="checkbox"/> Mail order/telephone order (MOTO) <input checked="" type="checkbox"/> E-Commerce <input type="checkbox"/> Card-present (face-to-face)	Which payment channels are covered by this SAQ? <input type="checkbox"/> Mail order/telephone order (MOTO) <input checked="" type="checkbox"/> E-Commerce <input type="checkbox"/> Card-present (face-to-face)
--	---

Note: If your organization has a payment channel or process that is not covered by this SAQ, consult your acquirer or payment brand about validation for the other channels.

Part 2b. Description of Payment Card Business

How and in what capacity does your business store, process and/or transmit cardholder data?

Part 2c. Locations

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

Type of facility	Number of facilities of this type	Location(s) of facility (city, country)
<i>Example: Retail outlets</i>	3	<i>Boston, MA, USA</i>
Mobile App Development HQ	1	South Bend, IN, USA

Part 2d. Payment Application

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

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

Payment Application Name	Version Number	Application Vendor	Is application PA-DSS Listed?	PA-DSS Listing Expiry date (if applicable)
Stripe	2016-07-06	Stripe	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	

Part 2e. Description of Environment

Provide a **high-level** description of the environment covered by this assessment.

For example:

- *Connections into and out of the cardholder data environment (CDE).*
- *Critical system components within the CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.*

Connections to Stripe API, data storage, databases, web servers, mobile apps for iOS and Android, and all other applicable hardware and software systems

Does your business use network segmentation to affect the scope of your PCI DSS environment?
(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation)

Yes No

Part 2f. Third-Party Service Providers

<p>Does your company use a Qualified Integrator & Reseller (QIR)?</p> <p>If Yes:</p> <p>Name of QIR Company:</p> <p>QIR Individual Name:</p> <p>Description of services provided by QIR:</p>	<p><input type="checkbox"/> Yes <input checked="" type="checkbox"/> No</p>
<p>Does your company share cardholder data with any third-party service providers (for example, Qualified Integrator & Resellers (QIR), gateways, payment processors, payment service providers (PSP), web-hosting companies, airline booking agents, loyalty program agents, etc.)?</p>	<p><input type="checkbox"/> Yes <input checked="" type="checkbox"/> No</p>

If Yes:

Name of service provider:	Description of services provided:

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

Part 2g. Eligibility to Complete SAQ A

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

- Merchant 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;
- Merchant does not electronically store, process, or transmit any cardholder data on merchant systems or premises, but relies entirely on a third party(s) to handle all these functions;
- Merchant has confirmed that all third party(s) handling storage, processing, and/or transmission of cardholder data are PCI DSS compliant; **and**
- Any cardholder data the merchant retains is on paper (for example, printed reports or receipts), and these documents are not received electronically.
- 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).


Section 2: Self-Assessment Questionnaire A

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

Self-assessment completion date:





Build and Maintain a Secure Network and Systems


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

PCI DSS Question	Expected Testing	Response (Check one response for each question)			
		Yes	Yes with CCW	No	N/A
<p> 2.1</p> <p>(a) Are vendor-supplied defaults always changed before installing a system on the network?</p> <p><i>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.).</i></p>	<ul style="list-style-type: none"> Review policies and procedures Examine vendor documentation Observe system configurations and account settings Interview personnel 	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p>(b) Are unnecessary default accounts removed or disabled before installing a system on the network?</p>	<ul style="list-style-type: none"> Review policies and procedures Review vendor documentation Examine system configurations and account settings Interview personnel 	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>




Implement Strong Access Control Measures






Requirement 8: Identify and authenticate access to system components

PCI DSS Question	Expected Testing	Response (Check one response for each question)			
		Yes	Yes with CCW	No	N/A
<p> 8.1.1</p> <p>Are all users assigned a unique ID before allowing them to access system components or cardholder data?</p>	<ul style="list-style-type: none"> ▪ Review password procedures ▪ Interview personnel 	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p> 8.1.3</p> <p>Is access for any terminated users immediately deactivated or removed?</p>	<ul style="list-style-type: none"> ▪ Review password procedures ▪ Examine terminated users accounts ▪ Review current access lists ▪ Observe returned physical authentication devices 	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p> 8.2</p> <p>In addition to assigning a unique ID, is one or more of the following methods employed to authenticate all users?</p> <ul style="list-style-type: none"> ▪ 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 	<ul style="list-style-type: none"> ▪ Review password procedures ▪ Observe authentication processes 	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p> 8.2.3</p> <p>(a) Are user password parameters configured to require passwords/passphrases meet the following?</p> <ul style="list-style-type: none"> • A minimum password length of at least seven characters • Contain both numeric and alphabetic characters <p>Alternatively, the passwords/passphrases must have complexity and strength at least equivalent to the parameters specified above.</p>	<ul style="list-style-type: none"> ▪ Examine system configuration settings to verify password parameters 	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI DSS Question	Expected Testing	Response (Check one response for each question)			
		Yes	Yes with CCW	No	N/A
<p> 9.5</p> <p>Are group, shared, or generic accounts, passwords, or other authentication methods prohibited as follows:</p> <ul style="list-style-type: none"> ▪ 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? 	<ul style="list-style-type: none"> ▪ Review policies and procedures ▪ Examine user ID lists ▪ Interview personnel 	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Requirement 9: Restrict physical access to cardholder data

PCI DSS Question	Expected Testing	Response (Check one response for each question)			
		Yes	Yes with CCW	No	N/A
<p> 9.5</p> <p>Are all media physically secured (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes)? <i>For purposes of Requirement 9, "media" refers to all paper and electronic media containing cardholder data.</i></p>	<ul style="list-style-type: none"> ▪ Review policies and procedures for physically securing media ▪ Interview personnel 	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p> 9.6</p> <p>(a) Is strict control maintained over the internal or external distribution of any kind of media? (b) Do controls include the following:</p>	<ul style="list-style-type: none"> ▪ Review policies and procedures for distribution of media 	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p> 9.6.1</p> <p>Is media classified so the sensitivity of the data can be determined?</p>	<ul style="list-style-type: none"> ▪ Review policies and procedures for media classification ▪ Interview security personnel 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>




PCI DSS Question	Expected Testing	Response (Check one response for each question)			
		Yes	Yes with CCW	No	N/A
9.6.2 	<p>Is media sent by secured courier or other delivery method that can be accurately tracked?</p> <ul style="list-style-type: none"> Interview personnel Examine media distribution tracking logs and documentation 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
9.6.3 	<p>Is management approval obtained prior to moving the media (especially when media is distributed to individuals)?</p> <ul style="list-style-type: none"> Interview personnel Examine media distribution tracking logs and documentation 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
9.7 	<p>Is strict control maintained over the storage and accessibility of media?</p> <ul style="list-style-type: none"> Review policies and procedures 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
9.8 	<p>(a) Is all media destroyed when it is no longer needed for business or legal reasons?</p> <p>(c) Is media destruction performed as follows:</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
9.8.1 	<p>(a) Are hardcopy materials cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed?</p> <ul style="list-style-type: none"> Review periodic media destruction policies and procedures Interview personnel Observe processes <p>(b) Are storage containers used for materials that contain information to be destroyed secured to prevent access to the contents?</p> <ul style="list-style-type: none"> Examine security of storage containers 	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>




Maintain an Information Security Policy

Don't Have a Security Policy? Click Here to Download a Template.

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

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

PCI DSS Question	Expected Testing	Response (Check one response for each question)			
		Yes	Yes with CCW	No	N/A
12.8 Are policies and procedures maintained and implemented to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows:					
 12.8.1 Is a list of service providers maintained, including a description of the service(s) provided?	<ul style="list-style-type: none"> Review policies and procedures Observe processes Review list of service providers 	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
 12.8.2 Is a written agreement maintained that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process, or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment? Note: The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.	<ul style="list-style-type: none"> Observe written agreements Review policies and procedures 	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
 12.8.3 Is there an established process for engaging service providers, including proper due diligence prior to engagement?	<ul style="list-style-type: none"> Observe processes Review policies and procedures and supporting documentation 	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI DSS Question	Expected Testing	Response (Check one response for each question)			
		Yes	Yes with CCW	No	N/A
 2.8.4 Is a program maintained to monitor service providers' PCI DSS compliance status at least annually?	<ul style="list-style-type: none"> ▪ Observe processes ▪ Review policies and procedures and supporting documentation 	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
 2.8.5 Is information maintained about which PCI DSS requirements are managed by each service provider, and which are managed by the entity?	<ul style="list-style-type: none"> ▪ Observe processes ▪ Review policies and procedures and supporting documentation 	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
 2.10.1 (a) Has an incident response plan been created to be implemented in the event of system breach?	<ul style="list-style-type: none"> ▪ Review the incident response plan ▪ Review incident response plan procedures 	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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)**:

<input checked="" type="checkbox"/>	<p>Compliant: All sections of the PCI DSS SAQ are complete, all questions answered affirmatively, resulting in an overall COMPLIANT rating; thereby (<i>Merchant Company Name</i>) has demonstrated full compliance with the PCI DSS.</p>						
<input type="checkbox"/>	<p>Non-Compliant: Not all sections of the PCI DSS SAQ are complete, or not all questions are answered affirmatively, resulting in an overall NON-COMPLIANT rating, thereby (<i>Merchant Company Name</i>) has not demonstrated full compliance with the PCI DSS.</p> <p>Target Date for Compliance:</p> <p>An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. <i>Check with your acquirer or the payment brand(s) before completing Part 4.</i></p>						
<input type="checkbox"/>	<p>Compliant but with Legal exception: One or more requirements are marked “No” due to a legal restriction that prevents the requirement from being met. This option requires additional review from acquirer or payment brand.</p> <p><i>If checked, complete the following:</i></p> <table border="1" style="width: 100%;"> <thead> <tr> <th style="width: 40%;">Affected Requirement</th> <th>Details of how legal constraint prevents requirement being met</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> </tbody> </table>	Affected Requirement	Details of how legal constraint prevents requirement being met				
Affected Requirement	Details of how legal constraint prevents requirement being met						

Part 3a. Acknowledgement of Status

Signatory(s) confirms:

(Check all that apply)


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



Part 3a. Acknowledgement of Status (continued)

<input checked="" type="checkbox"/>	No evidence of full track data ¹ , CAV2, CVC2, CID, or CVV2 data ² , or PIN data ³ storage after transaction authorization was found on ANY system reviewed during this assessment.
<input type="checkbox"/>	ASV scans are being completed by the PCI SSC Approved Scanning Vendor (<i>ASV Name</i>)

Part 3b. Merchant Attestation

	Date: 4/19/2017
Signature of Merchant Executive Officer ↑	
Merchant Executive Officer Name:	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:	
--	--

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

Part 3d. Internal Security Assessor (ISA) Involvement (if applicable)

If an ISA(s) was involved or assisted with this assessment, identify the ISA personnel and describe the role performed:	
---	--

¹ 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	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8	Identify and authenticate access to system components	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9	Restrict physical access to cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12	Maintain a policy that addresses information security for all personnel	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

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

