Payment Card Industry (PCI)
Data Security Standard

Attestation of Compliance for Self-Assessment Questionnaire A

Version 3.1
April 2015

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:	KENTUCKY SOCIETY OF HEALTHCARE R		DBA(s):	[KENTUCKY SOCIETY OF HEALTHCARE R]	
Contact Name:	John Chaney		Title:		
ISA Name(s)(if applicable):			Title:		
Telephone:	270-745-1429		E-mail:	jachaney@chc.net	
Business Address:	800 PARK ST		City:	BOWLING GREEN	
State/Province:	Kentucky	Country:	US	Zip:	42101

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

Company Name:	This is a self-assessment completed using tools provided by Trustwave.				
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)

☐ Retailer	☐ Telecommunication	☐ Grocery and Supermarkets
☐ Petroleum	☒ E-Commerce	☐ Mail/Telephone-Order
☒ Others (please specify): Nonprofit		

What types of payment channels does your business serve?	Which payment channels are covered by this SAQ?
☐ Mail order/telephone order (MOTO)	☐ Mail order/telephone order (MOTO)
☒ E-Commerce	☒ E-Commerce
☐ Card-present (face-to-face)	☐ 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 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 and a summary of locations included in the PCI DSS review (for example, retail outlets, corporate offices, data centers, call centers, etc.)

Type of facility	Location(s) of facility (city, country)
Primary Address	BOWLING GREEN, US

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)
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ 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.*	
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	
Does your company share cardholder data with any third-party service providers (for example, gateways, payment processors, payment service providers (PSP), web-hosting companies, airline booking agents, loyalty program agents, etc.)?	☒ Yes ☐ No

If Yes

Name of service provider:	**Description of services provided:**
Authorize.net	PAYMENT_PROCESSING
StarChapter	WEB_SITE_HOSTING

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 payment acceptance and processing are entirely outsourced to PCI DSS validated third-party service providers;
☒	Merchant has no direct control of the manner in which cardholder data is captured, processed, transmitted, or stored;
☒	Merchant does not electronically store, proce ss, 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 acceptance, storage, processing, and/or transmission of cardholder data are PCI DSS compliant; and
☒	Merchant retains only paper reports or receipts with cardholder data, and these documents are not received electronically.
☒	*Additionally, for e-commerce channels:* The entirety of all payment pages delivered to the consumer's browser originates directly from a third-party PCI DSS validated service provider(s).

Section 2: Self-Assessment Questionnaire A

This Attestation of Compliance reflects the results of a self-assessment, which is documented in an accompanying SAQ.

The assessment documented in this attestation and in the SAQ was completed on:	2016-07-25 10:03 AM
Have compensating controls been used to meet any requirement in the SAQ?	☐ Yes ☒ No
Were any requirements in the SAQ identified as being not applicable (N/A)?	☒ Yes ☐ No
Were any requirements in the SAQ unable to be met due to a legal constraint?	☐ Yes ☒ No

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

Based on the results noted in the SAQ A dated *2016-07-25 10:03 AM*, 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 as of *:* ***(check one):***

☒ **Compliant**: All sections of the PCI DSS SAQ are complete, and all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby *KENTUCKY SOCIETY OF HEALTHCARE R* has demonstrated full compliance with the PCI DSS.

☐ **Non-Compliant**: Not all sections of the PCI DSS SAQ are complete, or not all questions are answered affirmatively, resulting in an overall **NON-COMPLIANT** rating, thereby *KENTUCKY SOCIETY OF HEALTHCARE R* has not demonstrated full compliance with the PCI DSS.

Target Date for Compliance:

An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. *Check with your acquirer or the payment brand(s) before completing Part 4.*

☐ **Compliant but with legal exception**: One or more requirements are marked "No" due to a legal restriction that prevents the requirement from being met. This option requires additional review from acquirer or payment brand.
If checked, complete the following:

Affected Requirement	Details of how legal constraint prevents requirement being met

Part 3a. Acknowledgement of Status

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

☒	PCI DSS Self-Assessment Questionaire A,Version *v3.1*, 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 full 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.
☒	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.
☐	ASV scans are being completed by the PCI SSC Approved Scanning Vendor (*Trustwave*) .

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 3b. Merchant Attestation	
This SAQ was electronically signed by John Chaney, Treasurer, KENTUCKY SOCIETY OF HEALTHCARE R, on 2016-07-25 10:03 AM	
Signature of Merchant Executive Officer↑	*Date:* 2016-07-25 10:03 AM
Merchant Executive Officer Name: John Chaney	*Title*: Treasurer

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

Signature of QSA↑	*Date:*
QSA Individual Name:	*QSA Company Represented*:

Part 3d. ISA Acknowledgement (if applicable)	
If a ISA was involved or assisted with this assessment, describe the role performed:	

Signature of ISA↑	*Date:*
ISA Name:	*Title*:

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	Compliance Status (Select One)		Remediation Date and Actions (if Compliance Status is "NO")
		YES	NO	
9	Restrict physical access to cardholder data	☒	☐	
12	Maintain a policy that addresses information security for all personnel	☒	☐	