Payment Card Industry (PCI)

Data Security Standard

Attestation of Compliance for Self-Assessment Questionnaire D – Service Providers

For use with PCI DSS Version 3.2.1

July 2018

Section 1: Assessment Information

Instructions for Submission

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

Part 1. Service Provider and Qualified Security Assessor Information					
Part 1a. Service Provider Organization Information					
Company Name:	SiteSpect, Inc.		DBA (doing business as):		
Contact Name:	Paul Silevitch		Title:	VP of Engineering	
Telephone:	1 (800) 683-9832		E-mail:	psilevitch@sitespect.com	
Business Address:	275 Grove Street, Suite 3-400		City:	Auburndale	
State/Province:	MA	Country:	USA	Zip:	02466
URL:	www.sitespect.com				
Part 1b. Qualified Security Assessor Company Information (if applicable)					
Company Name:	System Experts Corporation				
Lead QSA Contact Name:	Joseph Kurfehs		Title:	Head of Compliance Practice	
Telephone:	888-749-9800		E-mail:	joseph.kurfehs@ systemexperts.com	
Business Address:	11 Spiller Rd.		City:	Sudbury	
State/Province:	MA	Country:	USA	Zip:	01776
URL:	www.systemexperts.com				

Part 2. Executive Summary

Part 2a. Scope Verification

Services that were INCLUDED in the scope of the PCI DSS Assessment (check all that apply):

Name of service(s) assessed:	SiteSpect application

Type of service(s) assessed:

Hosting Provider:	**Managed Services (specify):**	**Payment Processing:**
☐ Applications / software	☐ Systems security services	☐ POS / card present
☐ Hardware	☐ IT support	☐ Internet / e-commerce
☐ Infrastructure / Network	☐ Physical security	☐ MOTO / Call Center
☐ Physical space (co-location)	☐ Terminal Management System	☐ ATM
☐ Storage	☐ Other services (specify):	☐ Other processing (specify):
☐ Web		
☐ Security services		
☐ 3-D Secure Hosting Provider		
☐ Shared Hosting Provider		
☐ Other Hosting (specify):		
☐ Account Management	☐ Fraud and Chargeback	☐ Payment Gateway/Switch
☐ Back-Office Services	☐ Issuer Processing	☐ Prepaid Services
☐ Billing Management	☐ Loyalty Programs	☐ Records Management
☐ Clearing and Settlement	☐ Merchant Services	☐ Tax/Government Payments
☐ Network Provider		
☒ Others (specify): multi-variant web testing		

***Note**: These categories are provided for assistance only, and are not intended to limit or predetermine an entity's service description. If you feel these categories don't apply to your service, complete "Others."*

If you're unsure whether a category could apply to your service, consult with the applicable payment brand.

Part 2a. Scope Verification *(continued)*

Services that are provided by the service provider but were NOT INCLUDED in the scope of the PCI DSS Assessment (check all that apply):

Name of service(s) not assessed:	

Type of service(s) not assessed:

Hosting Provider:	**Managed Services (specify):**	**Payment Processing:**
☐ Applications / software	☐ Systems security services	☐ POS / card present
☐ Hardware	☐ IT support	☐ Internet / e-commerce
☐ Infrastructure / Network	☐ Physical security	☐ MOTO / Call Center
☐ Physical space (co-location)	☐ Terminal Management System	☐ ATM
☐ Storage	☐ Other services (specify):	☐ Other processing (specify):
☐ Web		
☐ Security services		
☐ 3-D Secure Hosting Provider		
☐ Shared Hosting Provider		
☐ Other Hosting (specify):		
☐ Account Management	☐ Fraud and Chargeback	☐ Payment Gateway/Switch
☐ Back-Office Services	☐ Issuer Processing	☐ Prepaid Services
☐ Billing Management	☐ Loyalty Programs	☐ Records Management
☐ Clearing and Settlement	☐ Merchant Services	☐ Tax/Government Payments
☐ Network Provider		
☐ Others (specify):		

Provide a brief explanation why any checked services were not included in the assessment:	

Part 2b. Description of Payment Card Business

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	SiteSpect acts as a reverse proxy for client websites and potentially transmits clients' customers' cardholder data
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	

Part 2c. Locations

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

Type of facility	Number of facilities of this type	Location(s) of facility (city, country)
Example: Retail outlets	*3*	*Boston, MA, USA*
data centers	10	Boston MA, San Jose CA, Dallas TX, Los Angeles CA, Chicago IL, Atlanta GA, Secaucus NJ, Amsterdam NL, London UK x 2
corporate offices	1	Auburndale MA

Part 2d. Payment Applications

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

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

Payment Application Name	Version Number	Application Vendor	Is application PA-DSS Listed?	PA-DSS Listing Expiry date (if applicable)
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ 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.*	This assesment covered SiteSpect's CDE environment, which includes web proxy engines, firewalls, and databases; as well as SiteSpect's corporate office environment
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 have a relationship with a Qualified Integrator Reseller (QIR) for the purpose of the services being validated?	☐ Yes ☒ No
If Yes:	
Name of QIR Company:	
QIR Individual Name:	
Description of services provided by QIR:	

Part 2f. Third-Party Service Providers (Continued)	
Does your company have a relationship with one or more 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.) for the purpose of the services being validated?	☒ Yes ☐ No

If Yes:

Name of service provider:	**Description of services provided:**
data center	physical location, physical security, and network connectivity
secured log aggregation	log visualization and alerting

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

Part 2g. Summary of Requirements Tested

For each PCI DSS Requirement, select one of the following:

- Full – The requirement and all sub-requirements were assessed for that Requirement, and no sub-requirements were marked as "Not Tested" or "Not Applicable" in the SAQ.
- Partial – One or more sub-requirements of that Requirement were marked as "Not Tested" or "Not Applicable" in the SAQ.
- None – All sub-requirements of that Requirement were marked as "Not Tested" and/or "Not Applicable" in the SAQ.

For all requirements identified as either "Partial" or "None," provide details in the "Justification for Approach" column, including:

- Details of specific sub-requirements that were marked as either "Not Tested" and/or "Not Applicable" in the SAQ
- Reason why sub-requirement(s) were not tested or not applicable

Note: *One table to be completed for each service covered by this AOC. Additional copies of this section are available on the PCI SSC website*.

Name of Service Assessed:	multi-variant testing

PCI DSS Requirement	**Details of Requirements Assessed**			
	Full	**Partial**	**None**	**Justification for Approach** (Required for all "Partial" and "None" responses. Identify which sub-requirements were not tested and the reason.)
Requirement 1:	☐	☒	☐	**1.2.2 - Operationally, SiteSpect connects its switch to the router that is under the management and control of the datacenter provider.** **1.3.6 - By design and contract, SiteSpect acts as a real-time transmission conduit between the individual user and the SiteSpect client's website. SiteSpect does not store Cardholder Data (CHD).**
Requirement 2:	☒	☐	☐	
Requirement 3:	☐	☒	☐	**3.1 - SiteSpect does not store CHD nor does it perform card transactions. Logging is specifically designed and configured to avoid tainting the logs with any CHD.** **3.2 - SiteSpect does not store CHD nor does it perform card transactions. Logging is specifically designed and configured to avoid tainting the logs with any CHD.** **3.2.1 - SiteSpect does not process the CHD, it only retransmits it and the full contents of Track 1 or Track 2 data would not be included in any customer's**

				transmission. **3.2.2 - SiteSpect does not process the CHD or the Card Verification Code, it only retransmits it. The information gathered as part of the SiteSpect service only includes abstracted behavioral and cookie information.** **3.2.3 - SiteSpect does not process the CHD, it only retransmits it and the PIN or PIN Block would not be sent as part of a customer's transmission.** **3.3 - SiteSpect does not store or display CHD. As long as the customer provides a masked PAN to SiteSpect, SiteSpect will not have the ability to display an unmasked PAN.** **3.4 - SiteSpect does not process the CHD or the credit card account number, it only retransmits it, hence the PAN is never stored by any SiteSpect system or service.** **3.6.6 - SiteSpect's cryptographic key usage and key management controls do not create a situation where split knowledge, dual control, split keying or split key escrow is required. In no situation are private keys transmitted in the clear.**
Requirement 4:	☒	☐	☐	
Requirement 5:	☒	☐	☐	
Requirement 6:	☐	☒	☐	**6.4.3 - SiteSpect does not store CHD nor perform any credit card transactions.**
Requirement 7:	☒	☐	☐	
Requirement 8:	☐	☒	☐	**8.5.1 - SiteSpect does not have access to devices on the customer premises. If SiteSpect did have such access, the customer would dictate the access controls and methods. Additionally, SiteSpect does not allow any service providers to have access to the CDE.** **8.7 - The Information Security Policy states**

				that SiteSpect does not store Cardholder Data and does not have any database containing Cardholder Data. The CDE acts solely as a transmission conduit between consumers and SiteSpect customers.
Requirement 9:	☐	☒	☐	**9.9 - SiteSpect is not a merchant and does not deploy Point-Of-Sale (POS) equipment.** **9.9.1 - SiteSpect is not a merchant and does not deploy Point-Of-Sale (POS) equipment.** **9.9.2 - SiteSpect is not a merchant and does not deploy Point-Of-Sale (POS) equipment.** **9.9.3 - SiteSpect is not a merchant and does not deploy Point-Of-Sale (POS) equipment.**
Requirement 10:	☐	☒	☐	**10.6.2 - Although this requirement is not specifically addressed in policy with a defined frequency, since logs for all systems are to be reviewed daily, this item can be considered not applicable.**
Requirement 11:	☒	☐	☐	
Requirement 12:	☐	☒	☐	**12.8.2 - SiteSpect does not store CHD, and thus does not share CHD with service providers.**
Appendix A1:	☐	☒	☐	**A1.1.1 - SiteSpect does not store cardholder data, and thus clients have no ability to access it using SiteSpect in an approved manner.** **A1.1.2 - SiteSpect's application runs as an unprivileged system account on each Engine System. Authorized client user access is controlled through the Control Panel application and:** **- Client users are allowed to view web transfer logs only for their environment** **- Client users do not have write access to shared system Admin System binaries (i.e., not part of the CDE)** **- Neither clients nor consumers have the ability to write any data directly to the CDE** **- Neither clients nor consumers have any**

				ability to view any log data within the CDE **- The application monitors resource usage to trigger actions when resources (such as CPU) are running low (i.e., such as when a given client is using generating too much traffic or otherwise consuming too many resources)**
Appendix A2:	☐	☒	☐	**A2.1 - SiteSpect is not a merchant and does not deploy Point-Of-Sale (POS) equipment.**

Section 2: Self-Assessment Questionnaire D – Service Providers

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:	3/25/20	
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 identified as being not tested?	☐ 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

This AOC is based on results noted in SAQ D (Section 2), dated *3/25/20.*

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

☒	**Compliant:** All sections of the PCI DSS SAQ are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby *SiteSpect* 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 *(Service Provide Company Name)* has not demonstrated full compliance with the PCI DSS. **Target Date** for Compliance: An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. *Check with 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 Questionnaire D, Version *3.2.1*, 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 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 3a. Acknowledgement of Status (continued)	
☒	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 *AlertLogic*

Part 3b. Service Provider Attestation

Signature of Service Provider Executive Officer ↑	*Date:* **3/25/20**
Service Provider Executive Officer Name: **Paul Silevitch**	*Title:* **VP of Engineering**

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

If a QSA was involved or assisted with this assessment, describe the role performed:	Assisted in completing self-assessment

Signature of Duly Authorized Officer of QSA Company ↑	*Date:* **3/25/20**
Duly Authorized Officer Name: **Joseph Kurfehs**	*QSA Company:* **System Experts**

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 the applicable payment brand(s) before completing Part 4.

PCI DSS Requirement	Description of Requirement	Compliant to PCI DSS Requirements (Select One)		Remediation Date and Actions (If "NO" selected for any Requirement)
		YES	NO	
1	Install and maintain a firewall configuration to protect cardholder data	☒	☐	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	☒	☐	
3	Protect stored cardholder data	☒	☐	
4	Encrypt transmission of cardholder data across open, public networks	☒	☐	
5	Protect all systems against malware and regularly update anti-virus software or programs	☒	☐	
6	Develop and maintain secure systems and applications	☒	☐	
7	Restrict access to cardholder data by business need to know	☒	☐	
8	Identify and authenticate access to system components	☒	☐	
9	Restrict physical access to cardholder data	☒	☐	
10	Track and monitor all access to network resources and cardholder data	☒	☐	
11	Regularly test security systems and processes	☒	☐	
12	Maintain a policy that addresses information security for all personnel	☒	☐	
Appendix A1	Additional PCI DSS Requirements for Shared Hosting Providers	☒	☐	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections.	☒	☐