Payment Card Industry (PCI)

Data Security Standard

Attestation of Compliance for Onsite Assessments – Service Providers

Version 3.2.1

June 2018

Section 1: Assessment Information

Instructions for Submission

This Attestation of Compliance must be completed as a declaration of the results of the service provider's 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:	Formstack, LLC.		DBA (doing business as):		
Contact Name:	Matt Gard		Title:	Vice President of Finance	
Telephone:	317.542.3125		E-mail:	compliance@ formstack.com	
Business Address:	11671 Lantern Road, Suite 300		City:	Indianapolis	
State/Province:	IN	Country:	USA	Zip:	46038
URL:	https://www.formstack.com				

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

Company Name:	Cadence Assurance, LLC				
Lead QSA Contact Name:	Jonathan Smith		Title:	QSA	
Telephone:	385-208-1313		E-mail:	jonathan@ thecadencegroup.com	
Business Address:	PO Box 711190		City:	Salt Lake City	
State/Province:	UT	Country:	USA	Zip:	84171
URL:	https://thecadencegroup.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:	Formstack Forms

Type of service(s) assessed:

Hosting Provider:

□ Applications / software
□ Hardware
□ Infrastructure / Network
□ Physical space (co-location)
□ Storage
□ Web
□ Security services
□ 3-D Secure Hosting Provider
□ Shared Hosting Provider
□ Other Hosting (specify):

Managed Services (specify):

□ Systems security services
□ IT support
□ Physical security
□ Terminal Management System
□ Other services (specify):

Payment Processing:

□ POS / card present
☒ Internet / e-commerce
□ MOTO / Call Center
□ ATM
□ Other processing (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): Form Filling/Completion

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:	N/A	
Type of service(s) not assessed:		
Hosting Provider: ☐ Applications / software ☐ Hardware ☐ Infrastructure / Network ☐ Physical space (co-location) ☐ Storage ☐ Web ☐ Security services ☐ 3-D Secure Hosting Provider ☐ Shared Hosting Provider ☐ Other Hosting (specify):	**Managed Services (specify):** ☐ Systems security services ☐ IT support ☐ Physical security ☐ Terminal Management System ☐ Other services (specify):	**Payment Processing:** ☐ POS / card present ☐ Internet / e-commerce ☐ MOTO / Call Center ☐ ATM ☐ Other processing (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:	N/A	

Part 2b. Description of Payment Card Business	
Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	Formstack is a data management system that helps non-technical users build online forms. The Formstack product makes the process to build forms and any resulting workflows easy for the end user. Users can use forms to collect information, such as job applications, payments, surveys, employee reviews, feedback forms, and so on. Users can then deploy these forms to collect and review relevant information from the completed forms. As part of this product, Formstack allowed customers to create forms that collected payment data from the customer's end users for purposes of routing to payment processors through either manual or automated means. The data flows for cardholder collection were as follows:

	1. Customer created form collecting cardholder data. 2. End user submits payment on Formstack form. The cardholder data was submitted to Formstack and was transmitted via HTTPS/TLS enforced by AWS Cloudfront load balancers to web servers with the Formstack AWS environment. 3. If customers elected to store cardholder data before authorization, they provided a password used to protect encryption keys that were used to encrypt the cardholder data at rest. In addition, AWS RDS encryption in conjunction with AWS KMS was utilized for databases storing cardholder data. 4. For customers not doing manual credit card processing, Formstack would forward the cardholder data onto the customers' processor for payment processing.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	Formstack also receives and transmits cardholder data for merchant transactions; this payment channel was included in Formstack's merchant Attestation of Compliance.

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*
Corporate Office	1	Fishers, Indiana, USA
AWS Cloud Environment	1	N. Virginia, USA (US-East Availability Zone)

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)
N/A	N/A	N/A	☐ Yes ☐ No	N/A

			□ 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.*	The cardholder data environment was hosted in AWS. Connections into and out of the CDE were through AWS load balancers, VPNs, and AWS security groups. Critical components in scope for this assessment consisted of: 1. AWS VPC/EC2 – platform the cloud network is built on 2. AWS security groups – used to control security groups 3. VPN – allows remote connection to servers within the CDE 4. Linux Servers – used to host system resources / services 5. Threatstack – IDS/IPS and threat management solution to report potentially malicious traffic 6. AWS RDS – database service 7. AWS KMS – Encryption and key management services 8. Endpoints – user endpoints used to manage and interact with the CDE 9. SumoLogic – logging/monitoring solution
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:		
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:**
Amazon Web Services (AWS)	AWS was the cloud hosting provider
Threatstack Sumo Logic	Threatstack provided threat intelligence to Formstack Sumo Logic provided log monitoring/review functionality
FoxPass	Foxpass provided authentication services
Pondurance	Pondurance was the Formstack penetration testing firm
Coalfire	Coalfire was the ASV
Bionic-Cat	Bionic-Cat managed endpoint controls for Formstack

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 of that requirement were assessed, and no sub-requirements were marked as "Not Tested" or "Not Applicable" in the ROC.
- **Partial** – One or more sub-requirements of that requirement were marked as "Not Tested" or "Not Applicable" in the ROC.
- **None** – All sub-requirements of that requirement were marked as "Not Tested" and/or "Not Applicable" in the ROC.

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 ROC
- 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:	Formstack Forms			
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; N/A as Formstack did not have access to routers that were part of the cardholder data environment. 1.2.3; N/A as there were no wireless networks that transmitted cardholder data or were otherwise directly connected to the cardholder data environment.
Requirement 2:	☐	☒	☐	2.1.1; N/A as there were no wireless networks that transmitted cardholder data or were otherwise directly connected to the cardholder data environment. 2.6; N/A as Formstack was not a shared hosting provider.
Requirement 3:	☐	☒	☐	3.4.1; N/A as full disk encryption was not used. 3.6; N/A as Formstack did not share keys with customers. 3.6.6; N/A as manual clear-text cryptographic key-management operations were not used.
Requirement 4:	☐	☒	☐	4.1.1; N/A as there were no wireless networks that transmitted cardholder data or were otherwise directly connected to the cardholder data environment.

Requirement 5:	☒	☐	☐	
Requirement 6:	☐	☒	☐	6.3.1; N/A as pre-production and/or custom application accounts, user IDs and/or passwords were not included as part of code that would be migrated into production.
Requirement 7:	☒	☐	☐	
Requirement 8:	☐	☒	☐	8.1.5; N/A as vendors did not have logical access to in-scope systems. 8.5.1; N/A as Formstack did not have remote access to customer premises.
Requirement 9:	☐	☒	☐	9.5, 9.5.1, 9.6, 9.6.1 - 9.6.3, 9.7, 9.7.1, 9.8.1; N/A as Formstack did not backup media containing cardholder data nor did it collect cardholder data on paper. 9.9, 9.9.1 -9.9.3; N/A as Formstack did collect data via physical point-of-sale devices, nor did Formstack manage physical point-of-sale devices.
Requirement 10:	☒	☐	☐	
Requirement 11:	☒	☐	☐	
Requirement 12:	☐	☒	☐	12.3.9; N/A as vendors did not have logical access to in-scope systems.
Appendix A1:	☐	☐	☒	
Appendix A2:	☐	☐	☒	

Section 2: Report on Compliance

This Attestation of Compliance reflects the results of an onsite assessment, which is documented in an accompanying Report on Compliance (ROC).

The assessment documented in this attestation and in the ROC was completed on:	April 10, 2020	
Have compensating controls been used to meet any requirement in the ROC?	☒ Yes	☐ No
Were any requirements in the ROC identified as being not applicable (N/A)?	☒ Yes	☐ No
Were any requirements not tested?	☐ Yes	☒ No
Were any requirements in the ROC 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 the ROC dated April 10, 2020*.*

Based on the results documented in the ROC 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 ROC are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby Formstack, LLC has demonstrated full compliance with the PCI DSS.
☐	**Non-Compliant:** Not all sections of the PCI DSS ROC are complete, or not all questions are answered affirmatively, resulting in an overall **NON-COMPLIANT** rating, thereby *(Service Provider 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 "Not in Place" 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)

☒	The ROC was completed according to the *PCI DSS Requirements and Security Assessment Procedures*, Version 3.2.1, and was completed according to the instructions therein.
☒	All information within the above-referenced ROC 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 Coalfire Systems, Inc

Part 3b. Service Provider Attestation

Matthew J. Gard

Signature of Service Provider Executive Officer ↑	*Date:* April 10, 2020
Service Provider Executive Officer Name: Matt Gard	*Title:* Vice President of Finance

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

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

Jonathan Smith

Signature of Duly Authorized Officer of QSA Company ↑	*Date:* April 10, 2020
Duly Authorized Officer Name: Jonathan Smith	*QSA Company:* Cadence Assurance, LLC

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:	N/A

[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	☒	☐	

AMERICAN EXPRESS DISCOVER JCB mastercard VISA