Payment Card Industry (PCI)
Data Security Standard

Attestation of Compliance for Onsite Assessments – Service Providers

Version 3.2.1 (released June 2018 by the PCI SSC)

Spreedly, Inc.

October 28, 2019

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:	Spreedly, Inc.		DBA (doing business as):		
Contact Name:	Ryan Daigle		Title:	CTO	
Telephone:	888.727.7750		E-mail:	ryan@spreedly.com	
Business Address:	733 Foster Street Suite 100		City:	Durham	
State/Province:	NC	Country:	USA	Zip:	27701
URL:	www.spreedly.com				

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

Company Name:	Sikich LLP				
Lead QSA Contact Name:	Ruth Barra		Title:	Senior Consultant	
Telephone:	877.403.5227		E-mail:	ruth.barra@sikich.com	
Business Address:	13400 Bishops Lane Suite 300		City:	Brookfield	
State/Province:	WI	Country:	USA	Zip:	53005
URL:	www.sikich.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:	Spreedly API hosted at https://core.spreedly.com/v1, including Spreedly Express and Spreedly's iframe service

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): Card vault – tokenization and primary account number (PAN) Account Updater (AU)		

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:	None	
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:		

Part 2b. Description of Payment Card Business

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	Spreedly captured CHD via HTTPS from their merchant customers, stored the CHD, and provided tokenization services. Spreedly captured CHD via their custom API and through payment pages (hosted iframe, direct post, or Spreedly Express form). Spreedly integrated directly with payment gateways and third-party receivers specified by their merchant customers in order to transmit CHD via HTTPS. For recurring transactions, merchants passed a Spreedly-provided token and payment transaction request to Spreedly's API, where the token was mapped to the vaulted CHD and passed from Spreedly directly to the merchant-specified payment gateway or third-party receiver. Spreedly also received batches of CHD for import via SFTP over SSH v2.0. Spreedly transmitted CHD bimonthly to Vantiv, Inc. (Vantiv) via SFTP over SSH v2.0 and obtained updated PAN data and expiration dates. The updated PAN was returned in a result file on the SFTP server over SSH v2.0 and fetched by the server-side AU component.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	Spreedly did not provide services, other than those described above, with the ability to impact the security of CHD for other entities.

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	2	Elk Grove Village, IL, USA US-EAST, USA

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)
Not applicable	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.*	This assessment covered the Spreedly API, which included application servers running a custom web application that accepted CHD via HTTPS to facilitate payment transactions and PAN tokenization. The Spreedly API relied on a web service and database server architecture to provide their payment gateway services, supported by a managed switch, firewalls, load balancers, web servers, storage servers, a log aggregation server, authentication and authorization services, and monitoring services.
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:**
ServerCentral, Inc.	Managed data center
Amazon Web Services (AWS)	Cloud services
Sumo Logic, Inc.	Log management and analytics
Worldpay, Inc. (DBA Vantiv, Inc.)	PAN, expiry data updates

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:	Spreedly API hosted at https://core.spreedly.com/v1, including Spreedly Express and Spreedly's iframe service

	Details of Requirements Assessed			
PCI DSS Requirement	**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:	☒	☐	☐	
Requirement 2:	☐	☒	☐	**Requirement 2.1.1 was not applicable. Spreedly did not have wireless networks that transmitted CHD or had connectivity with the cardholder data environment (CDE).** **Requirement 2.6 was not applicable. Spreedly was not a shared hosting provider.**
Requirement 3:	☐	☒	☐	**Requirement 3.4.1 was not applicable. Spreedly did not use disk encryption.** **Requirement 3.6 was not applicable. Spreedly did not share keys with their customers for the transmission or storage of CHD.**
Requirement 4:	☐	☒	☐	**Requirement 4.1.1 was not applicable. Spreedly did not have wireless networks that transmitted CHD or had connectivity with the CDE.**
Requirement 5:	☒	☐	☐	

Requirement 6:	☐	☒	☐	**Requirement 6.4.6 was not applicable. Spreedly had not performed a significant change within the previous 12 months.** **Requirement 6.5.10 was not applicable. The Spreedly API did not use session management. Calls through this application were stateless and required no session data.**
Requirement 7:	☒	☐	☐	
Requirement 8:	☐	☒	☐	**Requirement 8.1.5 was not applicable. Spreedly did not allow vendors to have remote access to in-scope systems.** **Requirement 8.5.1 was not applicable. Spreedly did not have remote access to customer premises.**
Requirement 9:	☐	☒	☐	**Requirement 9.5.1 was not applicable. Spreedly did not store CHD on physical backup media.** **Requirement 9.6 and its sub-requirements were not applicable. Spreedly did not distribute media containing CHD.** **Requirement 9.8.1 was not applicable. Spreedly did not write CHD to hardcopy media or otherwise maintain hardcopy materials containing CHD.** **Requirement 9.9 and its sub-requirements were not applicable. Spreedly did not maintain devices that captured CHD via direct physical interaction with the card.**
Requirement 10:	☐	☒	☐	**Requirement 10.6.2 was not applicable. Spreedly did not have other system components identified as being outside the scope of requirement 10.6.1 and, therefore, reviewed audit trails for in-scope components on a daily basis.**
Requirement 11:	☐	☒	☐	**Requirement 11.2.3 was not applicable. Spreedly had not made any significant changes to their PCI environment in the past 12 months.** **Requirement 11.3.4 and its sub-requirement were not applicable. Spreedly employed segmentation methods that limited connectivity to publicly-accessible services. For more information, see the 3.3. Network Segmentation section within the Description of Scope of Work and Approach Taken portion of the Report on Compliance.**
Requirement 12:	☐	☒	☐	**Requirement 12.3.9 was not applicable. Spreedly did not allow vendors to have remote access to in-scope systems.**
Appendix A1:	☐	☐	☒	**Spreedly was not a shared hosting provider.**

Appendix A2:	☐	☐	☒	**Spreedly did not maintain devices that captured CHD via direct physical interaction with the card within the scope of this assessment.**

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:	*October 28, 2019*	
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 *October 28, 2019*.

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 *Spreedly, Inc.* 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.

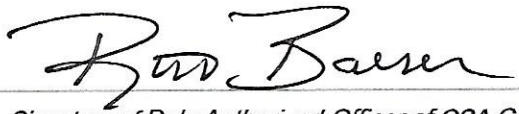
Part 3a. Acknowledgement of Status (continued)	
☒	No evidence of full track data[1], CAV2, CVC2, CID, or CVV2 data[2], or PIN data[3] storage after transaction authorization was found on ANY system reviewed during this assessment.
☒	ASV scans are being completed by the PCI SSC Approved Scanning Vendor *Sikich LLP*

Part 3b. Service Provider Attestation

Signature of Service Provider Executive Officer ↑	*Date:* **October 28, 2019**
Service Provider Executive Officer Name: **Ryan Daigle**	*Title:* **CTO**

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

If a QSA was involved or assisted with this assessment, describe the role performed:	*Sikich LLP provided PCI DSS assessment and consulting services.*



Signature of Duly Authorized Officer of QSA Company ↑	*Date:* ***October 28, 2019***
Duly Authorized Officer Name: **Ruth Barra**	*QSA Company:* **Sikich LLP**

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	☐	☐