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:	MobileCause, Inc.		DBA (doing business as):	MobileCause	
Contact Name:	Gerard Mackey		Title:	Chief Technology Officer	
Telephone:	+1 310.387.8581		E-mail:	ged@mobilecause.com	
Business Address:	27001 Agoura Road, Suite 350A		City:	Calabasas	
State/Province:	CA	Country:	USA	Zip:	91301
URL:	https://www.mobilecause.com				

Part 1b. Qualified Security Assessor Company Information (if applicable)					
Company Name:	Tevora Business Solutions, Inc. (DBA Tevora)				
Lead QSA Contact Name:	Cody Firuta		Title:	Information Security Consultant	
Telephone:	+1 949-250-3290		E-mail:	qsa@tevora.com	
Business Address:	17875 Von Karman Ave #100		City:	Irvine	
State/Province:	CA	Country:	USA	Zip:	92614
URL:	https://www.tevora.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:	MobileCause Cloud Based Fundraising	
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):		

***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:	Not Applicable	
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:	Not Applicable	

Part 2b. Description of Payment Card Business	
Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	Donors access the MobileCause mobile phone application or client website, hosted on the MobileCause application "app.mobilecause.com", to determine what cause to donate to. When donors have chosen, they are taken to one of the following payment gateways by an iFrame redirect: • CyberSource • BrainTree • CardConnect Donors input cardholder data (CHD) on a web donation form that is hosted on one of the payment gateways and contains an embedded iFrame API. Once submitted, the donation is automatically processed by the payment gateways; payment gateways then return a token that MobileCause stores. MobileCause does not store CHD on their systems. Only tokenized data is received from the payment gateways.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	MobileCause does not directly store, process, or transmit CHD as this is done through the payment gateways. MobileCause only stores a token representing CHD from the payment gateway after the payment gateway processes donations. CHD is not transmitted over open public networks as a complete redirect to the payment gateway occurs prior to CHD being entered.

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):
Corporate Headquarters	1	Calabasas, CA, USA
Colocation Facility (Flexential)	1	Denver, CO, USA
Colocation Secondary Facility (Flexential)	1	OR, 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	Not Applicable	Not Applicable	☐ Yes ☐ No	Not Applicable

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 into and out of the production environment are made through HTTPS over TLS and pass through a web application firewall to Cisco ASA firewalls hosted in the data center by Flexential, where the load balancers determine where to route the connection internally. Critical system components in the CDE include Linux virtual servers, Cisco firewalls, Brocade load balancers, and Kona SQL databases hosted by Flexential. MobileCause uses cloud-hosted applications such as Cloudflare web application firewall, Alert Logic for Intrusion Detection System/ Intrusion Prevention System(IDS/IPS) and Security information and event management (SIEM) solution, and TrendMicro for anti-virus.
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:	Not Applicable
QIR Individual Name:	Not Applicable
Description of services provided by QIR:	Not Applicable
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:**
Flexential Inc.	Data Center, Hosting Provider for Server and Network Devices. Also manages and maintains all devices from the Operating System (OS) down to the hardware level.
Alert Logic	Intrusion Detection, Log Management, Web Application Security, Managed Service Monitoring
CardConnect Corp.	Payment Gateway and Tokenization
BrainTree	Payment Gateway and Tokenization
CyberSource	Payment Gateway and Tokenization
Flexential Inc.	Data Center, Hosting Provider for Server and Network Devices. Also manages and maintains all devices from the Operating System (OS) down to the hardware level.

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:	MobileCause Cloud Based Fundraising

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:	☐	☒	☐	Requirement 1.3.6 – No system components store process or transmit cardholder data.
Requirement 2:	☐	☒	☐	Requirement 2.1.1 – MobileCause does not have wireless networks in the CDE. Requirement 2.2.3 – There are no insecure protocols in use. Requirement 2.6 – MobileCause is not a shared hosting provider.
Requirement 3:	☐	☒	☐	Requirement 3.1 – 3.2d, 3.3 – 3.7 – MobileCause does not store any CHD. MobileCause only has access to tokenized data returned from the payment processors. Therefore encryption, truncation, encryption keys, and management of the following above is not applicable. Requirement 3.2 – MobileCause is not an issuer and does not support issuing services. MobileCause also does not receive sensitive authentication data. Requirement 3.3 - 3.7: Not Applicable. MobileCause does not store CHD. Only transaction tokens are stored.
Requirement 4:	☐	☐	☒	Requirement 4 – MobileCause does not transmit CHD over open, public networks. MobileCause performs a complete redirect to payment gateways prior to CHD being entered.

Requirement 5:	☒	☐	☐	
Requirement 6:	☐	☒	☐	Requirement 6.4.3 – MobileCause does not develop applications that interact with CHD. Requirement 6.4.6 – MobileCause has not had any significant changes within the last 12 months.
Requirement 7:	☐	☒	☐	Requirement 7.1.4 – No new hires joined within the last 12 months. Requirement 7.3: Not Applicable. MobileCause does not store CHD.
Requirement 8:	☐	☒	☐	Requirement 8.1.3 – No terminations within the last 12 months. Requirement 8.5.1: MobileCause has no access to customer systems. Requirement 8.7 – MobileCause does not store any CHD.
Requirement 9:	☐	☒	☐	Requirement 9.5 – 9.8.2 – MobileCause does not store, process, or transmit CHD using physical media. Requirement 9.9 – 9.10 – MobileCause does not store or backup any CHD onto physical media.
Requirement 10:	☐	☒	☐	Requirement 10.2 – No CHD in the MobileCause production environment. Requirement 10.8.1.b – No critical control failures occurred within the last year.
Requirement 11:	☐	☒	☐	Requirement 11.1.a – Requirement 11.1.c – No wireless is issued in the production environment and is forbidden by Flexential. Requirement 11.1.1 – 11.1.2 – No wireless is issued in the production environment and is forbidden by Flexential. Requirement 11.2.1.b, 11.2.2.b, 11.2.3.b – No rescan was necessary. Requirement 11.3.3 – No high or critical vulnerabilities were found for the most recent biannual penetration test report.
Requirement 12:	☒	☐	☐	
Appendix A1:	☐	☐	☒	MobileCause is not a shared hosting provider.
Appendix A2:	☐	☐	☒	MobileCause does not use early TLS/SSL.

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:	*TBD*	
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 TBD.

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 *MobileCause, 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: *N/A* 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 "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
N/A	N/A

Part 3a. Acknowledgement of Status

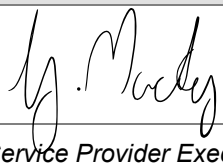
Signatory(s) confirms:

(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 *Trustwave Holdings, Inc.*

Part 3b. Service Provider Attestation



Signature of Service Provider Executive Officer ↗	*Date:* Aug 6th 2020
Service Provider Executive Officer Name: Gerard Mackey	*Title:* Chief Technology Officer

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

If a QSA was involved or assisted with this assessment, describe the role performed:	*Tevora performed the PCI DSS assessment, including conducting interviews, collecting samples, review documentation, report writing and QA activities.*

Signature of Duly Authorized Officer of QSA Company ↗	*Date:* Aug 6th 2020
Duly Authorized Officer Name: Cody Firuta	*QSA Company:* Tevora

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:	Not Applicable. No ISAs were involved or assisted with this assessment.

[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	☒	☐