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:	MINDBODY Inc.		DBA (doing business as):	N/A	
Contact Name:	Jason Loomis		Title:	Chief Information Security Officer, VP Cybersecurity	
Telephone:	+1.877.755.4279		E-mail:	CustSecQ@mindbodyonline.com	
Business Address:	651 Tank Farm Road		City:	San Luis Obispo	
State/Province:	CA	Country:	USA	Zip:	93401
URL:	https://mindbodyonline.com				

Part 1b. Qualified Security Assessor Company Information (if applicable)					
Company Name:	Urbane Security, LLC.				
Lead QSA Contact Name:	Magen Wu		Title:	Senior Associate	
Telephone:	+1.312.313.3700		E-mail:	PCI@UrbaneSecurity.com	
Business Address:	311 South Wacker Drive Suite 6030		City:	Chicago	
State/Province:	Illinois	Country:	USA	Zip:	60606
URL:	https://UrbaneSecurity.com				

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

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:	MINDBODY, Booker, FitMetrix, and Bowtie	
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.*

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

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.	MINDBODY, Booker, Bowtie, and FitMetrix receive cardholder data via website, mobile, or physical point of sale devices, transmits it through the applicable brand APIs to their processors and partners, and store when necessary for business needs in either the relevant MINDBODY or Booker databases with field-level encryption.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	The assessed brands and services have the ability to impact the security of cardholder data being transmitted through their API, transmitted to processors, and during the encryption and decryption processes occurring while storing and accessing cardholder data in databases.

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

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*
Amazon Web Services	2	USA
Google Cloud	2	USA
Microsoft Azure	1	USA
Rackspace Hosting	1	Chicago, IL, USA
Switch Datacenter	1	Las Vegas, NV, USA
Zayao Datacenter	1	Irvine, CA, 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)
MINDBODY	Rolling	MINDBODY	☐ Yes ☒ No	N/A
Booker	Rolling	MINDBODY	☐ Yes ☒ No	N/A
Bowtie Payments	Rolling	MINDBODY	☐ Yes ☒ No	N/A
FitMetrix Payments	Rolling	MINDBODY	☐ Yes ☒ No	N/A

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.*

Urbane reviewed the following scope of the MINDBODY cardholder data environments as a service provider:

- Mobile and E-commerce processes for MINDBODY, Booker, Bowtie, and FitMetrix.
- Card-present processes and hardware for MINDBODY and Booker merchants.
- Cardholder data environments supporting these processes within Rackspace, Azure, Google Cloud, Amazon Web Services, and dedicated hosting facilities.
- Encryption, storage, and tokenization of cardholder data within the MINDBODY and Booker cardholder data environments.
- The management and technical operation, configuration, and maintenance of systems, services, and network devices that can impact the security of systems within the cardholder data environments of the assessed brands and services.
- Security controls, including segmentation, logical access, vulnerability management, and connectivity to the cardholder data environments for each assessed brand and service.

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

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:**
3C Payment USA Corp	Payment Processing
Akamai	Cloud CDN and WAF
Amazon Web Services	Cloud Platform as a Service
Microsoft Azure	Cloud Platform as a Service
Bluefin	Payment Gateway
Cloudflare	Cloud WAF
Elavon	Payment Processing
Ezidebit	Payment Gateway
First Data	Payment Processing
Google Cloud	Cloud platform as a service
Imperva	Cloud WAF
PaySafe	Payment Processing
Poynt	Cloud smart terminal payment services
Rackspace	Platform as a Service and System Management
Stripe	Payment Processing
Switch	Co-location
TSYS	Payment Processing
Vantiv	Payment Processing
Zayo	Co-location

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

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

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:	MINDBODY and Booker

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 2:	☐	☒	☐	**2.1.1 – Not Applicable:** There were no wireless environments connected to assessed cardholder data environments nor that transmits cardholder data. **2.2.3 – Not Applicable:** The assessed cardholder data environments were observed to not be running any insecure services, daemons, or protocols at the time of assessment. **2.6 – Not Applicable:** The assessed brands and services were not shared hosting providers.
Requirement 3:	☐	☒	☐	**3.6.6 – Not Applicable:** The assessed services' storage of cardholder data did not rely on clear-text key-management.
Requirement 4:	☐	☒	☐	**4.1 - Not Applicable:** There were no wireless environments connected to the assessed cardholder data environments nor that transmits cardholder data.
Requirement 5:	☒	☐	☐	
Requirement 6:	☒	☐	☐	
Requirement 7:	☒	☐	☐	
Requirement 8:	☐	☒	☐	**8.5.1 – Not Applicable:** None of the assessed brands or services had remote access into customer environments.

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

Requirement 9:	☐	☒	☐	**9.6.2 – Not Applicable:** Media containing cardholder data was not physically transported unless destroyed in alignment with data destruction processes. **9.8.1 – Not Applicable:** Cardholder data did not exist on hard-copy materials for the assessed services. **9.9, 9.9.1, 9.9.2, 9.9.3 – Not Applicable – Customer Control:** The responsibility for physical security of card-present points of interaction was the responsibility of the merchants leveraging the equipment.
Requirement 10:	☒	☐	☐	
Requirement 11:	☒	☐	☐	
Requirement 12:	☒	☐	☐	
Appendix A1:	☐	☐	☒	**Not Applicable –** The assessed services were not a shared hosting provider.
Appendix A2:	☐	☐	☒	**Not Applicable –** The assessed services did not utilize weakened transport encryption protocols or algorithms.

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

Name of Service Assessed:	Bowtie and FitMetrix

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:	☐	☒	☐	**1.3.6 – Not Applicable:** The assessed services did not store cardholder data.
Requirement 2:	☐	☒	☐	**2.1.1 – Not Applicable:** There were no wireless environments connected to assessed cardholder data environments nor that transmits cardholder data. **2.2.3 – Not Applicable:** The assessed cardholder data environments were observed to not be running any insecure services, daemons, or protocols at the time of assessment. **2.6 – Not Applicable:** The assessed brands and services were not shared hosting providers.
Requirement 3:	☐	☒	☐	**3.4, 3.4.1, 3.5, 3.5.1, 3.5.1, 3.5.3, 3.5.4, 3.6, 3.6.1, 3.6.2, 3.6.3, 3.6.3, 3.6.5, 3.6.6, 3.6.7, 3.6.8 – Not Applicable:** The assessed services did not store cardholder data.
Requirement 4:	☐	☒	☐	**4.1 - Not Applicable:** There were no wireless environments connected to the assessed cardholder data environments nor that transmits cardholder data.
Requirement 5:	☒	☐	☐	
Requirement 6:	☒	☐	☐	
Requirement 7:	☒	☐	☐	
Requirement 8:	☐	☒	☐	**8.5.1 – Not Applicable:** None of the assessed brands or services had remote access into customer environments. **8.7 – Not Applicable:** The assessed services did not store cardholder data.
Requirement 9:	☐	☒	☐	**9.5, 9.5.1, 9.6.2, 9.7, 9.8, 9.8.1, 9.8.2 – Not Applicable:** The assessed services did not store cardholder data. **9.9, 9.9.1, 9.9.2, 9.9.3 – Not Applicable – Customer Control:** The responsibility for physical security of card-present points of interaction was the responsibility of the merchants leveraging the equipment.
Requirement 10:	☒	☐	☐	
Requirement 11:	☒	☐	☐	
Requirement 12:	☒	☐	☐	

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

Appendix A1:	☐	☐	☒	**Not Applicable –** The assessed services were not a shared hosting provider.
Appendix A2:	☐	☐	☒	**Not Applicable –** The assessed services did not utilize weakened transport encryption protocols or algorithms.

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

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:	*September 30, 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

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in the ROC dated *September 30, 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 *MINDBODY* 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 *MINDBODY* 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.

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

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 *Qualys.*

Part 3b. Service Provider Attestation

Jason Loomis

Signature of Service Provider Executive Officer ↗	*Date:* Sep 30, 2019
Service Provider Executive Officer Name: Jason Loomis	*Title:* Chief Information Security Officer

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

If a QSA was involved or assisted with this assessment, describe the role performed:	*Urbane independently and fully assessed the entirety of the above listed scope of this assessment for compliance to the PCI DSS Version 3.2.1.*

Zack Fasel (Sep 30, 2019)

Signature of Duly Authorized Officer of QSA Company ↗	*Date:* Sep 30, 2019
Duly Authorized Officer Name: Zack Fasel	*QSA Company:* Urbane Security, 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:	None

[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.

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

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	☒	☐	

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

MINDBODY 2019 PCI DSS Service Provider Attestation of Compliance

Final Audit Report 2019-09-30

Created:	2019-09-30
By:	Zack Fasel (zfasel@urbanesecurity.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAAUf-S2WWauwEcWwJxA_CkejB_kGTb6AEC

"MINDBODY 2019 PCI DSS Service Provider Attestation of Compliance" History

Document created by Zack Fasel (zfasel@urbanesecurity.com)
2019-09-30 - 7:14:29 PM GMT- IP address: 198.54.108.221

Document emailed to Jason Loomis (jason.loomis@mindbodyonline.com) for signature
2019-09-30 - 7:17:32 PM GMT

Email viewed by Jason Loomis (jason.loomis@mindbodyonline.com)
2019-09-30 - 7:32:31 PM GMT- IP address: 76.217.7.200

Jason Loomis (jason.loomis@mindbodyonline.com) has agreed to the terms of use and to do business electronically with Urbane Security
2019-09-30 - 7:33:00 PM GMT- IP address: 76.217.7.200

Document e-signed by Jason Loomis (jason.loomis@mindbodyonline.com)
Signature Date: 2019-09-30 - 7:33:00 PM GMT - Time Source: server- IP address: 76.217.7.200

Document emailed to Zack Fasel (zfasel@urbanesecurity.com) for signature
2019-09-30 - 7:33:02 PM GMT

Email viewed by Zack Fasel (zfasel@urbanesecurity.com)
2019-09-30 - 8:08:05 PM GMT- IP address: 198.54.108.221

Zack Fasel (zfasel@urbanesecurity.com) has agreed to the terms of use and to do business electronically with Urbane Security
2019-09-30 - 8:08:12 PM GMT- IP address: 198.54.108.221

Document e-signed by Zack Fasel (zfasel@urbanesecurity.com)
Signature Date: 2019-09-30 - 8:08:12 PM GMT - Time Source: server- IP address: 198.54.108.221

Signed document emailed to Magen Wu (mwu@urbanesecurity.com), Zack Fasel (zfasel@urbanesecurity.com), nicolas.edmonds@mindbodyonline.com, and Jason Loomis (jason.loomis@mindbodyonline.com)

2019-09-30 - 8:08:12 PM GMT