



# 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):	Booker Software, Inc.		
Contact Name:	Jason Loomis	Title:	Chief Information Security Officer		
Telephone:	+1.877.755.4279	E-mail:	custsecq@mindbodyonline.com		
Business Address:	651 Farm Tank Road	City:	San Luis Obispo		
State/Province:	California	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:	Sr. Associate		
Telephone:	+1.312.313.3700	E-mail:	mwu@urbanesecurity.com		
Business Address:	171 N Aberdeen Street Suite 400	City:	Chicago		
State/Province:	Illinois	Country:	USA	Zip:	60607
URL:	https://UrbaneSecurity.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:	MINDBODY Booker FitMetrix Messenger[ai]
------------------------------	--

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):

- |  |   |  |
|--|---|--|
| <input type="checkbox"/> Account Management      | <input type="checkbox"/> Fraud and Chargeback | <input type="checkbox"/> Payment Gateway/Switch  |
| <input type="checkbox"/> Back-Office Services    | <input type="checkbox"/> Issuer Processing    | <input type="checkbox"/> Prepaid Services        |
| <input type="checkbox"/> Billing Management      | <input type="checkbox"/> Loyalty Programs     | <input type="checkbox"/> Records Management      |
| <input type="checkbox"/> Clearing and Settlement | <input type="checkbox"/> Merchant Services    | <input type="checkbox"/> Tax/Government Payments |
| <input type="checkbox"/> Network Provider        |   |  |
| <input type="checkbox"/> 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: None

Type of service(s) not assessed:

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

<p>Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.</p>	<p><b>All Assessed Brands and Services:</b> The assessed services receive cardholder data from consumers and customers via web applications, mobile applications, and physical point of interaction devices.</p> <p><b>MINDBODY</b> receives cardholder data through their Payments and Next Generation Payment (NGP) platforms for processing and transmission to their payment gateways. Upon successful processing, cardholder data is stored using field-level encryption for future transactions.</p> <p><b>Booker</b> receives card-not-present and card-present cardholder data through their web services and transmits it to Booker Payments v1 or v2 for further transmission to their designated processors. Upon confirmation of authorization, cardholder data is stored using field-level encryption for future transactions.</p> <p><b>FitMetrix and Messenger[ai]</b> receive cardholder data through their web services and directly forward the cardholder data to MINDBODY and Booker for processing and storage.</p>
<p>Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.</p>	<p><b>All Assessed Brands and Services</b> directly process cardholder data for transactions that occur on their platforms.</p>

### 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):
<i>Example: Retail outlets</i>	3	Boston, MA, USA
Amazon Web Services (AWS)	2	USA
Microsoft Azure	2	USA
Heroku	1	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	Internal	MINDBODY	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	Not Applicable
Booker	Internal	MINDBODY	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	Not Applicable
FitMetrix	Internal	MINDBODY	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	Not Applicable
Messenger[ai]	Internal	MINDBODY	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> 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.*

Urbane reviewed the following scope of MINDBODY’s brands and services’ cardholder data environments as a service provider:

- The receipt and processing of cardholder data from users across all mobile and web platforms for the assessed services, including the development and deployment of applications and services, mechanisms used to encrypt cardholder data, the handling of cardholder data by the payment applications, transmission of cardholder data to payment partners for processing, and the tokenization and detokenization flows of cardholder data.
- Card-present processes and supported hardware for MINDBODY and Booker merchants.
- Cardholder data environments supporting the above processes within AWS, Azure, and Heroku.
- The network topology of all cardholder data environments, segmentation controls, access controls, and connectivity to and from the cardholder data environments.
- The management, technical operation, configuration, and maintenance of components that could impact the security of the resources within the cardholder data environments.
- All other processes, services, and environments serving as external dependencies which could directly or indirectly impact the confidentiality of cardholder data of the assessed 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: 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 Corp USA	Payment Processing
Amazon Web Services	Platform as a Service
Bluefin	Payment Gateway
Cloudflare	Cloud Web Application Firewall
Elavon	Payment Processing
EZidebit	Payment Processing
First Data	Payment Processing
Microsoft Azure	Platform as a Service
PaySafe	Payment Processing
Poynt	Terminal Payment Services
Stripe	Payment Processing
TSYS	Payment Processing
Vantiv Payments	Payment Processing

**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:		MINDBODY, Booker		
PCI DSS Requirement	Details of Requirements Assessed			Justification for Approach (Required for all “Partial” and “None” responses. Identify which sub-requirements were not tested and the reason.)
	Full	Partial	None	
Requirement 1:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 2:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p><b>2.1.1</b> – Urbane reviewed network diagrams and network resource configurations and observed all traffic was denied between wireless environments and the cardholder data environments.</p> <p><b>2.2.3</b> - The assessed cardholder data environments were observed to not be utilizing any insecure services, daemons, or protocols.</p> <p><b>2.6</b> - None of the assessed brands or services were shared hosting providers.</p>
Requirement 3:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p><b>3.4.1</b> - Urbane reviewed system configurations and agreements with third party service providers and observed MINDBODY and Booker did not rely on disk encryption for the protection of cardholder data.</p> <p><b>3.6</b> - None of the assessed brands and services shared keys with customers.</p>
Requirement 4:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p><b>4.1.1</b> - The assessed services did not contain wireless environments connected to cardholder data environments nor otherwise transmitted cardholder data wirelessly.</p>
Requirement 5:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	



Requirement 6:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 7:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 8:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<b>8.5.1</b> - Urbane observed none of the assessed brands and services had access to customer environments
Requirement 9:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p><b>9.6.2</b> - Urbane gathered through review of processes, documented policies, and interviews that cardholder data was never stored on distributed media.</p> <p><b>9.8.1 – Not Applicable:</b> The assessed services did not utilize hard-copy materials with cardholder data. The responsibility for the use of any point of interaction device was observed to be the responsibility of the customer</p> <p><b>9.9, 9.9.1, 9.9.2, 9.9.3 - Customer Control</b> - The responsibility for the use of any point of interaction device was observed to be the responsibility of the customer.</p>
Requirement 10:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 11:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<b>11.3.3</b> - Urbane reviewed documented penetration test results and observed exploitable vulnerabilities were not discovered during testing.
Requirement 12:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Appendix A1:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<b>Not Applicable</b> – The assessed services did not provide shared hosting.
Appendix A2:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<b>Not Applicable</b> – The assessed services did not utilize weakened transport encryption protocols or algorithms.

Name of Service Assessed:		FitMetrix, Messenger[ai]		
PCI DSS Requirement	Details of Requirements Assessed			
	Full	Partial	None	Justification for Approach <small>(Required for all "Partial" and "None" responses. Identify which sub-requirements were not tested and the reason.)</small>
Requirement 1:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<b>1.3.6</b> – The assessed services did not store cardholder data.
Requirement 2:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<b>2.1.1</b> – Urbane reviewed network diagrams and network resource configurations and observed all traffic was denied between wireless environments and the cardholder data environments.  <b>2.2.3</b> - The assessed cardholder data environments were observed to not be utilizing any insecure services, daemons, or protocols.  <b>2.6</b> - None of the assessed brands or services were shared hosting providers.
Requirement 3:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<b>3.4.1, 3.5, 3.5.1, 3.5.2, 3.5.3, 3.5.4, 3.6, 3.6.1, 3.6.2, 3.6.3, 3.6.4, 3.6.5, 3.6.6, 3.6.7, 3.6.8</b> - Urbane reviewed cardholder data flows and gathered through interviews that FitMetrix and Messenger[ai] did not store cardholder data within their environments.  <b>3.6</b> - None of the assessed brands and services shared keys with customers.
Requirement 4:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<b>4.1.1</b> - The assessed services did not contain wireless environments connected to cardholder data environments nor otherwise transmitted cardholder data wirelessly.
Requirement 5:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 6:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 7:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 8:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<b>8.5.1</b> - Urbane observed none of the assessed brands and services had access to customer environments.  <b>8.7</b> - Urbane reviewed cardholder data flows and gathered through interviews that FitMetrix and Messenger[ai] did not store cardholder data within their environments.
Requirement 9:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<b>9.5, 9.5.1, 9.6.1, 9.6.2, 9.6.3, 9.7, 9.7.1, 9.8, 9.8.1, 9.8.2</b> - Urbane reviewed cardholder data flows and gathered through interviews that FitMetrix and Messenger[ai] did not store cardholder data within their environments.

				<b>9.9, 9.9.1, 9.9.2, 9.9.3 - Customer Control</b> - The responsibility for the use of any point of interaction device was observed to be the responsibility of the customer.
Requirement 10:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 11:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<b>11.3.3</b> - Urbane reviewed documented penetration test results and observed exploitable vulnerabilities were not discovered during testing.
Requirement 12:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Appendix A1:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<b>Not Applicable</b> – The assessed services did not provide shared hosting.
Appendix A2:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<b>Not Applicable</b> – The assessed services did not utilize weakened transport encryption protocols or algorithms.

## 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:	<i>October 8, 2021</i>	
Have compensating controls been used to meet any requirement in the ROC?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Were any requirements in the ROC identified as being not applicable (N/A)?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
Were any requirements not tested?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Were any requirements in the ROC unable to be met due to a legal constraint?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No

## Section 3: Validation and Attestation Details

### Part 3. PCI DSS Validation

This AOC is based on results noted in the ROC dated **October 8, 2021**.

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**):

<input checked="" type="checkbox"/>	<p><b>Compliant:</b> All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall <b>COMPLIANT</b> rating; thereby <i>MINDBODY</i> has demonstrated full compliance with the PCI DSS.</p>						
<input type="checkbox"/>	<p><b>Non-Compliant:</b> Not all sections of the PCI DSS ROC are complete, or not all questions are answered affirmatively, resulting in an overall <b>NON-COMPLIANT</b> rating, thereby <i>MINDBODY</i> has not demonstrated full compliance with the PCI DSS.</p> <p><b>Target Date</b> for Compliance:</p> <p>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. <i>Check with the payment brand(s) before completing Part 4.</i></p>						
<input type="checkbox"/>	<p><b>Compliant but with Legal exception:</b> 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.</p> <p><i>If checked, complete the following:</i></p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 35%;">Affected Requirement</th> <th>Details of how legal constraint prevents requirement being met</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> </tbody> </table>	Affected Requirement	Details of how legal constraint prevents requirement being met				
Affected Requirement	Details of how legal constraint prevents requirement being met						

### Part 3a. Acknowledgement of Status

Signatory(s) confirms:

(Check all that apply)

<input checked="" type="checkbox"/>	The ROC was completed according to the <i>PCI DSS Requirements and Security Assessment Procedures, Version 3.2.1</i> , and was completed according to the instructions therein.
<input checked="" type="checkbox"/>	All information within the above-referenced ROC and in this attestation fairly represents the results of my assessment in all material respects.
<input type="checkbox"/>	I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
<input checked="" type="checkbox"/>	I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
<input checked="" type="checkbox"/>	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)**

<input checked="" type="checkbox"/>	No evidence of full track data <sup>1</sup> , CAV2, CVC2, CID, or CVV2 data <sup>2</sup> , or PIN data <sup>3</sup> storage after transaction authorization was found on ANY system reviewed during this assessment.
<input checked="" type="checkbox"/>	ASV scans are being completed by the PCI SSC Approved Scanning Vendor <i>Tenable.io</i>

**Part 3b. Service Provider Attestation**

*Jason Loomis*

Signature of Service Provider Executive Officer ↑	Date: Oct 8, 2021
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:	<i>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.</i>
--	---

  
 Zack Fasel (Oct 8, 2021 18:24 CDT)

Signature of Duly Authorized Officer of QSA Company ↑	Date: Oct 8, 2021
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:	Not Applicable
---	----------------

<sup>1</sup> 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.

<sup>2</sup> 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.

<sup>3</sup> 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	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3	Protect stored cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
4	Encrypt transmission of cardholder data across open, public networks	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
5	Protect all systems against malware and regularly update anti-virus software or programs	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6	Develop and maintain secure systems and applications	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
7	Restrict access to cardholder data by business need to know	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8	Identify and authenticate access to system components	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9	Restrict physical access to cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10	Track and monitor all access to network resources and cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
11	Regularly test security systems and processes	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12	Maintain a policy that addresses information security for all personnel	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Appendix A1	Additional PCI DSS Requirements for Shared Hosting Providers	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	<input checked="" type="checkbox"/>	<input type="checkbox"/>	












# MINDBODY 2021 PCI DSS Assessment Attestation of Compliance Service Provider

Final Audit Report

2021-10-08

Created:	2021-10-08
By:	Zack Fasel (zfasel@urbanesecurity.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAA6kroNf4nh5_ZXXgNUQPAa0UOmF5-9P2B

## "MINDBODY 2021 PCI DSS Assessment Attestation of Compliance Service Provider" History

-  Document created by Zack Fasel (zfasel@urbanesecurity.com)  
2021-10-08 - 10:44:38 PM GMT- IP address: 174.197.84.201
-  Document emailed to Jason Loomis (jason.loomis@mindbodyonline.com) for signature  
2021-10-08 - 10:47:28 PM GMT
-  Email viewed by Jason Loomis (jason.loomis@mindbodyonline.com)  
2021-10-08 - 11:22:29 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  
2021-10-08 - 11:23:57 PM GMT- IP address: 76.217.7.200
-  Document e-signed by Jason Loomis (jason.loomis@mindbodyonline.com)  
Signature Date: 2021-10-08 - 11:23:57 PM GMT - Time Source: server- IP address: 76.217.7.200
-  Document emailed to Zack Fasel (zfasel@urbanesecurity.com) for signature  
2021-10-08 - 11:23:59 PM GMT
-  Email viewed by Zack Fasel (zfasel@urbanesecurity.com)  
2021-10-08 - 11:24:26 PM GMT- IP address: 107.77.198.7
-  Zack Fasel (zfasel@urbanesecurity.com) has agreed to the terms of use and to do business electronically with Urbane Security  
2021-10-08 - 11:24:40 PM GMT- IP address: 107.77.198.7
-  Document e-signed by Zack Fasel (zfasel@urbanesecurity.com)  
Signature Date: 2021-10-08 - 11:24:40 PM GMT - Time Source: server- IP address: 107.77.198.7



✔ Agreement completed.

2021-10-08 - 11:24:40 PM GMT