Payment Card Industry (PCI)
Data Security Standard
Self-Assessment Questionnaire A

Card-not-present Merchants,
All Cardholder Data Functions Fully Outsourced

For use with PCI DSS Version 3.2.1
Merchant #: 17766418
Merchant Name: Bloom Growth

June 2018

Section 2: Self-Assessment Questionnaire A

***Note:** The following questions are numbered according to PCI DSS requirements and testing procedures, as defined in the PCI DSS Requirements and Security Assessment Procedures document.*

Self-assessment completion date: 7/20/2023

Build and Maintain a Secure Network and Systems

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
2.1	(a) Are vendor-supplied defaults always changed before installing a system on the network? This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, Simple Network Management Protocol (SNMP) community strings, etc.).	- Review policies and procedures - Examine vendor documentation - Observe system configurations and account settings - Interview personnel	☑	□	□	□
	(b) Are unnecessary default accounts removed or disabled before installing a system on the network?	- Review policies and procedures - Review vendor documentation - Examine system configurations and account settings - Interview personnel	☑	□	□	□

Maintain a Vulnerability Management Program

Requirement 6: Develop and maintain secure systems and applications

	PCI DSS Question	Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
6.2	(a) Are all system components and software protected from known vulnerabilities by installing applicable vendor-supplied security patches?	- Review policies and procedures	☑	□	□	□
	(b) Are critical security patches installed within one month of release?	- Review policies and procedures - Examine system components - Compare list of security patches installed to recent vendor patch lists	☑	□	□	□

Implement Strong Access Control Measures

Requirement 8: Identify and authenticate access to system components

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
8.1.1	Are all users assigned a unique ID before allowing them to access system components or cardholder data?	- Review password procedures - Interview personnel	☑	□	□	□
8.1.3	Is access for any terminated users immediately deactivated or removed?	- Review password procedures - Examine terminated users accounts - Review current access lists - Observe returned physical authentication devices	☑	□	□	□
8.2	In addition to assigning a unique ID, is one or more of the following methods employed to authenticate all users? • Something you know, such as a password or passphrase • Something you have, such as a token device or smart card • Something you are, such as a biometric	- Review password procedures - Observe authentication processes	☑	□	□	□
8.2.3	(a) Are user password parameters configured to require passwords/passphrases meet the following? • A minimum password length of at least seven characters • Contain both numeric and alphabetic characters Alternatively, the passwords/phrases must have complexity and strength at least equivalent to the parameters specified above.	- Examine system configuration settings to verify password parameters	☑	□	□	□

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
8.5	Are group, shared, or generic accounts, passwords, or other authentication methods prohibited as follows: • Generic user IDs and accounts are disabled or removed; • Shared user IDs for system administration activities and other critical functions do not exist; and • Shared and generic user IDs are not used to administer any system components?	- Review policies and procedures - Examine user ID lists - Interview personnel	☑	□	□	□

Requirement 9: Restrict physical access to cardholder data

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
9.5	Are all media physically secured (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes)? For purposes of Requirement 9, "media" refers to all paper and electronic media containing cardholder data.	- Review policies and procedures for physically securing media - Interview personnel	☑	☐	☐	☐
9.6	(a) Is strict control maintained over the internal or external distribution of any kind of media?	- Review policies and proceduresfor distribution of media	☑	☐	☐	☐
9.6.1	Is media classified so the sensitivity of the data can be determined?	- Review policies and procedures for media classification - Interview security personnel	☑	☐	☐	☐
9.6.2	Is media sent by secured courier or other delivery method that can be accurately tracked?	- Interview personnel - Examine media distribution tracking logs and documentation	☑	☐	☐	☐
9.6.3	Is management approval obtained prior to moving the media (especially when media is distributed to individuals)?	- Interview personnel - Examine media distribution tracking logs and documentation	☑	☐	☐	☐
9.7	Is strict control maintained over the storage and accessibility of media?	- Review policies and procedures	☑	☐	☐	☐
9.8	(a) Is all media destroyed when it is no longer needed for business or legal reasons?	- Review periodic media destruction policies and procedures	☑	☐	☐	☐
9.8.1	(a) Are hardcopy materials cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed?	- Interview personnel - Examine procedures - Observe processes	☑	☐	☐	☐
	(b) Are storage containers used for materials that contain information to be destroyed secured to prevent access to the contents?	- Examine security of storage containers	☑	☐	☐	☐

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security for all personnel

***Note:** For the purposes of Requirement 12, "personnel" refers to full-time part-time employees, temporary employees and personnel, and contractors and consultants who are "resident" on the entity's site or otherwise have access to the company's site cardholder data environment.*

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
12.8	Are policies and procedures maintained and implemented to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows:					
12.8.1	Is a list of service providers maintained, including a description of the service(s) provided?	- Review policies and procedures - Observe processes - Review list of service providers	☑	□	□	□
12.8.2	Is a written agreement maintained that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process, or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment? Note: The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.	- Observe written agreements - Review policies and procedures	☑	□	□	□
12.8.3	Is there an established process for engaging service providers, including proper due diligence prior to engagement?	- Observe processes - Review policies and procedures and supporting documentation	☑	□	□	□

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
12.8.4	Is a program maintained to monitor service providers' PCI DSS compliance status at least annually?	- Observe processes - Review policies and procedures and supporting documentation	☑	□	□	□
12.8.5	Is information maintained about which PCI DSS requirements are managed by each service provider, and which are managed by the entity?	- Observe processes - Review policies and procedures and supporting documentation	☑	□	□	□
12.10.1	(a) Has an incident response plan been created to be implemented in the event of system breach?	- Review the incident response plan - Review incident response plan procedures	☑	□	□	□

Appendix A: Additional PCI DSS Requirements

Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers

This appendix is not used for merchant assessments.

Appendix A2: Additional PCI DSS Requirements for Entities using SSL/early TLS

This appendix is not used for SAQ A merchant assessments.

Appendix A3: Designated Entities Supplemental Validation (DESV)

This Appendix applies only to entities designated by a payment brand(s) or acquirer as requiring additional validation of existing PCI DSS requirements. Entities required to validate to this Appendix should use the DESV Supplemental Reporting Template and Supplemental Attestation of Compliance for reporting, and consult with the applicable payment brand and/or acquirer for submission procedures.

Appendix B: Compensating Controls Worksheet

Use this worksheet to define compensating controls for any requirement where "YES with CCW" was checked.

***Note:** Only companies that have undertaken a risk analysis and have legitimate technological or documented business constraints can consider the use of compensating controls to achieve compliance.*

Refer to Appendices B, C, and D of PCI DSS for information about compensating controls and guidance on how to complete this worksheet.

Requirement Number and Definition:

	Information Required	**Explanation**
1. Constraints	List constraints precluding compliance with the original requirement.	
2. Objective	Define the objective of the original control; identify the objective met by the compensating control.	
3. Identified Risk	Identify any additional risk posed by the lack of the original control.	
4. Definition of Compensating Controls	Define the compensating controls and explain how they address the objectives of the original control and the increased risk, if any.	
5. Validation of Compensating Controls	Define how the compensating controls were validated and tested.	
6. Maintenance	Define process and controls in place to maintain compensating controls.	

Appendix C: Explanation of Non-Applicability

If the "N/A" (Not Applicable) column was checked in the questionnaire, use this worksheet to explain why the related requirement is not applicable to your organization.

Requirement	Reason Requirement is Not Applicable
Example:	
3.4	Cardholder data is never stored electronically