Security Standards Council®

Payment Card Industry (PCI) Data Security Standard

Self-Assessment Questionnaire A and Attestation of Compliance

For use with PCI DSS Version 4.0.1

Revision 1

Publication Date: January 2025

Section 1: Assessment Information

Instruction for Submission

This document must be completed as a declaration of the results of the merchant's self-assessment with the *Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures* (PCI DSS). Complete all sections: The merchant is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact acquirer (merchant bank) or the payment brands to determine reporting and submission procedures.

Part 1. Contact Information

Part 1a. Assessed Merchant

Company name:	Winter International LLC Bloom
DBA (doing business as):	Bloom Growth
Company mailing address:	1201 Infinity Ct
Company main website:	
Company contact name:	
Company contact title:	
Company phone number:	402-378-9545
Company e-mail address:	compliance@bloomgrowth.com

Part 1b. Assessor

Provide the following information for all assessors involved in the assessment. If there was no assessor for a given assessor type, enter Not Applicable.

PCI SSC Internal Security Assessor(s)	
ISA name(s):	
Qualified Security Assessor	
Company name:	
Company mailing address:	
Company website:	
Lead Assessor Name:	
Assessor phone number:	
Assessor e-mail address:	
Assessor certificate number:	

Part 2. Executive Summary

Part 2a. Merchant Business Payment Channels (select all that apply):

Indicate all payment channels used by the business that are included in this assessment.

- □ Mail order/telephone order (MOTO)
- ☑ E-Commerce
- □ Card-present

Are any payment channels not included in this assessment? If yes, indicate which channel(s) is not included in the assessment and provide a brief explanation about why the channel was excluded.	☐ Yes ☑ No

__Note:__ If the organization has a payment channel that is not covered by this SAQ, consult with the entity(ies) to which t AOC will be submitted about validation for the other channels.

Part 2b. Description of Role with Payment Cards

For each payment channel included in this assessment as selected in Part 2a above, describe how the business stores, processes, and/or transmits account data.

E-Commerce	We do not electronically store or transmit consumer account data.

Part 2c. Description of Payment Card 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 POI devices, databases, web servers, etc., and any other necessary payment components, as applicable.* *• System components that could impact the security of account data.*	
Indicate whether the environment includes segmentation to reduce the scope of the assessment. *(Refer to “Segmentation” section of PCI DSS for guidance on segmentation.)*	☐ Yes ☑ No

Part 2d. In-Scope Locations/Facilities

List all types of physical locations/facilities (for example, retail locations, corporate offices, data centers, call centers, and ma rooms) in scope for the PCI DSS assessment.

Facility Type	**Total number of locations** (How many locations of this type are in scope)	**Location(s) of facility (city, country)**
E-Commerce	1	17766418, Lincoln, NE, US

Part 2e. PCI SSC Validated Products and Solutions

Does the merchant use any item identified on any PCI SSC Lists of Validated Products and Solutions * ?

□ Yes □ No

Provide the following information regarding each item the merchant uses from PCI SSC's Lists of Validated Products and Solutions.

Name of PCI SSC - validated Product or Solution	Version of Product or Solution	PCI SSC Standard to which product or solution was validated	PCI SSC listing reference number	Expiry date of listing (YYYY-MM-DD)
				YYYY-MM-DD

* For purposes of this document, "Lists of Validated Products and Solutions" means the lists of validated products, solutions, and/or components appearing on the PCI SSC website (www.pcisecuritystandards.org) - for example, 3DS Software Development Kits, Approved PTS Devices, Validated Payment Software, Payment Applications (PADSS), Point to Point Encryption (P2PE) solutions, Software-Based PIN Entry on COTS (SPoC) solutions, and Contactless Payments on COTS (CPoC) solutions.

Part 2f. Third-Party Service Providers

Does the merchant have relationships with one or more third-party service providers that:

• Store, process, or transmit account data on the merchant's behalf (for example, payment gateways, payment processors, payment service providers (PSPs), and off-site storage)	□ Yes ☑ No
• Manage system components included in the scope of the merchant's PCI DSS assessment (for example, via network security control services, anti-malware services, security incident and event management (SIEM), contact and call centers, web-hosting services, and IaaS, PaaS, SaaS, and FaaS cloud providers.	□ Yes ☑ No
• Could impact the security of the merchant's CDE (for example, vendors providing support via remote access, and/or bespoke software developers)	□ Yes ☑ No

If Yes:

Name of service provider:	Description of service(s) provided:

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

Part 2g. Eligibility to Complete SAQ A

Merchant certifies eligibility to complete this shortened version of the Self-Assessment Questionnaire because, for this payme channel:

☑	Merchant accepts only card-not-present (e-commerce or mail/telephone-order) transactions);
☑	All processing of cardholder data is entirely outsourced to PCI DSS validated third-party service providers;
☑	Merchant does not electronically store, process, or transmit any cardholder data on merchant systems or premises, but relies entirely on a third party(s) to handle all these functions;

☑	Merchant has confirmed that all third party(s) handling storage, processing, and/or transmission of cardholder data are PCI DSS compliant; **and**
☑	Any cardholder data the merchant retains is on paper (for example, printed reports or receipts), and these documents are not received electronically.
☑	*Additionally, for e-commerce channels:* All elements of the payment page(s) delivered to the consumer's browser originate only and directly from a PCI DSS validated third-party service provider(s).

Section 2: Self-Assessment Questionnaire A

This Attestation of Compliance reflects the results of a self-assessment, which is documented in an accompanying SAQ.

The assessment documented in this attestation and in the SAQ was completed on:	7/31/2025	
Have compensating controls been used to meet any requirement in the SAQ?	□ Yes	☑ No
Were any requirements in the SAQ identified as being not applicable (N/A)?	□ Yes	☑ No
Were any requirements in the SAQ 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 SAQ A (Section 2), dated (7/31/2025).

Based on the results documented in the SAQ A 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 SAQ are complete, all questions answered affirmatively, resulting in an overa **COMPLIANT** rating; thereby *(Bloom Growth)* has demonstrated full compliance with the PCI DSS.

□ **Non-Compliant:** Not all sections of the PCI DSS SAQ are complete, or not all questions are answered affirmatively, resulting in an overall **NON-COMPLIANT** rating, thereby *(Bloom Growth)* 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 o 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 "No" 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)

☑ PCI DSS Self-Assessment Questionnaire A, Version *(4.0.1)* was completed according to the instructions therein.

☑ All information within the above-referenced SAQ and in this attestation fairly represents the results of my assessmen in all material respects.

☑ I have confirmed with my payment application vendor that my payment system does not store sensitive authenticatio 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 *(Aperia)*

Part 3b. Merchant Attestation

Clay Upton

Signature of Merchant Executive Officer ↑	*Date: 7/31/2025*
Merchant Executive Officer Name: Clay Upton	*Title: Member*

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

If a QSA was involved or assisted with this assessment, describe the role performed:	

Signature of Duly Authorized Officer of QSA Company ↑	*Date:*
Duly Authorized Officer Name:	*QSA Company:*

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 your acquirer or the 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	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	☑	□	
6	Develop and maintain secure systems and applications	☑	□	
8	Identify and authenticate access to system components	☑	□	
9	Restrict physical access to cardholder data	☑	□	
12	Maintain a policy that addresses information security for all personnel	☑	□	

* PCI DSS Requirements indicated here refer to the questions in Section 2 of the SAQ.