PCI Security Standards Council®

Payment Card Industry
Data Security Standard

Attestation of Compliance for Report on Compliance – Service Providers

Version 4.0.1

Publication Date: August 2024

PCI DSS v4.0.1 Attestation of Compliance for Report on Compliance – Service Providers

Entity Name: Wild Apricot Inc.

Date of Report as noted in the Report on Compliance: February 20, 2025

Date Assessment Ended: February 7, 2025

Section 1: Assessment Information

Instructions for Submission

This Attestation of Compliance (AOC) must be completed as a declaration of the results of the service provider's assessment against the *Payment Card Industry Data Security Standard (PCI DSS) Requirements and Testing Procedures (*"Assessment"). Complete all sections. The service provider is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the entity(ies) to which this AOC will be submitted for reporting and submission procedures.

This AOC reflects the results documented in an associated Report on Compliance (ROC). Associated ROC sections are noted in each AOC Part/Section below.

Capitalized terms used but not otherwise defined in this document have the meanings set forth in the PCI DSS Report on Compliance Template.

Part 1. Contact Information	
Part 1a. Assessed Entity (ROC Section 1.1)	
Company name:	Personify Inc.
DBA (doing business as):	Wild Apricot Inc.
Company mailing address:	7010 Easy Wind Dr Bldg. II, Ste. 210 Austin, TX 78752
Company main website:	http://www.personifycorp.com
Company contact name:	Paul Gavura
Company contact title:	Director of Security & IT
Contact phone number:	571-758-4919
Contact e-mail address:	pgavura@personifycorp.com
Part 1b. Assessor (ROC Section 1.1)	
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):	Not Applicable
Qualified Security Assessor	
Company name:	Marcum RAS, LLC dba CBIZ RAS
Company mailing address:	201 E Kennedy Blvd #1500, Tampa, FL 33602
Company website:	https://www.cbiz.com/
Lead Assessor name:	Christopher Shaffer
Assessor phone number:	(214) 276 1599
Assessor e-mail address:	christopher.shaffer@cbiz.com
Assessor certificate number:	204-508

Part 2. Executive Summary

Part 2a. Scope Verification

Services that were INCLUDED in the scope of the Assessment (select all that apply):

Name of service(s) assessed:	Wild Apricot Payment Processing	
Type of service(s) assessed:		
Hosting Provider: □ Applications / software □ Hardware □ Infrastructure / Network □ Physical space (co-location) □ Storage □ Web-hosting services □ Security services □ 3-D Secure Hosting Provider □ Multi-Tenant Service Provider □ Other Hosting (specify):	**Managed Services:** □ Systems security services □ IT support □ Physical security □ Terminal Management System □ Other services (specify):	**Payment Processing:** □ POI / 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 these categories do not apply to the assessed service, complete "Others." If it is not clear whether a category could apply to the assessed service, consult with the entity(ies) to which this AOC will be submitted.*

Part 2. Executive Summary *(continued)*

Part 2a. Scope Verification *(continued)*

Services that are provided by the service provider but were NOT INCLUDED in the scope of the Assessment (select all that apply):

Name of service(s) not assessed:	Web Hosting

Type of service(s) not assessed:

Hosting Provider:

☐ Applications / software
☐ Hardware
☐ Infrastructure / Network
☐ Physical space (co-location)
☐ Storage
☒ Web-hosting services
☐ Security services
☐ 3-D Secure Hosting Provider
☐ Multi-Tenant Service Provider
☐ Other Hosting (specify):

Managed Services:

☐ Systems security services
☐ IT support
☐ Physical security
☐ Terminal Management System
☐ Other services (specify):

Payment Processing:

☐ POI / 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:	Wild Apricot Payment Processing Services are included in this assessment. The hosting of client organization e-commerce pages is managed by an independent group within Wild Apricot, hosted in independent facilities, and validated through an independent assessment as a merchant. Those ecommerce web pages include functionality that allow client web browsers to leverage the payment processing service.

Part 2b. Description of Role with Payment Cards (ROC Sections 2.1 and 3.1)

Describe how the business stores, processes, and/or transmits account data.	Wild Apricot payment processing solutions hosts the scripts provided by payment gateways that handle the acceptance and transmittal of CHD and SAD.

Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	Payment request results are redirected to the independent payment processing service that initiated the request - Wild Apricot ecommerce hosting solutions (which is covered in a separate independent merchant validation). However, their merchant activities have no additional ability to impact the security of cardholder data.
Describe system components that could impact the security of account data.	Systems that could impact the security of the account data include the workstations of IT administrators, the server infrastructure supporting the application, the application which uses PCI-DSS validated service provider technology to capture account data, and the firewalls and routers use to faciliate and protect system components.

Part 2. Executive Summary *(continued)*

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.*	Wild Apricot payment web servers, in Armor Defense data centers, host the scripts provided by payment gateways that receive CHD (PAN, expiration date, cardholder name) and SAD (CVC2, CVV2, CID) from Wild Apricot users over the internet using HTTPS. For one-time payments, the authorization gateway then responds with last four digits of PAN, transaction ID, result, error message, etc. For recurring payments, in addition to the previously mentioned list, the authorization gateway would also return the profile ID. The returned fields are transmitted back to the requesting browser and then to the WA e-commerce website. WA payment infrastructure is isolated from office networks and other software components. Administrative access can only be obtained via the Armor Dashboard, which is connected to CDE nodes through an IPSEC VPN tunnel between Armor and AWS. Access to the Armor Dashboard and AWS Console is subject to username/password and MFA.
Indicate whether the environment includes segmentation to reduce the scope of the Assessment. (Refer to the "Segmentation" section of PCI DSS for guidance on segmentation)	☒ Yes ☐ No

Part 2d. In-Scope Locations/Facilities (ROC Section 4.6)

List all types of physical locations/facilities (for example, corporate offices, data centers, call centers and mail rooms) in scope for this Assessment.

Facility Type	Total Number of Locations (How many locations of this type are in scope)	Location(s) of Facility (city, country)
Example: Data centers	*3*	*Boston, MA, USA*
Armor Defense Inc.	2	DFW, ORD
AWS	1	US-East-1

Part 2. Executive Summary *(continued)*

Part 2e. PCI SSC Validated Products and Solutions (ROC Section 3.3)

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

☐ Yes ☒ No

Provide the following information regarding each item the entity 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
				YYYY-MM-DD
				YYYY-MM-DD
				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, Point to Point Encryption (P2PE) solutions, Software-Based PIN Entry on COTS (SPoC) solutions, Contactless Payments on COTS (CPoC) solutions), and Mobile Payments on COTS (MPoC) products.

Part 2. Executive Summary *(continued)*

Part 2f. Third-Party Service Providers
*(*ROC Section 4.4*)*

For the services being validated, does the entity have relationships with one or more third-party service providers that:

• Store, process, or transmit account data on the entity's behalf (for example, payment gateways, payment processors, payment service providers (PSPs, and off-site storage))	☒ Yes ☐ No
• Manage system components included in the entity's Assessment (for example, via network security control services, anti-malware services, security incident and event management (SIEM), contact and call centers, web-hosting companies, and IaaS, PaaS, SaaS, and FaaS cloud providers)	☐ Yes ☒ No
• Could impact the security of the entity'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 Services Provided:**
Amazon Web Services (AWS)	Infrastructure as a Service provider (IaaS)
Armor Defense Inc.	Managed Hosting

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

Part 2. Executive Summary *(continued)*

Part 2g. Summary of Assessment (ROC Section 1.8.1)

Indicate below all responses provided within each principal PCI DSS requirement.

For all requirements identified as either "Not Applicable" or "Not Tested," complete the "Justification for Approach" table below.

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: Wild Apricot Payment Processing

PCI DSS Requirement	Requirement Finding More than one response may be selected for a given requirement. Indicate all responses that apply.				Select If a Compensating Control(s) Was Used
	In Place	Not Applicable	Not Tested	Not in Place	
Requirement 1:	☒	☒	☐	☐	☐
Requirement 2:	☒	☒	☐	☐	☐
Requirement 3:	☐	☒	☐	☐	☐
Requirement 4:	☐	☒	☐	☐	☐
Requirement 5:	☒	☒	☐	☐	☐
Requirement 6:	☒	☒	☐	☐	☐
Requirement 7:	☒	☒	☐	☐	☐
Requirement 8:	☒	☒	☐	☐	☐
Requirement 9:	☒	☒	☐	☐	☐
Requirement 10:	☒	☒	☐	☐	☐
Requirement 11:	☒	☒	☐	☐	☐
Requirement 12:	☒	☒	☐	☐	☐
Appendix A1:	☐	☒	☐	☐	☐
Appendix A2:	☐	☒	☐	☐	☐

Justification for Approach

For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.	1.4.4, 3.x, 7.2.6, 9.2.3, 9.4.1-9.4.7, 10.2.1.1 - Wild Apricot does not store CHD. 2.3.x, 4.2.1.2 - No wireless networks are connected to or part of the CDE. 4.2.1 - Wild Apricot does not transmit CHD. 4.2.2 - No end-user messaging technologies utilized. 4.2.1.1, 5.2.3.1, 5.3.2.1, 5.3.3, 5.4.1, 6.3.2, 6.4.2, 6.4.3, 7.2.4-7.2.5.1, 8.3.6, 8.4.2, 8.5.1, 8.6.x, 9.5.1.2.1, 10.4.1.1, 10.4.2.1, 10.7.2, 11.3.1.x, 11.5.1.1, 11.6.1, 12.3.x, 12.5.2.1, 12.5.3, 12.6.2, 12.6.3.x, 12.10.4.1, 12.10.7 - This requirement is not currently required to be in place and considered for a PCI DSS assessment until after March 31, 2025. As such, the QSA did not review or test for this 2024 PCI DSS assessment. 8.2.3 - Wild Apricot does not have access to customer premises. 8.2.7 - Third parties do not have access to the CDE. 8.3.10 - Wild Apricot does not allow customers access to their CDE. 9.2.3 - Wild Apricot does not utilize wireless networking within the CDE. 11.4.7 - Wild Apricot is not a multi-tenant service provider. 12.3.2 - Wild Apricot did not use the customized approach. A1.x - Wild Apricot is not a shared hosting provider. A2.x - Wild Apricot does not use any POS/POI devices with SSL and/or early TLS.
For any Not Tested responses, identify which sub-requirements were not tested and the reason.	

Section 2 Report on Compliance

(**ROC Sections 1.2 and 1.3**)

Date Assessment began: ***Note:*** *This is the first date that evidence was gathered, or observations were made.*	10/6/2024
Date Assessment ended: ***Note:*** *This is the last date that evidence was gathered, or observations were made.*	February 7, 2025
Were any requirements in the ROC unable to be met due to a legal constraint?	☐ Yes ☒ No
Were any testing activities performed remotely?	☒ Yes ☐ No

Section 3 Validation and Attestation Details

Part 3. PCI DSS Validation (ROC Section 1.7)

This AOC is based on results noted in the ROC dated *(Date of Report as noted in the ROC February 20, 2025)*.

Indicate below whether a full or partial PCI DSS assessment was completed:

☒ **Full Assessment** – All requirements have been assessed and therefore no requirements were marked as Not Tested in the ROC.

☐ **Partial Assessment** – One or more requirements have not been assessed and were therefore marked as Not Tested in the ROC. Any requirement not assessed is noted as Not Tested in Part 2g above.

Based on the results documented in the ROC noted above, each signatory identified in any of Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document *(select one):*

☒ **Compliant:** All sections of the PCI DSS ROC are complete, and all assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall **COMPLIANT** rating; thereby Wild Apricot has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above.

☐ **Non-Compliant:** Not all sections of the PCI DSS ROC are complete, or one or more requirements are marked as Not in Place, resulting in an overall **NON-COMPLIANT** rating; thereby *(Service Provider Company Name)* has not demonstrated compliance with PCI DSS requirements.

Target Date for Compliance: *YYYY-MM-DD*

An entity submitting this form with a Non-Compliant status may be required to complete the Action Plan in Part 4 of this document. Confirm with the entity to which this AOC will be submitted before completing Part 4.

☐ **Compliant but with Legal exception:** One or more assessed requirements in the ROC are marked as Not in Place due to a legal restriction that prevents the requirement from being met and all other assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall **COMPLIANT BUT WITH LEGAL EXCEPTION** rating; thereby *(Service Provider Company Name)* has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above or as Not in Place due to a legal restriction.

This option requires additional review from the entity to which this AOC will be submitted.

If selected, complete the following:

Affected Requirement	Details of how legal constraint prevents requirement from being met

Part 3. PCI DSS Validation *(continued)*

Part 3a. Service Provider Acknowledgement

Signatory(s) confirms:
(Select all that apply)

☒	The ROC was completed according to *PCI DSS*, Version 4.0.1 and was completed according to the instructions therein.
☒	All information within the above-referenced ROC and in this attestation fairly represents the results of the Assessment in all material respects.
☒	PCI DSS controls will be maintained at all times, as applicable to the entity's environment.

Part 3b. Service Provider Attestation

DocuSigned by: Paul Gavura AD40E63A709C4B0...	
Signature of Service Provider Executive Officer ↑	Date: 2/26/2025
Service Provider Executive Officer Name: Paul Gavura	Title: Director of Security & IT

Part 3c. Qualified Security Assessor (QSA) Acknowledgement

If a QSA was involved or assisted with this Assessment, indicate the role performed:	☒ QSA performed testing procedures.
	☐ QSA provided other assistance. If selected, describe all role(s) performed:

DocuSigned by: Christopher Shaffer 346B24B230CB4CA...	
Signature of Lead QSA ↑	Date: 2/26/2025
Lead QSA Name: Christopher Shaffer	
DocuSigned by: Christopher Shaffer 346B24B230CB4CA...	
Signature of Duly Authorized Officer of QSA Company ↑	Date: 2/26/2025
Duly Authorized Officer Name: Christopher Shaffer	QSA Company: Marcum RAS LLC dba CBIZ RAS

Part 3d. PCI SSC Internal Security Assessor (ISA) Involvement

If an ISA(s) was involved or assisted with this Assessment, indicate the role performed:	☐ ISA(s) performed testing procedures.
	☐ ISA(s) provided other assistance. If selected, describe all role(s) performed:

Part 4. Action Plan for Non-Compliant Requirements

Only complete Part 4 upon request of the entity to which this AOC will be submitted, and only if the Assessment has Non-Compliant results noted in Section 3.

If asked to complete this section, select the appropriate response for “Compliant to PCI DSS Requirements” for each requirement below. For any “No” responses, include the date the entity expects to be compliant with the requirement and provide a brief description of the actions being taken to meet the requirement.

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 network security controls	□	□	
2	Apply secure configurations to all system components	□	□	
3	Protect stored account data	□	□	
4	Protect cardholder data with strong cryptography during transmission over open, public networks	□	□	
5	Protect all systems and networks from malicious software	□	□	
6	Develop and maintain secure systems and software	□	□	
7	Restrict access to system components and cardholder data by business need to know	□	□	
8	Identify users and authenticate access to system components	□	□	
9	Restrict physical access to cardholder data	□	□	
10	Log and monitor all access to system components and cardholder data	□	□	
11	Test security systems and networks regularly	□	□	
12	Support information security with organizational policies and programs	□	□	
Appendix A1	Additional PCI DSS Requirements for Multi-Tenant Service Providers	□	□	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	□	□	

Note: The PCI Security Standards Council is a global standards body that provides resources for payment security professionals developed collaboratively with our stakeholder community. Our materials are accepted in numerous compliance programs worldwide. Please check with your individual compliance accepting organization to ensure that this form is acceptable in their program. For more information about PCI SSC and our stakeholder community please visit: https://www.pcisecuritystandards.org/about_us/