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: Sertifi, Inc.

Date of Report as noted in the Report on Compliance: 2025 October 23

Date Assessment Ended: 2025 October 21

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:	Flywire Corporation
DBA (doing business as):	Sertifi by Flywire; Sertifi, Inc.; Sertifi
Company mailing address:	141 Tremont Street, Suite 10, Boston, MA 02111
Company main website:	https://flywire.com
Company contact name:	Barbara Cousins
Company contact title:	Chief Information Security Officer and Chief Information Officer
Contact phone number:	+1 (800) 346-9252
Contact e-mail address:	security@flywire.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:	SecurityMetrics, Inc.
Company mailing address:	1275 West 1600 North, Orem, Utah 84057
Company website:	www.securitymetrics.com
Lead Assessor name:	Thomas McCrory
Assessor phone number:	+1 (801) 705-5664
Assessor e-mail address:	aoc@securitymetrics.com
Assessor certificate number:	203-680

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:	Sertifi Agreement Platform	
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:	Not Applicable

Type of service(s) not assessed:

Hosting Provider:	**Managed Services:**	**Payment Processing:**
☐ Applications / software	☐ Systems security services	☐ POI / card present
☐ Hardware	☐ IT support	☒ Internet / e-commerce
☐ Infrastructure / Network	☐ Physical security	☐ MOTO / Call Center
☐ Physical space (co-location)	☐ Terminal Management System	☐ ATM
☐ Storage	☐ Other services (specify):	☐ Other processing (specify):
☐ Web-hosting services		
☐ Security services		
☐ 3-D Secure Hosting Provider		
☐ Multi-Tenant Service Provider		
☐ Other Hosting (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:	All services that involve storage, processing, and/or transmission of cardholder data were included in this assessment.

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.	When a payment request is made in the Sertifi Agreement Platform, the cardholder will receive an email with a link to a payment page. The payment page (*www.fps.sertifi.com*) is served from web servers located at the Digital Realty data center in Elk Grove, Illinois. Within the payment page is an iFRAME, which performs a transparent redirect to a web form served by Azure App Services located behind an Azure application gateway. Cardholder data entered into the web form may be sent to a third-party (Skyflow) for

	storage and tokenization or directly to a payment gateway for authorization. A token is retained for future transactions. All transmissions occur using HTTPS secured with at least TLS1.2. Sertifi does not store cardholder data.
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	The Sertifi Agreement Platform processes and transmits cardholder data as part of the authorization service.
Describe system components that could impact the security of account data.	Sertifi manages network security, web applications, TLS connections, and monitoring services that could impact the security of account data.

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.*	• All connections into and out of the in-scope Virtual Private Cloud instances in the Microsoft Azure environment • All connections into and out of the in-scope systems at the Elk Grove, Illinois data center • People, processes, and technologies used to support secure transmission to and from in-scope instances within the Microsoft Azure environment • Manual and automated processes such as monitoring, patching, and responding to alerts performed by personnel located at the Chicago, Illinois offices, as applicable • Secure software development
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*
Data Center	1	Redmond, WA, USA
Data Center	1	Elk Grove, IL, USA
Corporate Office	1	Chicago, IL, USA

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
Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable
				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:
Microsoft Corporation DBA Microsoft Azure	Cloud Hosting Provider, Platform-as-a-Service (PaaS)
Digital Realty Trust, L.P.	Co-location
Google LLC DBA Google Cloud Platform (GCP)	Software-as-a-Service (SaaS) – Anti-phishing
Okta, Inc.	Identity and Authentication Services
Skyflow, Inc.	Tokenization, Storage
PayPal, Inc.'s Braintree Payment Processing System	Payment Gateway/Transaction Processing
Merchant Link LLC	Payment Gateway/Transaction Processing
Elavon, Inc.	Payment Gateway/Transaction Processing
Stripe, Inc.	Payment Gateway/Transaction Processing
FreedomPay, Inc.	Payment Gateway/Transaction Processing
First Data Merchant Services DBA Payspring	Payment Gateway/Transaction Processing
CyberSource/Authorize.Net	Payment Gateway/Transaction Processing
Zuora, Inc.	Payment Gateway/Transaction Processing
Datatrans AG (Formerly Planet Payment)	Payment Gateway/Transaction Processing/3DS Services
Shift4 Payments, LLC	Payment Gateway/Transaction Processing

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: Sertifi Agreement Platform

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.	1.2.6 – No insecure services, protocols, or ports are in use within the CDE. 1.3.3 – No wireless networks are present. 1.4.4 – Sertifi does not store cardholder data. 2.2.5 – No insecure services, protocols, or daemons are in use. 2.3.1 and 2.3.2 – No wireless networks are present. 3.2.1 – Sertifi does not store cardholder data. 3.3.1.1 – Track data is not captured in the Sertifi CDE. 3.3.1.3 – PIN Block data is not captured in the Sertifi CDE. 3.3.2 – SAD is not stored within the Sertifi CDE. 3.3.3 – Sertifi is neither an issuer, nor supports issuing services. 3.4.1 – No displays of PAN are present. 3.4.2 – Sertifi does not store cardholder data. 3.5.1 – Sertifi does not store cardholder data. 3.5.1.1 – Sertifi does not store cardholder data. 3.5.1.2 – Disk-level or partition-level encryption are not used. 3.6.1 - 3.7.8 – Sertifi does not store cardholder data. 3.7.9 – Sertifi does not share cryptographic keys for symmetric encryption with its customers. 4.2.1.2 – No wireless networks are present. 5.2.3 - 5.2.3.1 – All instances within the Sertifi CDE are protected from malware. 5.3.2.1 – All instances within the Sertifi CDE are protected from malware. 5.3.3 – No removable electronic media is generated. 5.3.5 – Only system administrators can authenticate to systems within the CDE. 6.5.2 – No significant changes have occurred in the previous year. 7.2.6 – Sertifi does not store cardholder data. 8.2.3 – Sertifi does not have access to customer premises or systems. 8.2.7 – No third-party access is allowed into the CDE. 8.3.10 - 8.3.10.1 – No Sertifi customers are permitted to access cardholder data. 8.6.1 - 8.6.3 – No accounts can be used for interactive login. 9.4.1 - 9.4.7 – No media containing cardholder data is received, generated, distributed, or stored in the Sertifi CDE. 9.5.1 - 9.5.1.3 – No POI devices are in use. 10.2.1.1 – Sertifi does not store cardholder data. 10.4.2 - 10.4.2.1 – No other system components are present. 11.3.2.1 – No significant changes have been made to the CDE in the previous year. 11.4.2 – No internal connections to the CDE are present. 11.4.7 – Sertifi is not a multi-tenant service provider. 12.3.2 – No requirements are met using the customized approach. 12.5.3 – No significant changes have been made to the CDE in the previous year.
For any Not Tested responses, identify which sub-requirements were not tested and the reason.	Not Applicable

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.*	2025-07-29
Date Assessment ended: ***Note:*** *This is the last date that evidence was gathered, or observations were made.*	2025-10-21
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 *(2025 October 23)*.

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 *Flywire Corporation DBA Sertifi by Flywire; Sertifi, Inc.; Sertifi* 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 *Flywire Corporation DBA Sertifi by Flywire; Sertifi, Inc.; Sertifi* 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 *Flywire Corporation DBA Sertifi by Flywire; Sertifi, Inc.; Sertifi* 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

Signed by:
Barbara Cousins
B630FEBD218B464...

Signature of Service Provider Executive Officer ↑	Date: 2025-10-29
Service Provider Executive Officer Name: Barbara Cousins	Title: CISO, CIO

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:

Signed by:
Thomas McCrory
47D3F84EE0B2431...

Signature of Lead QSA ↑	Date: 2025-10-29
Lead QSA Name: Thomas McCrory	

Signed by:
Gary Glover
490DC91BF4FD4DF...

Signature of Duly Authorized Officer of QSA Company ↑	Date: 2025-10-29
Duly Authorized Officer Name: Gary Glover	QSA Company: SecurityMetrics, Inc.

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/