Docusign Envelope ID: 6B651D82-63A6-4485-B04E-146C26DD5125

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: Flowbird

Date of Report as noted in the Report on Compliance: 2024/12/13

Date Assessment Ended: 2024/12/13 (December 13th, 2024)

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

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:	FLOWBIRD
DBA (doing business as):	Flowbird UP, Flowbird SAS, Flowbird Sverige AB, Cale Systems, CaleAmerica, Flowbird North America, Cale Access, Parkeon
Company mailing address:	2Ter rue du Château, 92200 Neuilly-Sur-Seine, FRANCE
Company main website:	https://www.flowbird.com/
Company contact name:	Pierre CHABOUSSANT
Company contact title:	COO
Contact phone number:	+44 7387 419 905
Contact e-mail address:	pierre.chaboussant@flowbird.group
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):	Anne BOUQUET
Qualified Security Assessor	
Company name:	XMCO
Company mailing address:	18 rue Bayard, 75008 Paris, FRANCE
Company website:	https://www.xmco.fr/
Lead Assessor name:	Clémentin BENOIST
Assessor phone number:	+33 (0) 1 79 35 29 52
Assessor e-mail address:	clementin.benoist@xmco.fr
Assessor certificate number:	QSA - 206-761

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:	Payment Gateway Flowbird Mobile Eagle Hyperswitch CWO2 Payment and settlement support for owners of Flowbird UPTs WayToPark	
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): Unattended payment Terminals, parking
☐ 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:	StreetSmart, MyParkFolio, TransFolio
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:	StreetSmart, MyParkFolio, TransFolio, Other Maintenance services: All of these services are related to products (i.e. street parking meters/ticketing sale equipments) sold by Flowbird. These services do not process any payments or cardholder data. Also, all the products sold by Flowbird have not been included in this assessment: MiniPark, City Connector, Strada Evolution, StradaPAL, Module T-PAL, Astreo, Galexio, Axio Touch, Infigo, Park&Camp.

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.	Flowbird is a level-1 service provider which sells street parking meters/ticketing sales equipments and

	provides, to its customer, payment services and a management solution for all the deployed devices. The devices embed a card reader module (M1000 / A1000 / P1000) which reads the card (stripe or chip and PIN) and handles the payment processing by sending the authorization to the Flowbird's payment gateway servers. Flowbird receives authorization requests containing Cardholder Data (PAN, ISO2 track) from the card reader devices. Requests are encrypted by the card reader with 128 bits AES keys and sent through Internet/GPRS to the payment gateway servers managed by Flowbird. Flowbird transmits Cardholder Data to acquirer, gateway and payment providers through several protocols (HTTPS, SFTP or SSL tunnels). Flowbird stores Cardholder Data encrypted in a database (AES-128) for ArchiPEL and in a PostgreSQL (AES-256) for the PCI-SSF application called Monetra. Flowbird holds PAN, full track (or EMV equivalent) and card expiration date in system memory for authorization and reporting. Flowbird also handle cryptography secrets renewal (e.g. X509 certificates and public/private key pair) for the card reader module. Flowbird provides a web and mobile application called "Flowbird App" which is used by the end-users of parking meter to pay parking time. This web application does not receive any Cardholder Data but outsources all payment functions to a payment provider through a 302 redirection. Flowbird also provides a Payment Gateway called Eagle/Hyperswitch for card-not-present transactions. This application provides an API that can be used to dynamically generate a payment page or a consumer authentication page. CHD received by the Eagle application are routed to upstream PSP, depending on merchant/customer context. Flowbird holds PAN for debt collection and client's speficic business need. Flowbird (ex-Cale Systems) also provides payment gateway services as part of their UPT solution, as well as service and support for unattended payment and fess systems Flowbird processes card present transactions being sent from unattended payment terminals, primarily parking ticket machines. Transactions including track2 data are protected with TLS v1.2/1.3 with 2048-bit encryption. The outbound transmission for Authorizations are sent over TLS v1.2/1.3 and settlements are sent over SFTP (AES-256). PAN, Cardholder name and expiry date is received via TLS 1.2/1.3 with 2048-bit encryption as part of support for the WayToPark application. PAN is translated to a

	token by Flowbird backend. The token is used in the WayToPark server during authorization. Payment processing includes online and offline transaction containin track2 data, which are received and sent for authorization in the frontend systems and processed for settlements in the backoffice systems. Settlements never include SAD. If communications are down, SAD (track2, PAN) can be stored using RSA 2048-bit encryption before authorization.
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	N/A
Describe system components that could impact the security of account data.	Firewalls and network components handling the network segmentation of the scope Virtualization infrastructure Authentication infrastructure SaaS anti-malware solution SIEM used to review log and generate alerts SaaS WAF solution

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.*	The CDE is connected to the Internet using firewalls and to Flowbird's intranet through a IPSec VPN. The CDE is only reachable by users using a VPN with MFA. The CDE is composed of several VLAN (DMZ and INZ). The critical components within the CDE are ArchiPEL payments gateway servers, Eagle application servers (exposed on the Internet), databases, HSM, acquirer gateway (Monetra) servers and Crypto servers. The following technologies and critical system components are used in Flowbird CDE: - Payment gateways - Linux and windows servers - Firewalls, switches and routers - Nutanix virtualization - Multi-factor authentication systems - Anti-malware systems - IDS systems - SIEM solution - WAF solution
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*
Flowbird offices	2	Besançon, FRANCE Moorestown, New Jersey, USA
Datacenters	4	Saint-Denis, FRANCE Courbevoie, FRANCE

		North York/Toronto, CANADA Clifton, UNITED STATES

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
Monetra	9.0.0	PCI SSF	22-45.01232.001	2025-10-01
Merchant connect Multi	4.2	PCI SSF	22-45.00143.002	2025-04-01

* 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:
Worldline eCommerce Solutions BVBA / SPRL (Ogone / Ingenico) Nexi (SSB/SIA) CyberSource Corporation 3C Payment Luxembourg S.A. (formerly SIX Payment Services Luxembourg SA) Bluefin (Tecs) Till (Simplepay) PayEx	Payment Service Provider
Interxion (Digital Realty Trust) Equinix, Inc. Digital Realty Trust, Inc. and Digital Realty Trust, L.P. Precise Parklink, Inc.	Housing services
Amazon Web Services, Inc.	Cloud Service provider
CrowdStrike SentinelOne	Antimalware providers
Almond	SOC provider
Cloudflare	WAF provider
Nexi Digital Finland (Poplatek) Banca transilvania Redsys Bambora Canada Paynetwork X Optimal Payment (Paysafe) Eigen Managing Payments Vital Processing – TSYS ADS Heartland	Acquirer and/or Payment Service Provider. There is no contract between them and Flowbird. They are not in scope of this assessment. These TPSPs are under Flowbird's customers responsibility.

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

FifthThrid (Worldpay) RBS/RBSLink (Worldpay) Global Payments BPC Elavon CiCS Monext Atos Equens Pelecard (IPI) Moneris CA CHASE PAYMENTECH Fiserv Elavon US VisaNet Credit Agricole Nets BOC CIC Moneris MPGS Worldpay Worldline	
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: Payment Gateway, Flowbird Mobile, Eagle, Hyperswitch, CWO2, Payment and settlement support for owners of Flowbird UPTs, WayToPark

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: N/A: No insecure service, protocol or ports is in use in the scope of the assessment. 1.3.3: N/A: No wireless network is used in the scope. 2.2.5: N/A: no insecure services are enabled. 2.3.1, 2.3.2: N/A: there is no wireless environment connected to the cardholder data environment. 3.3.2: N/A: This requirement is a best practice until 31 March 2025. 3.3.3: N/A: FLOWBIRD does not support issuing servic:es. 3.4.2, 3.5.1.1, 3.5.1.2: N/A: This requirement is a best practice until 31 March 2025. 3.5.1.3: N/A: no disk encryption is in used in the assessed environment. 3.7.9: N/A: Flowbird does not share keys with its customers. 4.2.1.1: N/A: This requirement is a best practice until 31 March 2025. 4.2.2: N/A: FLOWBIRD does not use end-user messaging technologies to send PAN. 5.2.3.1, 5.3.2.1, 5.3.3, 5.4.1: N/A: This requirement is a best practice until 31 March 2025. 6.3.2, 6.4.2, 6.4.3: N/A: This requirement is a best practice until 31 March 2025. 7.2.4, 7.2.5, 7.2.5.1: N/A: This requirement is a best practice until 31 March 2025. 8.2.3: N/A: FLOWBIRD does not have access to customers' systems. 8.2.7: N/A: FLOWBIRD does not provided remote access to third parties on their systems. 8.3.10, 8.3.10.1: N/A: There is no non-consumer customer accessing cardholder data. 8.4.2, 8.5.1, 8.6.1, 8.6.2, 8.6.3: N/A: This requirement is a best practice until 31 March 2025. 9.4.3, 9.4.4: N/A: According to the personnel interviewed, there is no media outside the CDE. 9.4.6: N/A: there is no hard-copy materials (no paper nor imprints). This has been validated during the scoping phase. 9.5.1, 9.5.1.1, 9.5.1.2, 9.5.1.2.1, 9.5.1.3: N/A: There is no POI devices in the scope of the assessment. 10.4.2.1, 10.7.2: N/A: This requirement is a best practice until 31 March 2025. 11.3.1.1, 11.3.1.2: N/A: This requirement is a best practice until 31 March 2025. 11.4.7: N/A: Flowbird is not a multi-tenant service provider. 11.5.1.1, 11.6.1: N/A: This requirement is a best practice until 31 March 2025. 12.3.1: N/A: This requirement is a best practice until 31 March 2025. 12.3.2: N/A: No requirement was meet with the customized approach during the audit.

	12.3.3, 12.3.4, 12.5.2.1, 12.5.3, 12.6.2, 12.6.3.1, 12.6.3.2, 12.10.4.1, 12.10.7: N/A: This requirement is a best practice until 31 March 2025. Appendix A1: N/A: Flowbird is not a Multi-Tenant Service Provider. Appendix A2: N/A: There is no POS POI terminals in the scope of the assessment.
For any Not Tested responses, identify which sub-requirements were not tested and the reason.	N/A

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.*	2024-07-01
Date Assessment ended: ***Note:*** *This is the last date that evidence was gathered, or observations were made.*	2024-12-13
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 2024-12-13)*.

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 FLOWBIRD 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:
Pierre Chaboussant
58919FEA6B99493...

Signature of Service Provider Executive Officer ↑	Date: 12/13/2024 | 15:50:54 CET
Service Provider Executive Officer Name: Pierre CHABOUSSANT	Title: COO

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: Comprehensive assessment performed by a QSA

Signed by:
Clémentin Benoist
006082363D78489...

Signature of Lead QSA ↑	Date: 2024-12-13
Lead QSA Name: Clémentin BENOIST	

Signé par :
Jordan Hordé
6E8FEB56650642A...

Signature of Duly Authorized Officer of QSA Company ↑	Date: 2024-12-13
Duly Authorized Officer Name: Jordan HORDÉ	QSA Company: XMCO

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: Project Manager and primary contact for Flowbird's PCI-DSS Audit

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/

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.