Payment Card Industry (PCI)
Data Security Standard

Attestation of Compliance for
Onsite Assessments – Service Providers

Version 3.2.1

Revision 2

September 2022

PCI Security Standards Council ®

Document Changes

Date	Version	Description
September 2022	3.2.1 Revision 2	Updated to reflect the inclusion of UnionPay as a Participating Payment Brand.

Section 1: Assessment Information

Instructions for Submission

This Attestation of Compliance must be completed as a declaration of the results of the service provider's assessment with the *Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS).* Complete all sections: The service provider is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the requesting payment brand for reporting and submission procedures.

Part 1. Service Provider and Qualified Security Assessor Information						

Part 1a. Service Provider Organization Information						
Company Name:	FLOWBIRD SAS		DBA (doing business as):			
Contact Name:	Pierre CHABOUSSANT		Title:	COO		
Telephone:	+44 7387 419 905		E-mail:	pierre.chaboussant@flowbird.group		
Business Address:	2Ter rue du Château		City:	Neuilly-sur-Seine - France		
State/Province:		Country:	FRANCE		Zip:	92200
URL:	https://www.flowbird.group/					

Part 1b. Qualified Security Assessor Company Information (if applicable)						
Company Name:	XMCO					
Lead QSA Contact Name:	Jordan Hordé		Title:	Head of GRC department		
Telephone:	+33 (0) 1 79 35 29 52		E-mail:	jordan.horde@xmco.fr		
Business Address:	18 rue Bayard		City:	Paris		
State/Province:		Country:	FRANCE		Zip:	75008
URL:	https://www.xmco.fr/					

PCi Security Standards Council ®

Part 2. Executive Summary
Part 2a. Scope Verification
Services that were INCLUDED in the scope of the PCI DSS Assessment (check all that apply):

Name of service(s) assessed:	Payment Gateway Flowbird Mobile Eagle Card Reader Device Reparation Service

Type of service(s) assessed:

Hosting Provider:	**Managed Services (specify):**	**Payment Processing:**
☐ Applications / software	☐ Systems security services	☐ POS / 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	Card Reader Device Reparation Service	
☐ Security services		
☐ 3-D Secure Hosting Provider		
☐ Shared Hosting 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):		

Note: These categories are provided for assistance only, and are not intended to limit or predetermine an entity's service description. If you feel these categories don't apply to your service, complete "Others." If you're unsure whether a category could apply to your service, consult with the applicable payment brand.

Part 2a. Scope Verification *(continued)*
Services that are provided by the service provider but were NOT INCLUDED in the scope of the PCI DSS Assessment (check all that apply):

Name of service(s) not assessed:	StreetSmart, MyParkFolio, TransFolio, CWO2, Payment and settlement support for owners of Cale UPTs, Other Maintenance Services

Type of service(s) not assessed:

Hosting Provider:	**Managed Services (specify):**	**Payment Processing:**
☐ Applications / software	☐ Systems security services	☒ POS / 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		
☐ Security services		
☐ 3-D Secure Hosting Provider		
☐ Shared Hosting 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:	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.
	CWO2, Payment and settlement support for owners of Cale UPTs:
	These services are covered by another AOC delivered to the entity Flowbird Sverige AB.

PCI Security
Standards Council ®

Part 2b. Description of Payment Card Business

Describe how and in what capacity your business stores, processes, and/or transmits cardholder 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 Card Reader Device Reparation Service to customers. Flowbird receives card reader devices from its customers, checks their status and if necessary sends them for reparation. This reparation is performed by service provider Madic. There is no Cardholder Data processing involved in the reparation process.
	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 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.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.		

Part 2c. Locations

List types of facilities (for example, retail outlets, corporate offices, data centers, call centers, etc.) and a summary of locations included in the PCI DSS review.

Type of facility:	Number of facilities of this type	Location(s) of facility (city, country):
Example: Retail outlets	*3*	*Boston, MA, USA*
Offices	1	Besançon, FRANCE
Datacenters	4	Saint-Denis, FRANCE
		Courbevoie, FRANCE
		North York/Toronto, CANADA
		Clifton, UNITED STATES

Part 2d. Payment Applications

Does the organization use one or more Payment Applications? ☒ Yes ☐ No

Provide the following information regarding the Payment Applications your organization uses:

Payment Application Name	Version Number	Application Vendor	Is application PA-DSS Listed?	PA-DSS Listing Expiry date (if applicable)
Monetra	9.0.0	Main Street Softworks	☒ Yes ☐ No	10/01/2025 (October 1, 2025)
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	

Part 2e. Description of 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).*	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.

• *Critical system components within the CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.*	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 and acquirer gateway (Monetra) servers.
Does your business use network segmentation to affect the scope of your PCI DSS environment? *(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation)*	☒ Yes ☐ No

PCi Security Standards Council®

Part 2f. Third-Party Service Providers		
Does your company have a relationship with a Qualified Integrator & Reseller (QIR) for the purpose of the services being validated?	☐ Yes	☒ No

If Yes:	
Name of QIR Company:	
QIR Individual Name:	
Description of services provided by QIR:	

Does your company have a relationship with one or more third-party service providers (for example, Qualified Integrator Resellers (QIR), gateways, payment processors, payment service providers (PSP), web-hosting companies, airline booking agents, loyalty program agents, etc.) for the purpose of the services being validated?	☒ Yes ☐ No

If Yes:	

Name of service provider:	Description of services provided:
Global Payments BPC Elavon CiCS Monext Atos Equens Pelecard (IPI) Moneris CA Chase Paymentech Elavon US VisaNet Credit Agricole CIC Nets Bank Of China (BOC) MasterCard Payment Gateway Worldpay Worldline	Acquirers
Ogone / Ingenico Nexi (SSB/SIA) CyberSource Corporation 3C Payment Luxembourg S.A. (formerly SIX Payment Services Luxembourg SA) Tecs Poplatek Uniteller	Payment Service Providers (PSP)

Till (Simplepay)	
Redsys	
PayEx	
Worldline	
TNS	Transmission
InterXion Österreich GmbH	Housing
Precise ParkLink, Inc.	
Equinix, Inc.	
Digital Realty Trust, Inc. and Digital Realty Trust, L.P.	
Amazon Web Services, Inc.	Cloud Service Provider

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

Part 2g. Summary of Requirements Tested

For each PCI DSS Requirement, select one of the following:

- **Full** – The requirement and all sub-requirements of that requirement were assessed, and no sub-requirements were marked as "Not Tested" or "Not Applicable" in the ROC.

- **Partial** – One or more sub-requirements of that requirement were marked as "Not Tested" or "Not Applicable" in the ROC.

- **None** – All sub-requirements of that requirement were marked as "Not Tested" and/or "Not Applicable" in the ROC.

For all requirements identified as either "Partial" or "None," provide details in the "Justification for Approach" column, including:

- Details of specific sub-requirements that were marked as either "Not Tested" and/or "Not Applicable" in the ROC

- Reason why sub-requirement(s) were not tested or not applicable

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 App Mobile			
PCI DSS Requirement	**Details of Requirements Assessed**			
	Full	**Partial**	**None**	**Justification for Approach** (Required for all "Partial" and "None" responses. Identify which sub-requirements were not tested and the reason.)
Requirement 1:	☐	☒	☐	**1.2.2 - N/A: no router is included in the scope.**
Requirement 2:	☐	☒	☐	**2.1.1 - N/A: no wireless environment is included in the scope.** **2.2.3 - N/A: There is no insecure services, daemons, or protocols in use.** **2.6 - N/A: FLOWBIRD is not a shared hosting provider.**
Requirement 3:	☐	☒	☐	**3.4.1 - N/A: FLOWBIRD does not use disk encryption.** **3.6.6 - N/A: There is no process which includes manual clear-text cryptographic key-management operations.**
Requirement 4:	☐	☒	☐	**4.1.1 - N/A: no wireless environment used to transmit CHD or connected to the CDE.**
Requirement 5:	☒	☐	☐	
Requirement 6:	☒	☐	☐	
Requirement 7:	☒	☐	☐	
Requirement 8:	☐	☒	☐	**8.1.5 - N/A: FLOWBIRD does not provide remote access to third parties on their systems.** **8.5.1 - N/A: FLOWBIRD does not have access to customers' systems.**

Requirement 9:	☐	☐	☐	**9.8.1 - N/A: there is no hard-copy materials (no paper or imprints). This has been validated during the scoping phase.**
Requirement 10:	☒	☐	☐	
Requirement 11:	☒	☐	☐	
Requirement 12:	☒	☐	☐	
Appendix A1:	☐	☐	☒	**N/A: FLOWBIRD is not a shared hosting provider.**
Appendix A2:	☐	☐	☒	**N/A: there is no POS POI terminal in scope.**

Section 2: Report on Compliance

This Attestation of Compliance reflects the results of an onsite assessment, which is documented in an accompanying Report on Compliance (ROC).

The assessment documented in this attestation and in the ROC was completed on:	*12/22/2023 (December 22, 2023)*
Have compensating controls been used to meet any requirement in the ROC?	☐ Yes ☒ No
Were any requirements in the ROC identified as being not applicable (N/A)?	☒ Yes ☐ No
Were any requirements not tested?	☐ Yes ☒ No
Were any requirements in the ROC unable to be met due to a legal constraint?	☐ Yes ☒ No

![PCi Security Standards Council logo]

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in the ROC dated *12/22/2023 (December 22, 2023).*

Based on the results documented in the ROC 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 ROC are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby *FLOWBIRD* has demonstrated full compliance with the PCI DSS.
☐	**Non-Compliant:** Not all sections of the PCI DSS ROC are complete, or not all questions are answered affirmatively, resulting in an overall **NON-COMPLIANT** rating, thereby 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 of this document. *Check with the payment brand(s) before completing Part 4.*
☐	**Compliant but with Legal exception:** One or more requirements are marked "Not in Place" 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:

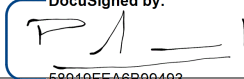*(Check all that apply)*

☒	The ROC was completed according to the *PCI DSS Requirements and Security Assessment Procedures*, Version *3.2.1*, and was completed according to the instructions therein.
☒	All information within the above-referenced ROC and in this attestation fairly represents the results of my assessment in all material respects.
☒	I have confirmed with my payment application vendor that my payment system does not store sensitive authentication 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.

PCi Security
Standards Council ®

Part 3a. Acknowledgement of Status (continued)

⊠	No evidence of full track data[1], CAV2, CVC2, CVN2, CVV2, or CID 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 *Qualys*

Part 3b. Service Provider Attestation

DocuSigned by:

[signature]

58919FEA6B99493...

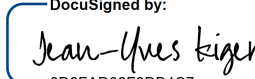| *Signature of Service Provider Executive Officer* ↑	*Date:* 27/12/2023
Service Provider Executive Officer Name: PIERRE CHABOUSSANT	*Title:* Group Chief Operating Officer

---

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

If a QSA was involved or assisted with this assessment, describe the role performed:	*Comprehensive assessment performed by a QSA of XMCO company*

DocuSigned by:

Jean-Yves Kiger

6D6FAD82F3DB4C7...

Signature of Duly Authorized Officer of QSA Company ↑	*Date: 12/22/2023 (December 22, 2023)*
Duly Authorized Officer Name: Jean-Yves KIGER	*QSA Company:* XMCO

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:	*Anne BOUQUET - Flowbird ISA* *Project Manager and primary contact for Flowbird's PCI-DSS Audit*

---

[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.

PCI Security Standards Council®

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 the applicable 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**	
1	Install and maintain a firewall configuration to protect cardholder data	⊠	☐	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	⊠	☐	
3	Protect stored cardholder data	⊠	☐	
4	Encrypt transmission of cardholder data across open, public networks	⊠	☐	
5	Protect all systems against malware and regularly update anti-virus software or programs	⊠	☐	
6	Develop and maintain secure systems and applications	⊠	☐	
7	Restrict access to cardholder data by business need to know	⊠	☐	
8	Identify and authenticate access to system components	⊠	☐	
9	Restrict physical access to cardholder data	⊠	☐	
10	Track and monitor all access to network resources and cardholder data	⊠	☐	
11	Regularly test security systems and processes	⊠	☐	
12	Maintain a policy that addresses information security for all personnel	⊠	☐	
Appendix A1	Additional PCI DSS Requirements for Shared Hosting Providers	⊠	☐	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	⊠	☐	