



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 UP

Date of Report as noted in the Report on Compliance: 2025/12/12

Date Assessment Ended: 2025/12/12 (December 12th, 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:	Flowbird UP
DBA (doing business as):	Flowbird UP, Flowbird SAS, Flowbird Sverige AB, Cale Systems, CaleAmerica, Flowbird North America, Cale Access, Parkeon, Arrive
Company mailing address:	2Ter rue du Château, 92200 Neuilly-Sur-Seine, FRANCE
Company main website:	https://arrive.com
Company contact name:	Martin Sandstrom
Company contact title:	Chief Strategy & Transformation Officer
Contact phone number:	+14704714851
Contact e-mail address:	martin.sandstrom@arrive.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):	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: <input type="checkbox"/> Applications / software <input type="checkbox"/> Hardware <input type="checkbox"/> Infrastructure / Network <input type="checkbox"/> Physical space (co-location) <input type="checkbox"/> Storage <input type="checkbox"/> Web-hosting services <input type="checkbox"/> Security services <input type="checkbox"/> 3-D Secure Hosting Provider <input type="checkbox"/> Multi-Tenant Service Provider <input type="checkbox"/> Other Hosting (specify):	Managed Services: <input type="checkbox"/> Systems security services <input type="checkbox"/> IT support <input type="checkbox"/> Physical security <input type="checkbox"/> Terminal Management System <input type="checkbox"/> Other services (specify):	Payment Processing: <input checked="" type="checkbox"/> POI / card present <input checked="" type="checkbox"/> Internet / e-commerce <input type="checkbox"/> MOTO / Call Center <input type="checkbox"/> ATM <input checked="" type="checkbox"/> Other processing (specify): Unattended payment Terminals, parking
<input type="checkbox"/> Account Management	<input type="checkbox"/> Fraud and Chargeback	<input checked="" type="checkbox"/> Payment Gateway/Switch
<input type="checkbox"/> Back-Office Services	<input type="checkbox"/> Issuer Processing	<input type="checkbox"/> Prepaid Services
<input type="checkbox"/> Billing Management	<input type="checkbox"/> Loyalty Programs	<input type="checkbox"/> Records Management
<input type="checkbox"/> Clearing and Settlement	<input checked="" type="checkbox"/> Merchant Services	<input type="checkbox"/> Tax/Government Payments
<input type="checkbox"/> Network Provider		
<input type="checkbox"/> 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:	Managed Services:	Payment Processing:
<input type="checkbox"/> Applications / software <input type="checkbox"/> Hardware <input type="checkbox"/> Infrastructure / Network <input type="checkbox"/> Physical space (co-location) <input type="checkbox"/> Storage <input type="checkbox"/> Web-hosting services <input type="checkbox"/> Security services <input type="checkbox"/> 3-D Secure Hosting Provider <input type="checkbox"/> Multi-Tenant Service Provider <input type="checkbox"/> Other Hosting (specify):	<input type="checkbox"/> Systems security services <input type="checkbox"/> IT support <input type="checkbox"/> Physical security <input type="checkbox"/> Terminal Management System <input type="checkbox"/> Other services (specify):	<input checked="" type="checkbox"/> POI / card present <input type="checkbox"/> Internet / e-commerce <input type="checkbox"/> MOTO / Call Center <input type="checkbox"/> ATM <input type="checkbox"/> Other processing (specify):
<input type="checkbox"/> Account Management	<input type="checkbox"/> Fraud and Chargeback	<input checked="" type="checkbox"/> Payment Gateway/Switch
<input type="checkbox"/> Back-Office Services	<input type="checkbox"/> Issuer Processing	<input type="checkbox"/> Prepaid Services
<input type="checkbox"/> Billing Management	<input type="checkbox"/> Loyalty Programs	<input type="checkbox"/> Records Management
<input type="checkbox"/> Clearing and Settlement	<input type="checkbox"/> Merchant Services	<input type="checkbox"/> Tax/Government Payments
<input type="checkbox"/> 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 specific 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



	<p>token by Flowbird backend. The token is used in the WayToPark server during authorization.</p> <p>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.</p> <p>If communications are down, SAD (track2, PAN) can be stored using RSA 2048-bit encryption before authorization.</p>
<p>Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.</p>	<p>N/A</p>
<p>Describe system components that could impact the security of account data.</p>	<p>Firewalls and network components handling the network segmentation of the scope</p> <p>Virtualization infrastructure</p> <p>Authentication infrastructure</p> <p>SaaS anti-malware solution</p> <p>SIEM used to review log and generate alerts</p> <p>SaaS WAF solution</p>



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)
<i>Example: Data centers</i>	3	<i>Boston, MA, USA</i>
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
Merchant Connect Multi	4.2	PCI SSF	25-45.00143.003	2028-06-02

* 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:

<ul style="list-style-type: none"> 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)) 	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
<ul style="list-style-type: none"> 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) 	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
<ul style="list-style-type: none"> Could impact the security of the entity's CDE (for example, vendors providing support via remote access, and/or bespoke software developers). 	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> 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) Elavon	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
Splunk LLC	SIEM provider
Nexi Digital Finland (Poplatek) Banca transilvania Redsys Bambora Canada Paynetwork X Optimal Payment (Paysafe) Eigen Managing Payments	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.



Vital Processing – TSYS ADS Heartland FifthThrid (Worldpay) RBS/RBSLink (Worldpay) Global Payments BPC CiCS Monext Atos Equens Pelec card (IPI) Moneris CA CHASE PAYMENTECH Fiserv 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:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 2:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 3:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 4:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 5:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 6:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 7:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 8:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 9:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 10:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 11:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 12:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Appendix A1:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Appendix A2:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Justification for Approach



For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.

- Req. 1.2.6: No insecure service, protocol or ports is in use in the scope of the assessment.
- Req. 1.3.3: No wireless network is used in the scope.
- Req. 2.2.5: no insecure services are enabled.
- Req. 2.3.1, 2.3.2: there is no wireless environment connected to the cardholder data environment.
- Req 3.3.2: ARRIVE does not store any Sensitive Authentication Data.
- Req. 3.3.3: ARRIVE does not support issuing service
- Req. 3.5.1.2, 3.5.1.3: no disk encryption is used in the assessed environment.
- Req. 3.7.9: ARRIVE does not share keys with its customers.
- Req. 4.2.1.2: there is no wireless environment connected to the cardholder data environment.
- Req. 4.2.2: ARRIVE does not use end-user messaging technologies to send PAN.
- Req. 5.3.2.1: Antimalwares perform continuous behavioral analysis of systems.
- Req. 6.4.1: This requirement is now superseded by Requirement 6.4.2
- Req. 8.2.3: ARRIVE does not have access to customers' systems.
- Req. 8.2.7: ARRIVE does not provide remote access to third parties on their systems.
- Req. 8.3.10: This requirement is now superseded by Requirement 8.3.10.1
- Req. 9.4.1.1, 9.4.1.2: There is no offline media backups with cardholder data.
- Req. 9.4.3, 9.4.4: According to the personnel interviewed, there is no media sent outside the CDE.
- Req. 9.4.6: there is no hard-copy materials (no paper nor imprints). This has been validated during the scoping phase.
- Req. 9.5.1, 9.5.1.1, 9.5.1.2, 9.5.1.2.1, 9.5.1.3: There is no POI terminals in the scope of the assessment.



	<p>Req. 10.7.1: This requirement is now superseded by Requirement 10.7.2</p> <p>Req. 11.2.2: there is no wireless environment connected to the cardholder data environment.</p> <p>Req. 11.4.7: Arrive is not a multi-tenant service provider.</p> <p>Req. 12.3.2: No requirement was met with the customized approach in the scope of the assessment.</p> <p>Req. A1: The assessed entity is not a multi-tenant service provider.</p> <p>Req. A2: There is no POS POI terminals in the scope of the assessment.</p> <p>Req A3: The assessed entity is not a designated entity.</p>
<p>For any Not Tested responses, identify which sub-requirements were not tested and the reason.</p>	<p>N/A</p>



Section 2 Report on Compliance

(ROC Sections 1.2 and 1.3)

Date Assessment began: <i>Note: This is the first date that evidence was gathered, or observations were made.</i>	2025-06-16
Date Assessment ended: <i>Note: This is the last date that evidence was gathered, or observations were made.</i>	2025-12-12
Were any requirements in the ROC unable to be met due to a legal constraint?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Were any testing activities performed remotely?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> 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 2025-12-12)*.

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)*:

<input checked="" type="checkbox"/>	<p>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 UP has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above.</p>								
<input type="checkbox"/>	<p>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 <i>(Service Provider Company Name)</i> has not demonstrated compliance with PCI DSS requirements.</p> <p>Target Date for Compliance: <i>YYYY-MM-DD</i></p> <p>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.</p>								
<input type="checkbox"/>	<p>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 <i>(Service Provider Company Name)</i> 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.</p> <p>This option requires additional review from the entity to which this AOC will be submitted.</p> <p><i>If selected, complete the following:</i></p> <table border="1" style="width: 100%; border-collapse: collapse; margin-top: 10px;"> <thead> <tr> <th style="width: 35%; padding: 5px;">Affected Requirement</th> <th style="padding: 5px;">Details of how legal constraint prevents requirement from being met</th> </tr> </thead> <tbody> <tr> <td style="height: 20px;"></td> <td></td> </tr> <tr> <td style="height: 20px;"></td> <td></td> </tr> <tr> <td style="height: 20px;"></td> <td></td> </tr> </tbody> </table>	Affected Requirement	Details of how legal constraint prevents requirement from being met						
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)

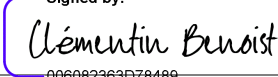
<input checked="" type="checkbox"/>	The ROC was completed according to <i>PCI DSS</i> , Version 4.0.1 and was completed according to the instructions therein.
<input checked="" type="checkbox"/>	All information within the above-referenced ROC and in this attestation fairly represents the results of the Assessment in all material respects.
<input checked="" type="checkbox"/>	PCI DSS controls will be maintained at all times, as applicable to the entity's environment.

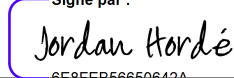
Part 3b. Service Provider Attestation

Signed by:  522F14961C8846F...	
Signature of Service Provider Executive Officer ↑	Date: 12/12/2025 11:11:59 CET
Service Provider Executive Officer Name: Martin Sandstrom	Title: Chief Strategy & Transformation Officer

Part 3c. Qualified Security Assessor (QSA) Acknowledgement

If a QSA was involved or assisted with this Assessment, indicate the role performed:	<input checked="" type="checkbox"/> QSA performed testing procedures.
	<input checked="" type="checkbox"/> QSA provided other assistance. If selected, describe all role(s) performed: Comprehensive assessment performed by a QSA

Signed by:  006082363D78489...	
Signature of Lead QSA ↑	Date: 2025-12-12
Lead QSA Name: Clémentin BENOIST	

Signé par :  6E8FEB56650642A...	
Signature of Duly Authorized Officer of QSA Company ↑	Date: 2025-12-12
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:	<input type="checkbox"/> ISA(s) performed testing procedures.
	<input checked="" type="checkbox"/> 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	<input type="checkbox"/>	<input type="checkbox"/>	
2	Apply secure configurations to all system components	<input type="checkbox"/>	<input type="checkbox"/>	
3	Protect stored account data	<input type="checkbox"/>	<input type="checkbox"/>	
4	Protect cardholder data with strong cryptography during transmission over open, public networks	<input type="checkbox"/>	<input type="checkbox"/>	
5	Protect all systems and networks from malicious software	<input type="checkbox"/>	<input type="checkbox"/>	
6	Develop and maintain secure systems and software	<input type="checkbox"/>	<input type="checkbox"/>	
7	Restrict access to system components and cardholder data by business need to know	<input type="checkbox"/>	<input type="checkbox"/>	
8	Identify users and authenticate access to system components	<input type="checkbox"/>	<input type="checkbox"/>	
9	Restrict physical access to cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
10	Log and monitor all access to system components and cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
11	Test security systems and networks regularly	<input type="checkbox"/>	<input type="checkbox"/>	
12	Support information security with organizational policies and programs	<input type="checkbox"/>	<input type="checkbox"/>	
Appendix A1	Additional PCI DSS Requirements for Multi-Tenant Service Providers	<input type="checkbox"/>	<input type="checkbox"/>	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	<input type="checkbox"/>	<input type="checkbox"/>	

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/