Payment Card Industry (PCI)

Data Security Standard

Attestation of Compliance for Onsite Assessments – Service Providers

Version 3.2.1

June 2018

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 Sverige AB		DBA (doing business as):	Flowbird, Cale Systems, Cale America, Flowbird North America, Cale Access, Parkeon		
Contact Name:	Poya Sedighi		Title:	PCI Responsible		
Telephone:	+46 8 799 37 05		E-mail:	poya.sedighi@flowbird.group		
Business Address:	Borgarfjordsgatan 7		City:	Kista		
State/Province:	Not applicable	Country:	Sweden		Zip:	164 21
URL:	https://www.flowbird.group					

Part 1b. Qualified Security Assessor Company Information (if applicable)						
Company Name:	VikingCloud					
Lead QSA Contact Name:	Björn Haraldsson		Title:	Principal Security Consultant		
Telephone:	+1 833 903 3469		E-mail:	bjornharaldsson@vikingcloud.com		
Business Address:	70 W Madison St Ste 400		City:	Chicago		
State/Province:	Illinois	Country:	USA		Zip:	Il 60602
URL:	https://www.vikingcloud.com					

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:	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 ☐ Security services ☐ 3-D Secure Hosting Provider ☐ Shared Hosting Provider ☐ Other Hosting (specify):	**Managed Services (specify):** ☐ Systems security services ☐ IT support ☐ Physical security ☐ Terminal Management System ☐ Other services (specify):	**Payment Processing:** ☒ POS / 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 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:	Not Applicable	
Type of service(s) not assessed:		
Hosting Provider: ☐ Applications / software ☐ Hardware ☐ Infrastructure / Network ☐ Physical space (co-location) ☐ Storage ☐ Web ☐ Security services ☐ 3-D Secure Hosting Provider ☐ Shared Hosting Provider ☐ Other Hosting (specify):	**Managed Services (specify):** ☐ Systems security services ☐ IT support ☐ Physical security ☐ Terminal Management System ☐ Other services (specify):	**Payment Processing:** ☐ POS / 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:	Not Applicable	

Part 2b. Description of Payment Card Business

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	Flowbird Sverige AB and Flowbird North America (Flowbird) are Level 1 Service Providers providing payment gateway services as part of their business as a global supplier of flexible unattended payment solutions (UPT), as well as service and support for unattended payment and fee systems. Flowbird Sverige AB (formerly known as Cale Access) serves the European market and operates out of Sweden. Flowbird North America (formerly known as Cale Systems) operates out of New Jersey, USA and has a datacenter in Montreal, Canada. Flowbird North America serves customers in Canada and the USA. Both entities are wholly owned by Flowbird Group, their French parent company. Flowbird processes transactions being sent from unattended payment terminals, primarily parking ticket machines. Transactions including track2 are protected using data packet encryption, employing RSA 1024-bit or 2048-bit encryption. The outbound transmissions for Authorizations are sent over TLS v1.2 and settlements are sent over SFTP. The HTTPS connections use a VeriSign certificate with AES 256-bit encryption. The SFTP connection use SSH with AES 256-bit encryption. For Flowbird North America, Card Security Code, PAN, Cardholder name and Expiry date is received via TLS v1.2 protected communication as part of support for an application and server called WayToPark. PAN is translated to a token by Flowbird North America´s back-end. The token is used in the WayToPark server during authorization. Payment processing includes online and offline transactions containing track-2 data, which are received and sent for authorization in the front-end systems and processed for settlement in the back-office systems; settlement only includes PAN and never SAD. Cardholder data, PAN, Expiry date and Truncated PAN (first 6 and last 4 digits) is stored after authorization in the CDE databases encrypted using RSA 2048-bit encryption. If communication is down during authorization, the incoming transactions are stored including track-2 and protected using data packet encryption, employing RSA 1024-bit or 2048-

	bit encryption. This is a temporary pre-authorization storage. Flowbird also uses lists of hashed PANs, SHA256 with an additional protection called Conlon algorithm. This list does not contain truncated PANs and are only used to verify if Card present or Card not present transaction use a blacklisted card.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	Not Applicable

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):
Head office	2	Kista, Sweden Moorestown, New Jersey, USA
Data center	2	Järfälla, Sweden Montreal, Canada

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)
Merchant Connect Multi	4.2.x	Tender Retail	☒ Yes ☐ No	28 Oct 2022
CaleTerminalGatewayService	Latest	In-house	☐ Yes ☒ No	Not applicable
MembershipPublicService	Latest	In-house	☐ Yes ☒ No	Not applicable
Cale Offline Processing Service	Latest	In-house	☐ Yes ☒ No	Not applicable
CaleCreditCardService	Latest	In-house	☐ Yes ☒ No	Not applicable
Cwo2PostpaymentService	Latest	In-house	☐ Yes ☒ No	Not applicable
Cwo2	Latest	In-house	☐ Yes ☒ No	Not applicable
Cwo2CitationPayment	Latest	In-house	☐ Yes ☒ No	Not applicable
CryptographySystemService	Latest	In-house	☐ Yes ☒ No	Not applicable

Allvis	Latest	In-house	☐ Yes ☒ No	Not applicable

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).*
• *Critical system components within the CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.*
	The assessment covered connections to and from the Flowbird CDE which included:
	• Connections from POI devices at retail locations using RSA 2048-bit encryption and legacy POI devices that only support RSA 1024-bit encryption. POI devices are not in scope for Flowbird as they are owned and operated by Flowbird´s customers.
	Connections are going out from Flowbird Sverige AB CDE to payment service providers and processors.
	The technologies and critical system components used in Flowbird Sverige AB CDE consists of:
	• Payment Gateways used to accept incoming transactions from POS systems.
	• Servers:
	  ○ Windows Server
	  ○ VMware ESXi
	  ○ CentOS
	• Network Segmentation Functions as applied by firewalls and jump hosts
	• Multi-factor Authentication Systems
	• Firewalls
	  ○ Border Firewalls
	  ○ Segmentation Firewalls
	• Switches
	• Internal network segments:
	• Log Management Systems
	• Processor Connections
	• IDS Systems
	• Log Management Systems
	• Anti-Virus Systems
	• Databases

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

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:	Not Applicable	
QIR Individual Name:	Not Applicable	
Description of services provided by QIR:	Not Applicable	
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:**	
AFFI Informatique	Media Destruction	
Cologix	Physical hosting provider, Montreal, Canada	
GlobalConnect	Physical hosting provider, Järfälla, Sweden	
Stena Recycling	Media Destruction	
Trustwave	Managed IDS and SIEM	
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:	CWO2, Payment and settlement support for owners of Flowbird UPTs, WayToPark

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: No routers are in scope
Requirement 2:	☐	☒	☐	2.1.1 Flowbird has no wireless environments connected to the cardholder data environment 2.6 Flowbird is not a shared hosting provider.
Requirement 3:	☐	☒	☐	3.4.1 Disk encryption is not used. 3.5.4: Cryptographic keys are not stored 3.6.3: Cryptographic keys are not stored
Requirement 4:	☐	☒	☐	4.1.1 Flowbird does not have any wireless networks connected to the cardholder data environment
Requirement 5:	☐	☒	☐	5.1.2: All applicable systems have anti-virus enabled
Requirement 6:	☐	☒	☐	6.4.6: No significant change has occurred
Requirement 7:	☒	☐	☐	
Requirement 8:	☐	☒	☐	8.1.5: No vendors have access to Flowbird´s systems 8.5.1: Flowbird does not have remote access to any customer systems.
Requirement 9:	☐	☒	☐	9.5.1: Flowbird does not have any media backups

				9.8.1: Flowbird does not have any hard-copy with cardholder data 9.9: Flowbird does not have any card-capture devices nor point-of-sale locations in scope. 9.9.1: Flowbird does not have any card-capture devices nor point-of-sale locations in scope. 9.9.2: Flowbird does not have any card-capture devices nor point-of-sale locations in scope. 9.9.3: Flowbird does not have any card-capture devices nor point-of-sale locations in scope.
Requirement 10:	☒	☐	☐	
Requirement 11:	☐	☒	☐	11.1.1: Flowbird does not have any wireless in the CDE. 11.2.3 Flowbird has not made any significant changes to their envirionment in the past 12 months.
Requirement 12:	☐	☒	☐	12.3.9: Flowbird does not grant third parties access to the cardholder data environment.
Appendix A1:	☐	☐	☒	Flowbird is not a shared hosting provider
Appendix A2:	☐	☐	☒	Flowbird does not have POS POI terminals with early SSL

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:	July 15, 2022	
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

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in the ROC dated July 15, 2022.

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 Sverige AB* 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 *(Service Provider Company Name)* 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.

Part 3a. Acknowledgement of Status (continued)	
☒	No evidence of full track data[1], CAV2, CVC2, CID, or CVV2 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 *SecureTrust*

[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.

Part 3b. Service Provider Attestation	
	
Signature of Service Provider Executive Officer ↑	*Date: July 15, 2022*
Service Provider Executive Officer Name: Poya Sedighi	*Title: Information System Security Officer*

Part 3c. Qualified Security Assessor (QSA) Acknowledgement (if applicable)	
If a QSA was involved or assisted with this assessment, describe the role performed:	Björn Haraldsson, QSA, PA QSA was the lead auditor and competed the Report on Compliance.

Signature of Duly Authorized Officer of QSA Company ↑	*Date: July 15, 2022*
Duly Authorized Officer Name: Björn Haraldsson	*QSA Company:* VikingCloud

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:	Not Applicable

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	☒	☐