



# **Payment Card Industry Data Security Standard**

---

## **Attestation of Compliance for Report on Compliance – Service Providers**

**Version 4.0**

Revision 2

Publication Date: August 2023



# **PCI DSS v4.0 Attestation of Compliance for Report on Compliance – Service Providers**

**Entity Name: Clover Network, Inc.**

**Assessment End Date: 13-Sep-2024**

**Date of Report as noted in the Report on Compliance: 17-Sep-2024**



## 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:	Clover Network, Inc.
DBA (doing business as):	Clover Network, Inc., Clover Sport, LLC, Bypass Mobile, LLC
Company mailing address:	415 Mathilda Ave, Sunnyvale, CA 94085 USA
Company main website:	<a href="https://www.clover.com">https://www.clover.com</a>
Company contact name:	Cory Lesley
Company contact title:	Director, Risk and Control
Contact phone number:	+1 (402) 819-6682
Contact e-mail address:	cory.lesley@fiserv.com

#### Part 1b. Assessor (ROC Section 1.1)

Provide the following information for all assessors involved in the Assessment. If there was no assessor for a given assessor type, enter Not Applicable.

PCI SSC Internal Security Assessor(s)	
ISA name(s):	Not Applicable
Qualified Security Assessor	
Company name:	VikingCloud
Company mailing address:	70 West Madison Street suite 400, Chicago, IL, 60602
Company website:	<a href="https://www.vikingcloud.com">https://www.vikingcloud.com</a>
Lead Assessor name:	Mark Turner
Assessor phone number:	+1 833 907 0702
Assessor e-mail address:	markturner@vikingcloud.com
Assessor certificate number:	204-190



## 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:		Clover Network, Clover Sport (Bypass Mobile) Payment Processing Services	
Type of service(s) assessed:			
<b>Hosting Provider:</b> <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): Content Manager		<b>Managed Services:</b> <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 type="checkbox"/> Account Management <input type="checkbox"/> Back-Office Services <input type="checkbox"/> Billing Management <input type="checkbox"/> Clearing and Settlement <input type="checkbox"/> Network Provider <input type="checkbox"/> Others (specify):		<b>Payment Processing:</b> <input type="checkbox"/> POI / card present <input checked="" type="checkbox"/> Internet / e-commerce <input type="checkbox"/> MOTO / Call Center <input type="checkbox"/> ATM <input type="checkbox"/> Other processing (specify):  <input type="checkbox"/> Fraud and Chargeback <input type="checkbox"/> Issuer Processing <input type="checkbox"/> Loyalty Programs <input type="checkbox"/> Merchant Services <input checked="" type="checkbox"/> Payment Gateway/Switch <input type="checkbox"/> Prepaid Services <input type="checkbox"/> Records Management <input type="checkbox"/> Tax/Government Payments	

**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: Clover POS

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:

The Clover POS is covered in a PCI DSS Pin Audit assessment dated 10/31/2023.

**Part 2b. Description of Role with Payment Cards (ROC Section 2.1)**

Describe how the business stores, processes, and/or transmits account data.

Clover comprised of Clover Network Inc. and Clover Sport LLC is a level 1 service provider.  
 Clover Network receives and transmits cardholder data (PAN, name, expiration date, card security code) that is branded by Visa, MasterCard, American Express, Discover, or JCB.  
 Clover Network does not store PAN, name, card security code, or expiration date.

When the credit card holder purchases an item, Java script is loaded into the credit card holder's browser and the credit data (PAN, name, expiration date, card security code) is encrypted using the RSA4096 public Key issued by the Transarmor service prior to sending to Clover Network. First Data Merchant Services is a business unit in Fiserv that is responsible for the Transarmor service which is assessed separately as part of the Global Business Solutions (GBS) assessment (GBS-ROC, GBS-AOC).

After encryption (RSA 4096-bit), this java script will pass this encrypted card data (PAN, name, card security code, expiration date) to Clover Network tokenization service via API endpoint using a TLS v1.2 (AES 256-bit) protocol which will send the payment data (PAN, name, expiry, card security code) Clover Network Payment service where the transaction (PAN, name, expiry, Card Security Code) is sent to FDNA Rapid Connect (payment gateway) for processing using TLS 1.2 AES-256. Upon successful authorization the Clover Network Tokenization service sends the payment data (PAN, name, expiry, card security code) to Transarmor for the tokenization process.

For reoccurring transactions the Clover Network tokenization service prepares the card data (PAN, name, card security code, expiration date) by ensuring the data is encrypted prior to sending to Transarmor for tokenization. The flow of this process starts when Clover Network Tokenization service receives the API request. It first checks if the incoming request has encrypted card data (PAN, name, expiration date, card security code). If the card data is not encrypted, then it first does the encryption with the same Transarmor RSA4096 public key and then passes (TLS v1.2 (AES-256)) this encrypted PAN, name, card security code, and expiration date to the Transarmor service for tokenization.

The Transarmor services tokenizes the PAN and purges the card security code and sends the token back to the Clover Network tokenization service (TLS v1.2 (AES 256-bit)). The Transarmor token is then encrypted by Clover Network tokenization service using the GCP HSM service (AES 256-bit). After this Clover Network tokenization service generates a random alphanumeric wrapper around the token called a "Clover Network token" it then returns the "Clover Network token" to its clients (TLS v1.2 (AES 256-bit)). The Clover Network tokenization service stores the encrypted (AES 256-bit) Transarmor token in a SQL database.

Clover Network does not store any card data.

Upon receiving the "Clover Network token", the clients call the server-to-server Clover Network payment service API to process the payment and passes (TLS

v1.2 (AES 256-bit)) the “Clover Network token” is in the request body.

Once Clover Network payment Service (Auth) receives this payment API request it reaches out to Clover Network tokenization service for detokenization of the “Clover Network token”.

For detokenizing the “Clover Network token”, the Clover Network tokenization service pulls the Transarmor token from the database and passes that to the Transarmor service. The Transarmor service then detokenizes its token and returns back the encrypted card (RSA4096) data (PAN) to Clover Network.

Clover Network tokenization service returns this encrypted card data (PAN, name, expiry) to Clover Network payment service (auth), for payment processing, which is passed TLS v1.2 (AES 256-bit) to the First Data Merchant Services Rapid Connect (payment gateway) for actual payment processing.

During payment processing neither the Clover Network tokenization service nor Clover Network Payment service will store the PAN information. These services are only processing encrypted card data in memory during payment processing.

Payeezy is a payment gateway that accepts payment calls from merchants/clients through Payeezy APIs utilizing TLS 1.2 AES-256 bit encryption. When a request comes in, the Payeezy API translation layer checks for unencrypted PAN, if found PAN will be encrypted with voltage AES-256 bit encryption and sent to the Clover Network Tokenization services for tokenizing the PAN. Once the PAN has been tokenized the Clover token is sent back to Payeezy API transaction layer where the transaction layer calls Clover Network (Clover payment services) to process the payment using the Clover token. If the request contained only a Clover token and no PAN then the API transaction layer calls Clover Network (Clover payment services) to process the payment using the Clover token.

BIN lookup service provides the bin lookup API that allows clients to look up credit card BIN (Bank Identification Number) details based on the first 6 digits of the card number.

This service accepts credit card numbers in RSA 4096-bit encrypted format and decrypts them in memory and then finds the bin details in the BIN file which is pre-populated by a separate process of downloading and parsing the Global BIN File (GBF) from the Fiserv system.

Once this service finds a matching BIN, the BIN file then pulls its BIN information and returns it to clients. No data related to the credit cards is being stored.



	<p>Clover Sport accepts Visa, MasterCard, American Express, and Discover branded cards. Clover Sport collects card data (PAN, name, expiry) through a web-based API accessed via TLS 1.2 AES-128/256 by client mobile applications, then transmits the pertinent data to Clover Network Tokenization Service (separate assessment) via TLS 1.2 AES-256 encrypted connections. Clover Sport receives back payment token data that is stored along with truncated PAN (last four), name, and expiry for future transaction management as needed. No full PAN is ever stored by Clover Sport. Non-transactional data is in the form of adjustments, order lookups, and refunds where Clover Sport will connect to Clover Network (separate assessment) using token previously provided.</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>Not Applicable – Clover is not otherwise involved or impact the security of cardholder data.</p>
<p>Describe system components that could impact the security of account data.</p>	<p>VPC access control lists AWS &amp; GCP security groups</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 following Clover logical environments were included in the production location:

- Firewalls
- AWS & GCP VPCs
- Servers for data transmission, encryption, and production support
- FIM
- IDS
- Antivirus
- Wireless Scanning
- Network connections
- Transmission protocols
- Encryption protocols
- Logging
- Time Synchronization
- Server Operating Systems

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>
Data Center	4	AWS: US-East-1a, US-East-1c, US-East-1d GCP - Dalles, Oregon, USA
Offices	1	Sunnyvale, CA, USA



**Part 2. Executive Summary (continued)**

**Part 2e. PCI SSC Validated Products and Solutions (ROC Section 3.3)**

Does the entity use any item identified on any PCI SSC Lists of Validated Products and Solutions\*?

Yes  No

Provide the following information regarding each item the entity uses from PCI SSC's Lists of Validated Products and Solutions:

Name of PCI SSC-validated Product or Solution	Version of Product or Solution	PCI SSC Standard to which Product or Solution Was Validated	PCI SSC Listing Reference Number	Expiry Date of Listing
Not Applicable	N/A	Not Applicable	Not Applicable	Not Applicable

---

\* 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](http://www.pcisecuritystandards.org))—for example, 3DS Software Development Kits, Approved PTS Devices, Validated Payment Software, Payment Applications (PA-DSS), Point to Point Encryption (P2PE) solutions, Software-Based PIN Entry on COTS (SPoC) solutions, and Contactless Payments on COTS (CPoC) solutions.



**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"> <li>• 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))</li> </ul>	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
<ul style="list-style-type: none"> <li>• 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)</li> </ul>	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
<ul style="list-style-type: none"> <li>• Could impact the security of the entity's CDE (for example, vendors providing support via remote access, and/or bespoke software developers).</li> </ul>	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No

**If Yes:**

<b>Name of Service Provider:</b>	<b>Description of Services Provided:</b>
AWS	Cloud Services (VPC)
GCP	Cloud Services (VPC)
Cloudflare	Web Application Firewall

**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:* Clover Network, Clover Sport (Bypass Mobile) Payment Processing Services

PCI DSS Requirement	Requirement Finding More than one response may be selected for a given requirement. Indicate all responses that apply.				Select If Below Method(s) Was Used	
	In Place	Not Applicable	Not Tested	Not in Place	Customized Approach	Compensating Controls
Requirement 1:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input 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"/>	<input type="checkbox"/>
Requirement 3:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input 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"/>	<input type="checkbox"/>
Requirement 5:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input 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"/>	<input type="checkbox"/>
Requirement 7:	<input checked="" type="checkbox"/>	<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"/>	<input type="checkbox"/>
Requirement 9:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input 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"/>	<input type="checkbox"/>
Requirement 11:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input 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"/>	<input type="checkbox"/>
Appendix A1:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input 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"/>	<input type="checkbox"/>

**Justification for Approach**



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

- 1.3.3 No wireless networks in scope.
- 1.4.4 Clover does not store cardholder data.
- 2.3.1 No wireless networks in scope.
- 2.3.2 No wireless networks in scope.
- 3.2.1 Clover does not store cardholder data.
- 3.3.2 Clover does not store SAD data.
- 3.3.3: Clover does not store SAD data.
- 3.4.1 Clover does not store cardholder data.
- 3.4.2: Not Applicable Best Practice.
- 3.5.1 Clover does not store cardholder data.
- 3.5.1.1: Not Applicable Best Practice.
- 3.5.1.2: Not Applicable Best Practice.
- 3.5.1.3 Clover does not store cardholder data.
- 3.6.1 Clover does not store cardholder data.
- 3.6.1.1 Not Applicable Best Practice.
- 3.6.1.2 Clover does not store cardholder data.
- 3.6.1.3 Clover does not store cardholder data.
- 3.6.1.4 Clover does not store cardholder data.
- 3.7.1 Clover does not store cardholder data.
- 3.7.2 Clover does not store cardholder data.
- 3.7.3 Clover does not store cardholder data.
- 3.7.4 Clover does not store cardholder data.
- 3.7.5 Clover does not store cardholder data.
- 3.7.6 Clover does not store cardholder data.
- 3.7.7 Clover does not store cardholder data.
- 3.7.8 Clover does not store cardholder data.
- 3.7.9 Clover does not store cardholder data.
- 4.2.1.1: Not Applicable Best Practice.
- 4.2.1.2 No wireless networks in scope.
- 4.2.2: No PAN is sent using end-user messaging.
- 5.2.3.1: Not Applicable Best Practice.
- 5.3.2.1: Not Applicable Best Practice.
- 5.3.3 Not Applicable Best Practice.
- 5.4.1: Not Applicable Best Practice.
- 6.3.2: Not Applicable Best Practice.
- 6.4.2 Not Applicable Best Practice.
- 6.4.3: Not Applicable Best Practice.
- 7.2.4: Not Applicable Best Practice.
- 7.2.5: Not Applicable Best Practice.
- 7.2.5.1: Not Applicable Best Practice.
- 7.2.6 Clover does not store cardholder data.
- 8.2.3 Clover does not have access to customer premise.
- 8.3.6: Not Applicable Best Practice.
- 8.3.10 Not Applicable Best Practice.
- 8.3.10.1: Not Applicable Best Practice.
- 8.4.2: Not Applicable Best Practice.



	<p>8.5.1: Not Applicable Best Practice.              8.6.1: Not Applicable Best Practice.              8.6.2: Not Applicable Best Practice.              8.6.3: Not Applicable Best Practice.              9.5.1: No POS devices in use at Clover.              9.5.1.1: No POS devices in use at Clover.              9.5.1.2: No POS devices in use at Clover.              9.5.1.2.1: No POS devices in use at Clover.              9.5.1.3: No POS devices in use at Clover.              10.4.1.1: Not Applicable Best Practice.              10.4.2.1: Not Applicable Best Practice.              10.7.2: Not Applicable Best Practice.              11.3.1.1: Not Applicable Best Practice.              11.3.1.2: Not Applicable Best Practice.              11.4.7: Not Applicable Best Practice.              11.5.1.1: Not Applicable Best Practice.              11.6.1 Not Applicable Best Practice.              12.3.1: Not Applicable Best Practice.              12.3.3: Not Applicable Best Practice.              12.3.4: Not Applicable Best Practice.              12.5.2.1: Not Applicable Best Practice.              12.5.3: Not Applicable Best Practice.              12.6.2: Not Applicable Best Practice.              12.6.3.1: Not Applicable Best Practice.              12.6.3.2: Not Applicable Best Practice.              12.10.4.1 Not Applicable Best Practice.              12.10.7 Not Applicable Best Practice.              A1.1.1: Not Applicable Best Practice.              A1.1.2 Clover is not a multi-tenant service provider.              A1.1.3 Clover is not a multi-tenant service provider.              A1.1.4: Not Applicable Best Practice.              A1.2.1 Clover is not a multi-tenant service provider              A1.2.2 Clover is not a multi-tenant service provider.              A1.2.3: Not Applicable Best Practice.              A2.1.1: Clover does not use early SSL or TLS.              A2.1.2: Clover does not use early SSL or TLS.              A2.1.3: Clover does not use early SSL or TLS.</p>
<p>.For any Not Tested responses, identify which sub-requirements were not tested and the reason.</p>	<p>Not Applicable</p>



## Section 2 Report on Compliance

(ROC Sections 1.2 and 1.3.2)

Date Assessment began: <i>Note: This is the first date that evidence was gathered, or observations were made.</i>		04-Dec-2023
Date Assessment ended: <i>Note: This is the last date that evidence was gathered, or observations were made.</i>		13-Sep-2024
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? If yes, for each testing activity below, indicate whether remote assessment activities were performed:		<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
• Examine documentation	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
• Interview personnel	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
• Examine/observe live data	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
• Observe process being performed	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
• Observe physical environment	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
• Interactive testing	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
• Other:	<input type="checkbox"/> Yes	<input checked="" 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 17-Sep-2024.

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><b>Compliant:</b> 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 <b>COMPLIANT</b> rating; thereby Clover Network Inc, / Clover Sport, LLC has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above.</p>								
<input type="checkbox"/>	<p><b>Non-Compliant:</b> 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 <b>NON-COMPLIANT</b> rating; thereby (<i>Service Provider Company Name</i>) has not demonstrated compliance with PCI DSS requirements.</p> <p><b>Target Date</b> for Compliance: YYYY-MM-DD</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><b>Compliant but with Legal exception:</b> 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 <b>COMPLIANT BUT WITH LEGAL EXCEPTION</b> 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%;">Affected Requirement</th> <th>Details of how legal constraint prevents requirement from being met</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> <tr> <td> </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)**

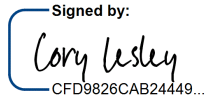
**Part 3a. Service Provider Acknowledgement**

**Signatory(s) confirms:**

(Select all that apply)

- The ROC was completed according to *PCI DSS*, Version 4.0 and was completed according to the instructions therein.
- All information within the above-referenced ROC and in this attestation fairly represents the results of the Assessment in all material respects.
- PCI DSS controls will be maintained at all times, as applicable to the entity's environment.

**Part 3b. Service Provider Attestation**

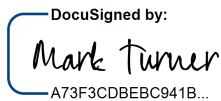
Signed by:  
  
 CFD9826CAB24449...

Signature of Service Provider Executive Officer ↑	Date: 23-Sep-2024
Service Provider Executive Officer Name: Cory Lesley	Title: Director, Risk & Control

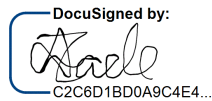
**Part 3c. Qualified Security Assessor (QSA) Acknowledgement**

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:

DocuSigned by:  
  
 A73F3CDBEBC941B...

Signature of Lead QSA ↑	Date: 23-Sep-2024
Lead QSA Name: Mark Turner	

DocuSigned by:  
  
 C2C6D1BD0A9C4E4...

Signature of Duly Authorized Officer of QSA Company ↑	Date: 23-Sep-2024
Duly Authorized Officer Name: Michael Aminzade	QSA Company: VikingCloud



**Part 3d. PCI SSC Internal Security Assessor (ISA) Involvement**

If an ISA(s) was involved or assisted with this Assessment, indicate the role performed:

ISA(s) performed testing procedures.

ISA(s) provided other assistance.

If selected, describe all role(s) performed:



## Part 4. Action Plan for Non-Compliant Requirements

Only complete Part 4 upon request of the entity to which this AOC will be submitted, and only if the Assessment has Non-Compliant results noted in Section 3.

If asked to complete this section, select the appropriate response for “Compliant to PCI DSS Requirements” for each requirement below. For any “No” responses, include the date the entity expects to be compliant with the requirement and provide a brief description of the actions being taken to meet the requirement.

PCI DSS Requirement	Description of Requirement	Compliant to PCI DSS Requirements (Select One)		Remediation Date and Actions (If “NO” selected for any Requirement)
		YES	NO	
1	Install and maintain network security controls	<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"/>	

