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: Preczn Inc.

Date of Report as noted in the Report on Compliance: November 15, 2025

Date Assessment Ended: November 15, 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:	Preczn, Inc.
DBA (doing business as):	Not Applicable
Company mailing address:	2384 Copper Springs Dr, Reno, NV 89521
Company main website:	https://www.preczn.com/
Company contact name:	Bobby Bonestell
Company contact title:	Information Security Officer
Contact phone number:	+1 404-800-1166
Contact e-mail address:	bobby@preczn.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:	Prescient Security LLC
Company mailing address:	1900 Church Street, Suite 300 Nashville, TN 37203
Company website:	https://prescientsecurity.com/
Lead Assessor name:	Himanshu Goel
Assessor phone number:	+1 212-271-0175
Assessor e-mail address:	pci@prescientsecurity.com
Assessor certificate number:	PCI DSS QSA Certificate Number: 203-539

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:	Preczn Platform	
Type of service(s) assessed:		
Hosting Provider: ☐ Applications / software ☐ Hardware ☐ Infrastructure / Network ☐ Physical space (co-location) ☐ Storage ☐ Web-hosting services ☐ Security services ☐ 3-D Secure Hosting Provider ☐ Multi-Tenant Service Provider ☐ Other Hosting (specify):	**Managed Services:** ☐ Systems security services ☐ IT support ☐ Physical security ☐ Terminal Management System ☐ Other services (specify):	**Payment Processing:** ☐ POI / card present ☒ Internet / e-commerce ☐ MOTO / Call Center ☐ ATM ☐ Other processing (specify):
☒ 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): None		

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:	Not Applicable

Type of service(s) not assessed:

Hosting Provider:	**Managed Services:**	**Payment Processing:**
☐ Applications / software	☐ Systems security services	☐ POI / 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-hosting services		
☐ Security services		
☐ 3-D Secure Hosting Provider		
☐ Multi-Tenant Service 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:	Not Applicable

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.	Preczn provides a cloud-native software-as-a-service (SaaS) payment orchestration platform. The Preczn platform performs the following functions with regard the security of cardholder data (CHD): ▪ Forwarding of transactions to designated payment service providers for authorization and settlement of card transactions. ▪ Tokenization and storage of PAN and Expiry for use in recurring transactions and for reducing the scope of PCI compliance for customers. ▪ Payment orchestration provides dynamic routing of transactions to optimize the management of transaction fees.

	The Preczn platform operates in Amazon Web Services (AWS), is made up of the following core components: ▪ Payment Gateway – AWS ECS that process all CHD transactions. ▪ Partner Integrations – API integrations to the Payment Gateway. ▪ Management Portal – external to the direct processing of CHD used by customers to manage their relationship with Preczn, including the registration of API keys used for authentication of the checkout and API integrations. ▪ Database Storage and Encryption – use of AWS PCI compliant services to store and encrypt PAN and Expiry in a secure manner. Transmission of CHD Preczn accepts online e-commerce CNP transactions (PAN, Expiry, CVV) either through a hosted checkout page embedded within their customers website or via an API integration with their customers. All transmission of cardholder data is secured via HTTPS over TLS 1.3. Processing of CHD Inbound transaction PANs, CVVs, and Expiry are sent to the designated payment service provider for transaction authorization and settlement. When the transaction is confirmed, Preczn strips the CVV from memory, encrypts the PAN using program-level (AES256) encryption, and inserts/stores the record (with encrypted PAN) for recurring payment. Storage of CHD Preczn stores encrypted PANs for recurring payments (as optioned by customer) in AWS NoSQL DynamoDB using program encryption (AWS KMS) (using AES256 encryption).
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	Transmission of CHD Preczn accepts online e-commerce CNP transactions (PAN, Expiry, CVV) either through a hosted checkout page embedded within their customers website or via an API integration with their customers. All transmission of cardholder data is secured via HTTPS over TLS 1.3. Processing of CHD Inbound transaction PANs, CVVs, and Expiry are sent to the designated payment service provider for transaction authorization and settlement. When the transaction is confirmed, Preczn strips the CVV from memory, encrypts the PAN using program-level (AES256) encryption, and inserts/stores the record (with encrypted PAN) for recurring payment. Storage of CHD Preczn stores encrypted PANs for recurring payments (as optioned by customer) in AWS NoSQL DynamoDB using program encryption (AWS KMS) (using AES256 encryption).
Describe system components that could impact the security of account data.	System Components include: ▪ AWS CloudFront, AWS API Gateway, and AWS Application Load Balancers (transmit).

	▪ AWS WAF (transmit). ▪ AWS S3 Buckets (web application resources). ▪ AWS Containers (transmit, process, and store) using custom application code, including Hosted Checkout, API Integrations, Payment Gateway, and Customer Portal. ▪ AWS KMS for managing the encryption infrastructure used for storing PAN. Program-level encryption (AES256). ▪ Workstations which access the CDE for systems and network support (Apple Mac OS). ▪ Security supporting technologies: ✓ Anti-Virus ✓ Intrusion Detection ✓ Centralized Log Management Preczn transmits all transactions to the payment processor for authorization, clearing and settlement via HTTPS TLSv1.3.

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.*	All in-bound traffic passes securely (HTTPS TLS v1.3) first through AWS Web Application Firewall services which are configured with security blocking rules and alerts within the AWS Oregon production data center. AWS API Gateway and Application Load Balancers (ALB) route transactions to the private network for processing by Payment Gateway services, which forward transactions to payment service providers, encrypt card data for use in future transactions, and return a tokenized value for the PAN to customers for reference in future or recurring transactions. Preczn operates from the Amazon Web Services (AWS) Oregon (Production) region including AWS PCI compliant Infrastructure as a Service (IaaS) support. All management of the infrastructure environment is performed by Preczn technology staff. System Components include: ▪ AWS CloudFront, AWS API Gateway, and AWS Application Load Balancers (transmit). ▪ AWS WAF (transmit). ▪ AWS S3 Buckets (web application resources). ▪ AWS Containers (transmit, process, and store) using custom application code, including Hosted Checkout, API Integrations, Payment Gateway, and Customer Portal. ▪ AWS KMS for managing the encryption infrastructure used for storing PAN. Program-level encryption (AES256). ▪ Workstations which access the CDE for systems and network support (Apple Mac OS). ▪ Security supporting technologies: ✓ Anti-Virus ✓ Intrusion Detection ✓ Centralized Log Management ▪ Preczn transmits all transactions to the payment processor for authorization, clearing and settlement via HTTPS TLSv1.3.
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)
AWS | Public Cloud Infrastructure as a Service	1	us-west-2 | Oregon, US West

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.	Not Applicable.	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) (for example, 3DS Software Development Kits, Approved PTS Devices, Validated Payment Software, Point to Point Encryption (P2PE) solutions, Software-Based PIN Entry on COTS (SPoC) solutions, Contactless Payments on COTS (CPoC) solutions), and Mobile Payments on COTS (MPoC) products.

Part 2. Executive Summary *(continued)*

Part 2f. Third-Party Service Providers (ROC Section 4.4)

For the services being validated, does the entity have relationships with one or more third-party service providers that:

• Store, process, or transmit account data on the entity's behalf (for example, payment gateways, payment processors, payment service providers (PSPs, and off-site storage))	☒ Yes ☐ No
• Manage system components included in the entity's Assessment (for example, via network security control services, anti-malware services, security incident and event management (SIEM), contact and call centers, web-hosting companies, and IaaS, PaaS, SaaS, and FaaS cloud providers)	☒ Yes ☐ No
• Could impact the security of the entity's CDE (for example, vendors providing support via remote access, and/or bespoke software developers).	☒ Yes ☐ No

If Yes:

Name of Service Provider:	Description of Services Provided:
Microsoft AWS	Infrastructure as a service provider
Stripe	Payment Processor
Adyen	Payment Processor
Google Cloud Identity	Identity Provider
Merchant eSolutions, Inc	Payment Processor
Payrix Holdings, LLC	Payment Processor
Checkout.com	Payment Processor
Braintree Payments	Payment Processor
PayPal Inc.	Payment Processor
AffiniPay LLC	Payment Processor
Finix Payments, Inc.	Payment Processor
Till Payments Solutions Pty Ltd (Nuvei)	Payment Processor
Authorize.net	Payment Processor
Rainforest	Payment Processor
Stax	Payment Processor

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: Preczn Platform

PCI DSS Requirement	Requirement Finding More than one response may be selected for a given requirement. Indicate all responses that apply.				Select If a Compensating Control(s) Was Used
	In Place	Not Applicable	Not Tested	Not in Place	
Requirement 1:	☒	☒	☐	☐	☐
Requirement 2:	☒	☒	☐	☐	☐
Requirement 3:	☒	☒	☐	☐	☐
Requirement 4:	☒	☒	☐	☐	☐
Requirement 5:	☒	☒	☐	☐	☐
Requirement 6:	☒	☒	☐	☐	☐
Requirement 7:	☒	☒	☐	☐	☐
Requirement 8:	☒	☒	☐	☐	☒
Requirement 9:	☒	☒	☐	☐	☐
Requirement 10:	☒	☒	☐	☐	☐
Requirement 11:	☒	☒	☐	☐	☒
Requirement 12:	☒	☒	☐	☐	☐
Appendix A1:	☐	☒	☐	☐	☐
Appendix A2:	☐	☒	☐	☐	☐

Justification for Approach

For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.	1.2.6 - Preczn did not support the use of insecure services, protocols, or ports. 1.3.3 - Preczn did not support wireless environments that connected to the CDE. 2.2.5 - No insecure services, daemons, or protocols were enabled.

	2.3.1, 2.3.2 - Preczn did not support wireless environments that connect to the CDE. 3.3.1.1 - Preczn API did not accept full track data. 3.3.1.2 - CVV was not stored in the Preczn databases. 3.3.1.3 - Preczn API did not accept PIN data. 3.3.2 - SAD was never stored electronically in the Preczn database. 3.3.3 - Preczn was not an issuer and did not support issuing services. 3.4.1 - Preczn did not provide a display of full PAN. 3.4.2 - PAN is not copied or relocated to remote environments 3.6.1.3 - Preczn did not use manual or clear text keys. 3.7.2 - Preczn did not distribute cryptographic keys. 3.7.6 - Preczn was not using manual clear text key management. 3.7.9 - Keys were not shared with Preczn customers. 4.2.1.2 - There were no wireless networks permitted for transmitting cardholder data. 4.2.2 - Preczn did not use end-user messaging technologies to send cardholder data. 5.2.3, 5.2.3.1 - All systems in the CDE were protected by anti-virus software. 6.4.1 – This requirement was superseded by Requirement 6.4.2 as of 31-March-2025. 6.4.3 - Preczn didn’t host the payment pages. 6.5.2 - Preczn had no significant changes during the assessment period. 8.2.2 - Preczn did not use shared authentication credentials. 8.2.3 - Preczn did not have remote access to customer premises. 8.2.7 - Vendors were not provided with access (local or remote) to the payment card environment. 8.3.10 - This requirement was superseded by Requirement 8.3.10.1 as of 31-March-2025. 8.3.10.1 - Customer didn’t have access to account data. 8.6.1, 8.6.2, 8.6.3 - Accounts used by systems or applications were not permitted for interactive login under any circumstances. 9.4.1, 9.4.1.1, 9.4.1.2, 9.4.2, 9.4.3, 9.4.4, 9.4.5, 9.4.5.1, 9.4.6, 9.4.7 - Preczn did not store CHD in physical media. 9.5.1, 9.5.1.1, 9.5.1.2, 9.5.1.2.1, 9.5.1.3 - Preczn was not responsible for the management of card reading devices. 10.7.1 - This requirement was superseded by Requirement 10.7.2 as of 31-March-2025. 11.2.2 - Preczn did not support wireless access points within the cardholder data environment.

	11.3.1.3, 11.3.2.1 - There were no significant changes to the Preczn system components during the assessment year. 11.4.5, 11.4.6 - Preczn did not rely on network segmentation to isolate the CDE. 11.4.7 - Preczn clients were not required to perform external pentation testing of the services they use from Preczn. 11.6.1 – Preczn didn't host the payment pages. 12.3.2 - There was no PCI DSS requirement that the Preczn met with the customized approach. Appendix A1 – Preczn was not considered a multi-tenant service provider. Appendix A2 – Preczn did not support SSL or early TLS.
For any Not Tested responses, identify which sub-requirements were not tested and the reason.	Not Applicable

Section 2 Report on Compliance

(**ROC Sections 1.2 and 1.3**)

Date Assessment began: ***Note:*** *This is the first date that evidence was gathered, or observations were made.*	September 17, 2025
Date Assessment ended: ***Note:*** *This is the last date that evidence was gathered, or observations were made.*	November 15, 2025
Were any requirements in the ROC unable to be met due to a legal constraint?	☐ Yes ☒ No
Were any testing activities performed remotely?	☒ Yes ☐ No

Section 3 Validation and Attestation Details

Part 3. PCI DSS Validation (ROC Section 1.7)

This AOC is based on results noted in the ROC dated November 15, 2025.

Indicate below whether a full or partial PCI DSS assessment was completed:

☒ **Full Assessment** – All requirements have been assessed and therefore no requirements were marked as Not Tested in the ROC.

☐ **Partial Assessment** – One or more requirements have not been assessed and were therefore marked as Not Tested in the ROC. Any requirement not assessed is noted as Not Tested in Part 2g above.

Based on the results documented in the ROC noted above, each signatory identified in any of Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document *(select one)**:***

☒	**Compliant:** All sections of the PCI DSS ROC are complete, and all assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall **COMPLIANT** rating; thereby ***Preczn, Inc. (Preczn Platform)*** has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above.
☐	**Non-Compliant:** Not all sections of the PCI DSS ROC are complete, or one or more requirements are marked as Not in Place, resulting in an overall **NON-COMPLIANT** rating; thereby *Not Applicable* has not demonstrated compliance with PCI DSS requirements. **Target Date** for Compliance: *Not Applicable* An entity submitting this form with a Non-Compliant status may be required to complete the Action Plan in Part 4 of this document. Confirm with the entity to which this AOC will be submitted before completing Part 4.
☐	**Compliant but with Legal exception:** One or more assessed requirements in the ROC are marked as Not in Place due to a legal restriction that prevents the requirement from being met and all other assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall **COMPLIANT BUT WITH LEGAL EXCEPTION** rating; thereby *Not Applicable* has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above or as Not in Place due to a legal restriction. This option requires additional review from the entity to which this AOC will be submitted. *If selected, complete the following:*

Affected Requirement	Details of how legal constraint prevents requirement from being met
Not Applicable.	Not Applicable.
Not Applicable.	Not Applicable.

Part 3. PCI DSS Validation *(continued)*

Part 3a. Service Provider Acknowledgement

Signatory(s) confirms:
(Select all that apply)

☒	The ROC was completed according to *PCI DSS*, Version 4.0.1 and was completed according to the instructions therein.
☒	All information within the above-referenced ROC and in this attestation fairly represents the results of the Assessment in all material respects.
☒	PCI DSS controls will be maintained at all times, as applicable to the entity's environment.

Part 3b. Service Provider Attestation

DocuSigned by:
Bobby Bonestell
219DD9D7E1C4491...

Signature of Service Provider Executive Officer ↑	Date: 12/1/2025
Service Provider Executive Officer Name: **Bobby Bonestell**	Title: **Information Security Officer**

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:

Signed by:
Himanshu Goel
6B14947C9CD74BE...

Signature of Lead QSA ↑	Date: 12/5/2025
Lead QSA Name: **Himanshu Goel**	

DocuSigned by:
Kevin Whalen
0B32514137D7445...

Signature of Duly Authorized Officer of QSA Company ↑	Date: 12/6/2025
Duly Authorized Officer Name: **Kevin Whalen**	QSA Company: **Prescient Security LLC**

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	☐	☐	
2	Apply secure configurations to all system components	☐	☐	
3	Protect stored account data	☐	☐	
4	Protect cardholder data with strong cryptography during transmission over open, public networks	☐	☐	
5	Protect all systems and networks from malicious software	☐	☐	
6	Develop and maintain secure systems and software	☐	☐	
7	Restrict access to system components and cardholder data by business need to know	☐	☐	
8	Identify users and authenticate access to system components	☐	☐	
9	Restrict physical access to cardholder data	☐	☐	
10	Log and monitor all access to system components and cardholder data	☐	☐	
11	Test security systems and networks regularly	☐	☐	
12	Support information security with organizational policies and programs	☐	☐	
Appendix A1	Additional PCI DSS Requirements for Multi-Tenant Service Providers	☐	☐	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	☐	☐	

Note: The PCI Security Standards Council is a global standards body that provides resources for payment security professionals developed collaboratively with our stakeholder community. Our materials are accepted in numerous compliance programs worldwide. Please check with your individual compliance accepting organization to ensure that this form is acceptable in their program. For more information about PCI SSC and our stakeholder community please visit: https://www.pcisecuritystandards.org/about_us/