



Payment Card Industry Data Security Standard

Attestation of Compliance for Report on Compliance – Service Providers

Version 4.0

Revision 1

Publication Date: December 2022



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

Entity Name: PAYSECURE TECHNOLOGY LIMITED

Assessment End Date: 7th December 2023

Date of Report as noted in the Report on Compliance: 7th December 2023



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: | PAYSECURE TECHNOLOGY LIMITED |
| DBA (doing business as): | |
| Company mailing address: | Office 5.11, 25 Wilton Road, Victoria, London SW1V 1LW, |
| Company main website: | https://api.paysecure.net/ https://api.choicepay.ca/ https://api.paymentsclub.net/ |
| Company contact name: | Sridhar Sethuraman |
| Company contact title: | COO / CPO |
| Contact phone number: | +44(0)7931642646 |
| Contact e-mail address: | sri@paysecure.net |

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: | Cybersigma Consulting Services LLP |
| Company mailing address: | support@cybersigmacs.com |
| Company website: | https://cybersigmacs.com |



| | |
|------------------------------|--------------------------|
| Lead Assessor name: | Sharwan Kumar |
| Assessor phone number: | +91 9650158347 |
| Assessor e-mail address: | sharwan@cybersigmacs.com |
| Assessor certificate number: | 205-518 |

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 Service Provider:- Paysecure Application | |
| 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 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 | | |
| <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 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: | All the services except the mentioned above | |
| Type of service(s) not 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 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 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 | | |
| <input type="checkbox"/> Others (specify): | | |
| Provide a brief explanation why any checked services were not included in the Assessment: | Paysecure is an collection of intelligent global payment gateway and payments licences portfolio with integrations and partnerships with acquirers around the world. We help online businesses and payment institutions optimize their payments and customer experience. | |

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

| | |
|--|--|
| Describe how the business stores, processes, and/or transmits account data. | Payment Services, Financial technology, and payment facilitation services |
| Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data. | Paysecure is an collection of intelligent global payment gateway and payments licences portfolio with integrations and partnerships with acquirers around the world. We help online businesses and payment institutions optimize their payments and customer experience. . |



Describe system components that could impact the security of account data.

Paysecure is an collection of intelligent global payment gateway and payments licences portfolio with integrations and partnerships with acquirers around the world. We help online businesses and payment institutions optimize their payments and customer experience.

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 Assesment covered the following areas of Paysecure application on AWS Cloud.

- 1:- Cloud Infrastructure components such as AWS involved in connections in into and out of CDE Environment.
- 2:- Card data flows such as E-Commerce
- 3:-Infrastructure servers including Web Application, Database etc.
- 4:- Security Solutions such as syslogs

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> |
| Corporate Office | 1 | Office 5.11, 25 Wilton Road, Victoria, London SW1V 1LW, |
| | | |
| | | |
| | | |
| | | |



**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 |
|---|--------------------------------|---|----------------------------------|------------------------|
| | | | | YYYY-MM-DD |
| | | | | YYYY-MM-DD |
| | | | | YYYY-MM-DD |
| | | | | YYYY-MM-DD |
| | | | | YYYY-MM-DD |
| | | | | YYYY-MM-DD |

* 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, 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:

- | | |
|---|---|
| <input type="checkbox"/> 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 type="checkbox"/> Yes <input checked="" type="checkbox"/> No |
| <input type="checkbox"/> 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 |
| <input type="checkbox"/> Could impact the security of the entity's CDE (for example, vendors providing support via remote access, and/or bespoke software developers). | <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No |

If Yes:

| Name of Service Provider: | Description of Services Provided: |
|---------------------------|-----------------------------------|
| Amazon Web Services | Cloud Hosting Service Provider |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

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



**Part 2g. Summary of Assessment
(ROC Section 1.8.1)**

Indicate below all responses provided within each principal PCI DSS requirement.

| 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 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"/> |



Section 2 Report on Compliance

(ROC Sections 1.2 and 1.3.2)

| | | |
|---|---|---|
| Date Assessment began: Note: This is the first date that evidence was gathered, or observations were made. | | 2023-12-07 |
| Date Assessment ended: Note: This is the last date that evidence was gathered, or observations were made. | | 2023-12-07 |
| 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 |
| <input type="checkbox"/> Examine documentation | <input checked="" type="checkbox"/> Yes | <input type="checkbox"/> No |
| <input type="checkbox"/> Interview personnel | <input checked="" type="checkbox"/> Yes | <input type="checkbox"/> No |
| <input type="checkbox"/> Examine/observe live data | <input checked="" type="checkbox"/> Yes | <input type="checkbox"/> No |
| <input type="checkbox"/> Observe process being performed | <input checked="" type="checkbox"/> Yes | <input type="checkbox"/> No |
| <input type="checkbox"/> Observe physical environment | <input checked="" type="checkbox"/> Yes | <input type="checkbox"/> No |
| <input type="checkbox"/> Interactive testing | <input checked="" type="checkbox"/> Yes | <input type="checkbox"/> No |
| <input type="checkbox"/> 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 *(Date of Report as noted in the ROC 2023-08-21)*.

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 PAYSECURE TECHNOLOGY LIMITED 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: 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>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;"> <thead> <tr> <th style="width: 30%;">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> </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 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 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

| | |
|---|------------------|
| Signature of Service Provider Executive Officer | Date: 2023-12-07 |
| Service Provider Executive Officer Name: Sridhar Sethuraman | Title: COO / CPO |

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: <small>29223C3766B74B8...</small> | |
| Signature of Lead QSA | Date: 2023-12-07 |
| Lead QSA Name: Sharwan Kumar | |
| DocuSigned by: <small>29223C3766B74B8...</small> | |
| Signature of Duly Authorized Officer of QSA Company | Date: 2023-12-07 |
| Duly Authorized Officer Name: Sharwan Kumar | QSA Company: Cybersigma Consulting Services |

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

