



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: Showpass

Date of Report as noted in the Report on Compliance: 2025.05.30

Date Assessment Ended: 2025.05.25

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: | Showpass |
| DBA (doing business as): | N/A |
| Company mailing address: | 3rd floor – 8500 Macleod Trail, Calgary, AB T2H 2N1 |
| Company main website: | https://www.showpass.com/ |
| Company contact name: | Lucas McCarthy |
| Company contact title: | CEO |
| Contact phone number: | ██████████ |
| Contact e-mail address: | ██████████ |

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): | N/A |
| Qualified Security Assessor | |
| Company name: | Secured Net Solutions Inc. |
| Company mailing address: | 1333 8 Street SW, Suite 1010, Calgary, AB, T2R 1M6 |
| Company website: | ██████████ |
| Lead Assessor name: | Steve Porter |
| Assessor phone number: | ██████████ |
| Assessor e-mail address: | ██████████ |
| Assessor certificate number: | QSA (#202-991) QPA (#1300-215) |

SSLCA (#1600-127)
SSA (#1500-126)

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: E-commerce

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):

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: N/A

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:

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.

The entity does not store, process, or transmit cardholder data.

Entity is a web-based event ticket seller, providing their clients with a platform to an e-commerce site hosted on the [REDACTED]. This e-commerce website is integrated with an i-frame using third-party payment processors [REDACTED] [REDACTED] [REDACTED].

The entity sometimes uses PCI SSC validated POI [REDACTED] terminals.

Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.

N/A

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

 services

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.*

Showpass is a web-based event ticket seller, providing clients with access to an e-commerce site hosted on the [REDACTED]

Showpass's website integrates third-party payment processors using an i-frame [REDACTED] Swuare, [REDACTED]

There are no wireless access points within this entity's CDE.

There is no storage, processing, or transmission of cardholder data within the entity's environment.

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 | 3rd Floor - 8500 Macleod Trail, Calgary, AB T2H 2N1 |
| [REDACTED] | 1 | US-WEST1 |
| | | |
| | | |
| | | |
| | | |

Part 2. Executive Summary *(continued)*

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

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

| | |
|--|---|
| <ul style="list-style-type: none"> Store, process, or transmit account data on the entity's behalf (for example, payment gateways, payment processors, payment service providers (PSPs, and off-site storage)) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| <ul style="list-style-type: none"> Manage system components included in the entity's Assessment (for example, via network security control services, anti-malware services, security incident and event management (SIEM), contact and call centers, web-hosting companies, and IaaS, PaaS, SaaS, and FaaS cloud providers) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| <ul style="list-style-type: none"> Could impact the security of the entity's CDE (for example, vendors providing support via remote access, and/or bespoke software developers). | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |

If Yes:

| Name of Service Provider: | Description of Services Provided: |
|---------------------------|---|
| ██████████ | Logging and alerting |
| ██████ | i-Frame redirect to payment processor |
| ██████████████████ | Cloud infrastructure services |
| ██████████ | End-user support ticketing system |
| ██████████ | i-Frame redirect to payment processor |
| ██████ | i-Frame redirect to payment processor and approved tap services |
| | |
| | |
| | |

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: E-Commerce

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

Justification for Approach

| | |
|--|--|
| <p>For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.</p> | <p>Entity does not use insecure protocols: 1.2.6 Entity does not store, transmit, or process CHD: 1.4.4, 3.2-3.6.1, 3.6.1.2, 3.7.1-3, 4.2.2, 6.5.5, 7.2.6, 9.4.1, 9.4.1.1, 9.4, 10.2.1.1 Entity does not send PAN over open, public, networks: 4.2.1, 4.2.1.1 Responsibility of █████ 1.2.8, 1.4.3, 9.2, 9.3.1, 9.3.2, 9.3.3, 9.3.4 Entity does not have wireless traffic that connects to the CDE: 1.3.3, 2.3.1, 2.3.2, 4.2.1.2 Entity is not an issuer: 3.3.3 Entity does not use cleartext key components: 3.6.1.3, 3.7.6 Entity does not use system or application accounts interactively: 8.6.1, 8.6.2. Entity does not have any third-party access into the CDE: 8.2.7. Entity does not use password only authentication: 8.3.9 Entity does not use shared accounts: 8.2.2. Entity does not use periodical flexibility in any requirements or TRA: 12.3.1 Entity does not meet any requirements with the customized approach: 12.3.2 Entity does not share cryptographic keys with its customers and does not store account data: 3.7.9 Entity does not have components not at risk for malware: 5.2.3, 5.2.3.1 Entity does not perform periodic malware scans: 5.3.2.1 Superseded: 6.4.1, 8.3.10, 10.7.1 Entity does not allow remote access for third-parties: 8.2.7 Entity is not a multi-tenant service provider: 11.4.7, A1 Entity does not use SSL and/or early TLS: A2 A3: Not required</p> |
| <p>For any Not Tested responses, identify which sub-requirements were not tested and the reason.</p> | <p>N/A</p> |

Section 2 Report on Compliance

(ROC Sections 1.2 and 1.3)

| | |
|---|---|
| Date Assessment began: Note: <i>This is the first date that evidence was gathered, or observations were made.</i> | 2025-04-01 |
| Date Assessment ended: Note: <i>This is the last date that evidence was gathered, or observations were made.</i> | 2025-05-25 |
| Were any requirements in the ROC unable to be met due to a legal constraint? | <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No |
| Were any testing activities performed remotely? | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |

Section 3 Validation and Attestation Details

Part 3. PCI DSS Validation (ROC Section 1.7)

This AOC is based on results noted in the ROC dated *(Date of Report as noted in the ROC 2025-05-30)*.

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 Showpass 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; 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

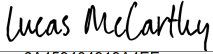
Signatory(s) confirms:

(Select all that apply)

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

Part 3b. Service Provider Attestation

Signed by:

| | | |
|--|--|------------------|
|  <small>6A459404919A4EE...</small> <i>Signature of Service Provider Executive Officer</i> ↑ | | Date: 2025-05-30 |
| Service Provider Executive Officer Name: Lucas McCarthy | | Title: CEO |

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>545F1F4A0CF146A...</small> <i>Signature of Lead QSA</i> ↑ | | Date: 2025-05-30 |
| Lead QSA Name: Steve Porter | | |

DocuSigned by:

| | | |
|--|--|---|
|  <small>545F1F4A0CF146A...</small> <i>Signature of Duly [Redacted] Officer of QSA Company</i> ↑ | | Date: 2025-05-30 |
| Duly [Redacted] Officer Name: Steve Porter | | QSA Company: Secured Net Solutions Inc. |

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"/> | |

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: