# Payment Card Industry (PCI)
# Data Security Standard

## Attestation of Compliance for
## Onsite Assessments – Service Providers

**Version 3.2.1**

June 2018

# Section 1: Assessment Information

## Instructions for Submission

This Attestation of Compliance must be completed as a declaration of the results of the service provider's assessment with the *Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS)*. Complete all sections: The service provider is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the requesting payment brand for reporting and submission procedures.

### Part 1. Service Provider and Qualified Security Assessor Information

#### Part 1a. Service Provider Organization Information

| | | | |
|---|---|---|---|
| Company Name: | Detroit Labs | DBA (doing business as): | Detroit Labs Cloud Platform Team |
| Contact Name: | Bryan Kelly | Title: | Lead Product Architect |
| Telephone: | 734-673-2760 | E-mail: | bryan@detroitlabs.com |
| Business Address: | 1520 Woodward Ave., Ste. 600 | City: | Detroit |
| State/Province: | Michigan | Country: US | Zip: 48226 |
| URL: | https://www.detroitlabs.com | | |

#### Part 1b. Qualified Security Assessor Company Information (if applicable)

| | | | |
|---|---|---|---|
| Company Name: | Structured Communication Systems, Inc | | |
| Lead QSA Contact Name: | Joe Bono | Title: | QSA |
| Telephone: | 503-513-4594 | E-mail: | |
| Business Address: | 12901 SE 97th Ave Suite 400 | City: | Clackmas |
| State/Province: | Oregon | Country: US | Zip: 97015 |
| URL: | www.structured.com | | |

## Part 2. Executive Summary

### Part 2a. Scope Verification

### Services that were INCLUDED in the scope of the PCI DSS Assessment (check all that apply):

| Name of service(s) assessed: | E-Commerce |
|---|---|

Type of service(s) assessed:

| **Hosting Provider:** | **Managed Services (specify):** | **Payment Processing:** |
|---|---|---|
| ☐ Applications / software | ☐ Systems security services | ☐ POS / 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 | | |
| ☐ Security services | | |
| ☐ 3-D Secure Hosting Provider | | |
| ☒ Shared Hosting 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):

*Note*: These categories are provided for assistance only, and are not intended to limit or predetermine an entity's service description. If you feel these categories don't apply to your service, complete "Others." If you're unsure whether a category could apply to your service, consult with the applicable payment brand.

| **Part 2a. Scope Verification** *(continued)* |
|---|

| **Services that are provided by the service provider but were NOT INCLUDED in the scope of the PCI DSS Assessment** (check all that apply): |
|---|

| Name of service(s) not assessed: | Non-PCI web application development. |
|---|---|

Type of service(s) not assessed:

| **Hosting Provider:** | **Managed Services (specify):** | **Payment Processing:** |
|---|---|---|
| ☒ Applications / software | ☐ Systems security services | ☐ POS / 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 | | |
| ☐ Security services | | |
| ☐ 3-D Secure Hosting Provider | | |
| ☐ Shared Hosting 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: | |

| **Part 2b. Description of Payment Card Business** |
|---|

| Describe how and in what capacity your business stores, processes, and/or transmits cardholder data. | Detroit Lab does not store, process and/or transmit cardholder data. Detroit Lab works within the Google Cloud Platform and administers the Kubernetes Cluster. All cardholder data is managed within and by Google controlled Key Management Services. |
|---|---|
| Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data. | Detroit Labs does not have direct access to cardholder data. GCP is the provider of security and access services for cardholder data. |

| **Part 2c. Locations** |
|---|

List types of facilities (for example, retail outlets, corporate offices, data centers, call centers, etc.) and a summary of locations included in the PCI DSS review.

| **Type of facility:** | **Number of facilities of this type** | **Location(s) of facility (city, country):** |
|---|---|---|
| *Example: Retail outlets* | *3* | *Boston, MA, USA* |
| HQ Detroit Labs Office | 1 | Detroit, Michigan |

| | | |
|---|---|---|
| | | |
| | | |
| | | |
| | | |

## Part 2d. Payment Applications

Does the organization use one or more Payment Applications?  ☒ Yes  ☐ No

Provide the following information regarding the Payment Applications your organization uses:

| Payment Application Name | Version Number | Application Vendor | Is application PA-DSS Listed? | PA-DSS Listing Expiry date (if applicable) |
|---|---|---|---|---|
| Olo  Inc. | 3.2.1 | | ☒ Yes  ☐ No | 1/21/2022 |
| Google Cloud Platform | | | ☐ Yes  ☒ No | |
| | | | ☐ Yes  ☐ No | |
| | | | ☐ Yes  ☐ No | |
| | | | ☐ Yes  ☐ No | |
| | | | ☐ Yes  ☐ No | |
| | | | ☐ Yes  ☐ No | |
| | | | ☐ Yes  ☐ No | |
| | | | ☐ Yes  ☐ No | |

## Part 2e. Description of Environment

| Provide a **_high-level_** description of the environment covered by this assessment. *For example:* <br> • *Connections into and out of the cardholder data environment (CDE).* <br> • *Critical system components within the CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.* | The card holder data (CHD) flow is entered by the customers who have access to the client's specific merchant website. This access is controlled by Google utilizing the Cloud Armor and the Kubernetes cluster in the cloud platform and the Labs Cloud Platform Team working in the GCP Strapi CMA for brand settings that communicates with the backend and frontend. All card data is encrypted and decrypted by the Google key management service and stored in the Redis/Cloud Memory store for temporary storage (15 minutes of inactivity and up to fours) and MySQL DB, for the duration period the customer determines. |
|---|---|

| Does your business use network segmentation to affect the scope of your PCI DSS environment? <br> *(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation)* | ☒ Yes  ☐ No |
|---|---|

| Part 2f. Third-Party Service Providers | | |
|---|---|---|
| Does your company have a relationship with a Qualified Integrator & Reseller (QIR) for the purpose of the services being validated? | ☐ Yes | ☒ No |

| If Yes: | |
|---|---|
| Name of QIR Company: | |
| QIR Individual Name: | |
| Description of services provided by QIR: | |

| Does your company have a relationship with one or more third-party service providers (for example, Qualified Integrator Resellers (QIR), gateways, payment processors, payment service providers (PSP), web-hosting companies, airline booking agents, loyalty program agents, etc.) for the purpose of the services being validated? | ☒ Yes ☐ No |
|---|---|

*If Yes:*

| Name of service provider: | Description of services provided: |
|---|---|
| Olo Inc. | Olo provides an eCommerce-based ordering platform. |
| Google Cloud Platform | Google Coud Platform provides an eCommerce-based ordering platform. |
| | |
| | |
| | |
| | |

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

**Part 2g. Summary of Requirements Tested**

For each PCI DSS Requirement, select one of the following:

- **Full** – The requirement and all sub-requirements of that requirement were assessed, and no sub-requirements were marked as "Not Tested" or "Not Applicable" in the ROC.
- **Partial** – One or more sub-requirements of that requirement were marked as "Not Tested" or "Not Applicable" in the ROC.
- **None** – All sub-requirements of that requirement were marked as "Not Tested" and/or "Not Applicable" in the ROC.

For all requirements identified as either "Partial" or "None," provide details in the "Justification for Approach" column, including:

- Details of specific sub-requirements that were marked as either "Not Tested" and/or "Not Applicable" in the ROC
- Reason why sub-requirement(s) were not tested or not applicable

*Note:* *One table to be completed for each service covered by this AOC. Additional copies of this section are available on the PCI SSC website.*

| Name of Service Assessed: | E-Commerce |
|---|---|

| PCI DSS Requirement | Details of Requirements Assessed | | | |
|---|---|---|---|---|
| | **Full** | **Partial** | **None** | **Justification for Approach** (Required for all "Partial" and "None" responses. Identify which sub-requirements were not tested and the reason.) |
| Requirement 1: | ☐ | ☒ | ☐ | Not applicable due to Detroit Labs utilizes Octocart, Googles Cloud Armor  WAF (web application firewall) for all ingress traffic into the cardholder data environment. The firewall requirements are covered by GCP which is covered as a third-party service provider with an included AOC. : Sections that are N/A:1.1, 1.2, 1.3, 1.4 |
| Requirement 2: | ☐ | ☒ | ☐ | There are no default passwords as Detroit Labs employees log into the google G suite product, using dual auth, Multi Factor Authentication. <br><br> There are no vendor-supplied defaults. Sections that are N/A : 2.1, 2.2, |
| Requirement 3: | ☐ | ☒ | ☐ | Protect stored cardholder data requirements are covered by GCP which is covered as a third-party service provider with an included AOC. Sections that are N/A: 3.2, 3.3, 3.4, 3.5, 3.6, |
| Requirement 4: | ☐ | ☒ | ☐ | Google Cloud Platform manages all encryption and decryption of card holder data in transits and at rest. Requirements are covered by GCP which is covered as a third-party service provider with an included AOC. Sections that are N/A: 4.1, 4.2, |
| Requirement 5: | ☐ | ☒ | ☐ | Protect all systems against malware and regularly update anti-virus software or programs is managed |

| | | | | |
|---|---|---|---|---|
| | ☐ | ☐ | ☐ | by Google Cloud Platform: Sections that are N/A: 5.1, 5.2, 5.3, |
| Requirement 6: | ☐ | ☒ | ☐ | Google is responsible for protecting the systems and infrastructure underlying GCP from vulnerabilities in compliance with the requirements in section 6. Sections that are N/A : 6.2, 6.3.1, 6.4.16.4.3, 6.4.6, |
| Requirement 7: | ☒ | ☐ | ☐ | |
| Requirement 8: | ☐ | ☒ | ☐ | There are no IDs used by third parties to access CHD: Sections that are N/A: 8.1.5, 8.2.1, 8.2.2, |
| Requirement 9: | ☐ | ☐ | ☒ | Detroit Lab does not have any physical office infrastructure or data centers in scope other than Google Cloud Platform, All sections are N/A |
| Requirement 10: | ☐ | ☒ | ☐ | NTP for the Google Cloud Platform is managed by Google: Sections that are N/A : 10.4, 10.5.1, 10.5.2, - 10.5.5, 10.8.1 |
| Requirement 11: | ☐ | ☒ | ☐ | Not applicable due to wireless in the office is to a service provider to the internet and other employees' access to the GCP is from their home office and direct through their service provider to the internet: Sections that are N/A : 11.1, 11.2.1, 11.5.a-.b, |
| Requirement 12: | ☐ | ☒ | ☐ | There is no remote-access technology in use for vendors and business partners: Sections 12.3.9, N/A, There is no previously reported incidents or alerts Sections 12.10.1.b - 12.11.b are all N/A |
| Appendix A1: | ☐ | ☒ | ☐ | Hosting provider does not allow hosted entities to run their own applications: Sections that are N/A : A1.1, A.1.2, A.1.3, |
| Appendix A2: | ☐ | ☐ | ☐ | No POS terminals are in use |

# Section 2: Report on Compliance

This Attestation of Compliance reflects the results of an onsite assessment, which is documented in an accompanying Report on Compliance (ROC).

| The assessment documented in this attestation and in the ROC was completed on: | 12 April 2022 | |
|---|---|---|
| Have compensating controls been used to meet any requirement in the ROC? | ☐ Yes | ☒ No |
| Were any requirements in the ROC identified as being not applicable (N/A)? | ☒ Yes | ☐ No |
| Were any requirements not tested? | ☐ Yes | ☒ No |
| Were any requirements in the ROC unable to be met due to a legal constraint? | ☐ Yes | ☒ No |

# Section 3: Validation and Attestation Details

## Part 3. PCI DSS Validation

**This AOC is based on results noted in the ROC dated** 12 April 2022*.*

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

| | |
|---|---|
| ☒ | **Compliant:** All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby Detroit Labs has demonstrated full compliance with the PCI DSS. |
| ☐ | **Non-Compliant:** Not all sections of the PCI DSS ROC are complete, or not all questions are answered affirmatively, resulting in an overall **NON-COMPLIANT** rating, thereby *(Service Provider Company Name)* has not demonstrated full compliance with the PCI DSS.<br><br>**Target Date** for Compliance:<br><br>An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. *Check with the payment brand(s) before completing Part 4.* |
| ☐ | **Compliant but with Legal exception:** One or more requirements are marked "Not in Place" due to a legal restriction that prevents the requirement from being met. This option requires additional review from acquirer or payment brand.<br><br>*If checked, complete the following:* |

| Affected Requirement | Details of how legal constraint prevents requirement being met |
|---|---|
| | |
| | |

## Part 3a. Acknowledgement of Status

**Signatory(s) confirms:**

*(Check all that apply)*

| | |
|---|---|
| ☒ | The ROC was completed according to the *PCI DSS Requirements and Security Assessment Procedures*, Version 3.2.1, and was completed according to the instructions therein. |
| ☒ | All information within the above-referenced ROC and in this attestation fairly represents the results of my assessment in all material respects. |
| ☒ | I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization. |
| ☒ | I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times. |
| ☒ | If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply. |

| **Part 3a. Acknowledgement of Status** (continued) | |
|:---:|:---|
| ☒ | No evidence of full track data[1], CAV2, CVC2, CID, or CVV2 data[2], or PIN data[3] storage after transaction authorization was found on ANY system reviewed during this assessment. |
| ☒ | ASV scans are being completed by the PCI SSC Approved Scanning Vendor Qualys |

| **Part 3b. Service Provider Attestation** |
|:---|

| | |
|:---|:---|
| *Signature of Service Provider Executive Officer* ↑ | *Date:* |
| *Service Provider Executive Officer Name:* | *Title:* |

| **Part 3c. Qualified Security Assessor (QSA) Acknowledgement (if applicable)** | |
|:---|:---|
| If a QSA was involved or assisted with this assessment, describe the role performed: | Performed a full PCI assessment with Report on Compliance. |

*Robert Wayt*

| | |
|:---|:---|
| *Signature of Duly Authorized Officer of QSA Company* ↑ | *Date:* 12 April 2022 |
| *Duly Authorized Officer Name:* Robert Wayt | *QSA Company:* Structured Communication Systems |

| **Part 3d. Internal Security Assessor (ISA) Involvement (if applicable)** | |
|:---|:---|
| If an ISA(s) was involved or assisted with this assessment, identify the ISA personnel and describe the role performed: | |

---

[1] Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full track data after transaction authorization. The only elements of track data that may be retained are primary account number (PAN), expiration date, and cardholder name.

[2] The three- or four-digit value printed by the signature panel or on the face of a payment card used to verify card-not-present transactions.

[3] Personal identification number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.

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

Select the appropriate response for "Compliant to PCI DSS Requirements" for each requirement. If you answer "No" to any of the requirements, you may be required to provide the date your Company expects to be compliant with the requirement and a brief description of the actions being taken to meet the requirement.

*Check with the applicable payment brand(s) before completing Part 4.*

| PCI DSS Requirement | Description of Requirement | Compliant to PCI DSS Requirements *(Select One)* | | Remediation Date and Actions (If "NO" selected for any Requirement) |
|---|---|---|---|---|
| | | **YES** | **NO** | |
| 1 | Install and maintain a firewall configuration to protect cardholder data | ☒ | ☐ | |
| 2 | Do not use vendor-supplied defaults for system passwords and other security parameters | ☒ | ☐ | |
| 3 | Protect stored cardholder data | ☒ | ☐ | |
| 4 | Encrypt transmission of cardholder data across open, public networks | ☒ | ☐ | |
| 5 | Protect all systems against malware and regularly update anti-virus software or programs | ☒ | ☐ | |
| 6 | Develop and maintain secure systems and applications | ☒ | ☐ | |
| 7 | Restrict access to cardholder data by business need to know | ☒ | ☐ | |
| 8 | Identify and authenticate access to system components | ☒ | ☐ | |
| 9 | Restrict physical access to cardholder data | ☒ | ☐ | |
| 10 | Track and monitor all access to network resources and cardholder data | ☒ | ☐ | |
| 11 | Regularly test security systems and processes | ☒ | ☐ | |
| 12 | Maintain a policy that addresses information security for all personnel | ☒ | ☐ | |
| Appendix A1 | Additional PCI DSS Requirements for Shared Hosting Providers | ☒ | ☐ | |
| Appendix A2 | Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections | ☐ | ☐ | |