# 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: | Cantaloupe, Inc | | DBA (doing business as): | N/A | |
| Contact Name: | Art Royce | | Title: | Sr Dir Compliance | |
| Telephone: | +1.484.324.1820 | | E-mail: | aroyce@cantaloupe.com | |
| Business Address: | 100 Deerfield, Suite #300 | | City: | Malvern | |
| State/Province: | PA | Country: | USA | Zip: | 19355 |
| URL: | Https://cantaloupe.com | | | | |

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

| | | | | | |
|---|---|---|---|---|---|
| Company Name: | Truvantis, Inc | | | | |
| Lead QSA Contact Name: | Dick Hacking | | Title: | Principal Security Analyst | |
| Telephone: | +1.415.422.9826 | | E-mail: | dick.hacking@truvantis.com | |
| Business Address: | 548 Market Street | | City: | San Francisco | |
| State/Province: | CA | Country: | USA | Zip: | 94104 |
| URL: | www.truvantis.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: | Seed, ePort, USALive, Getmore | |
| Type of service(s) assessed: | | |
| **Hosting Provider:**<br>□ Applications / software<br>□ Hardware<br>□ Infrastructure / Network<br>□ Physical space (co-location)<br>□ Storage<br>□ Web<br>□ Security services<br>□ 3-D Secure Hosting Provider<br>□ Shared Hosting Provider<br>□ Other Hosting (specify): | **Managed Services (specify):**<br>□ Systems security services<br>□ IT support<br>□ Physical security<br>□ Terminal Management System<br>□ Other services (specify): | **Payment Processing:**<br>☒ POS / card present<br>☒ Internet / e-commerce<br>☒ MOTO / Call Center<br>□ ATM<br>□ 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 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: | None |

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. | Entity primarily designs and sells PCI card reader devices for retrofitting into vending machines, unattended sales kiosks, gas station forecourt vacuum and air devices (but not the gas pumps themselves), and electric vehicle (EV) charging stations. They also create and maintain the software infrastructure and websites to accept CHD from those readers as payment for the various services. Entity also has its own BIN range for a non-branded pre-paid (affinity) card the pre-payment for which is effected through a website called "getmore.com" using a credit card. |
| Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data. | Entity also develops all the software used from the card reader to the mobile phone modem. |

## 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 | 1 | Malvern, PA, USA |

## 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) |
|---|---|---|---|---|
| None | N/A | N/A | □ Yes □ No | N/A |

## Part 2e. Description of Environment

| | |
|---|---|
| Provide a ***high-level*** description of the environment covered by this assessment.<br>*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.* | Entity has merged two different environments into a single ROC, even as the environments are implemented in different hosting paradigms. They are also undergoing a corporate name change and some of the evidence collected for this ROC does not yet reflect the changes, however it is all current and up to date in every other respect.<br>There are two similar but separate implementations which utilize a common set of policies and procedure documentation. The implementation is hosted by Rackspace for the "Seed" product, and by Oracle Cloud Infrastructure for the "ePort" and "Getmore" products. Where necessary the reports show the differences |
| 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: | None |
| QIR Individual Name: | N/A |
| Description of services provided by QIR: | N/A |

| | |
|---|---|
| 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:** |
|---|---|
| Oracle Cloud Infrastructure | Data center services, processing, and storage. |
| Rackspace | Data center services, processing, and storage. |
| AlertLogic | Log data preservation, monitoring, alerting. |
| Docusign | CHD transmission into the sales pipeline and then discarded. |
| Tier Point | Legacy data center (all CHD storage and processing was moved OCI), |
| Stericycle | Media destruction. |

***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:** | ePort, Seed, USALive, Getmore |

| **PCI DSS Requirement** | **Details of Requirements Assessed** | | | |
|---|---|---|---|---|
| | **Full** | **Partial** | **None** | **Justification for Approach**<br>(Required for all "Partial" and "None" responses. Identify which sub-requirements were not tested and the reason.) |
| Requirement 1: | ☒ | □ | □ | |
| Requirement 2: | □ | ☒ | □ | 2.2.3 - N/A no insecure protocols or services are implemented.<br>2.6 - N/A Entity is not a shared hosting provider. |
| Requirement 3: | □ | ☒ | □ | 3.4.1 Full disk encryption is not used. |
| Requirement 4: | ☒ | □ | □ | |
| Requirement 5: | ☒ | □ | □ | |
| Requirement 6: | ☒ | □ | □ | |
| Requirement 7: | ☒ | □ | □ | |
| Requirement 8: | □ | ☒ | □ | 8.1.5 - N/A No third parties are given access to the computing facilities.<br>8.5.1 - N/A Entity has no access to its customers premises. |
| Requirement 9: | □ | ☒ | □ | 9.1.2 - N/A Entity is implemented in co-location data centers, no publicly accessible jacks exist.<br>9.8.1 - N/A No printed or other hard-copy materials can be created containing full PAN since it is never stored. |

| | | | | |
|---|---|---|---|---|
| | | | | 9.9 - N/A The security of the card readers themselves is the responsibility of their owner/operators per the contract they have with Entity. |
| Requirement 10: | ☒ | □ | □ | |
| Requirement 11: | □ | ☒ | □ | 11.2 - N/A No wireless can exist in the co-lo data centers. |
| Requirement 12: | ☒ | □ | □ | |
| Appendix A1: | □ | □ | ☒ | Not applicable. Entity is not a shared hosting provider. |
| Appendix A2: | □ | □ | ☒ | Not applicable. Entity does not use SSL v3 or early TLS. |

## 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: | 9/25/2021 | |
| 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** 9/25/2021**.**

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 Cantaloupe, Inc 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>**Target Date** for Compliance:<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>*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 Tenable and Qualys |

## Part 3b. Service Provider Attestation

Paul Hamman

| | |
|---|---|
| *Signature of Service Provider Executive Officer* ↑ | *Date:* 10/04/2021 |
| *Service Provider Executive Officer Name:* | *Title:* Chief Information Security Officer |

## Part 3c. Qualified Security Assessor (QSA) Acknowledgement (if applicable)

| | |
|---|---|
| If a QSA was involved or assisted with this assessment, describe the role performed: | Full assessment according to the PCI DSS standard v3.2.1 for each product in the two data centers in which they are implemented. |

ACottrell

| | |
|---|---|
| *Signature of Duly Authorized Officer of QSA Company* ↑ | *Date:* 10/4/2021 |
| *Duly Authorized Officer Name:* Andy Cottrell | *QSA Company:* Truvantis, Inc |

## 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: | None |

[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 | □ | ☒ | Not Applicable |
| Appendix A2 | Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections | □ | ☒ | Not Applicable |