



# **Payment Card Industry (PCI) Data Security Standard**

Redistribution of this document is not permitted without the express written consent of Comprise Technologies, Inc. which reserves all rights to this document and the information contained therein.

---

## **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:	Comprise Technologies, Inc.	DBA (doing business as):	
Contact Name:	Christopher Hayes	Title:	Compliance Officer
Telephone:	+1-800-531-0132	E-mail:	<a href="mailto:chayes@comprisetechologies.com">chayes@comprisetechologies.com</a>
Business Address:	Corporate Office, 1041 Route 36	City:	Navesink
State/Province:	NJ	Country:	USA
URL:	<a href="http://www.comprisetechologies.com/">http://www.comprisetechologies.com/</a>		

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

Company Name:	ControlCase LLC		
Lead QSA Contact Name:	Faisal Bawani	Title:	PCI QSA
Telephone:	+1 703.483.6383	E-mail:	<a href="mailto:fbawani@controlcase.com">fbawani@controlcase.com</a>
Business Address:	12015 Lee Jackson Memorial Hwy, Suite 520	City:	Fairfax
State/Province:	VA	Country:	USA
URL:	<a href="https://www.controlcase.com/">https://www.controlcase.com/</a>		

## Section 3: Validation and Attestation Details

### Part 3. PCI DSS Validation

This AOC is based on results noted in the ROC dated March 15, 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 *Comprise Technologies, 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.
- Target Date** for Compliance:
- 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.
- 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)

<input checked="" type="checkbox"/>	No evidence of full track data <sup>1</sup> , CAV2, CVC2, CID, or CVV2 data <sup>2</sup> , or PIN data <sup>3</sup> storage after transaction authorization was found on ANY system reviewed during this assessment.
<input checked="" type="checkbox"/>	ASV scans are being completed by the PCI SSC Approved Scanning Vendor <b>ControlCase LLC</b> .

### Part 3b. Service Provider Attestation



Signature of Service Provider Executive Officer ↑	Date: <b>March 15, 2021</b>
Service Provider Executive Officer Name: <b>Christopher Hayes</b>	Title: <b>Compliance Officer</b>

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

If a QSA was involved or assisted with this assessment, describe the role performed:	The QSA performed the assessment against the PCI DSS 3.2.1 standard at the assessed entity and documented the findings in the report on compliance.
--	---



Signature of Duly Authorized Officer of QSA Company ↑	Date: <b>March 15, 2021</b>
Duly Authorized Officer Name: <b>Faisal Bawani</b>	QSA Company: <b>ControlCase LLC</b>

### 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:	<p>Christopher Hayes - The Compliance Officer who is responsible for running the PCI DSS Compliance Program.</p> <p>Justin Spaeth - The Network Administrator who is responsible for the Network Security Controls.</p>
---	---

<sup>1</sup> 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.

<sup>2</sup> 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.

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