



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

---

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

**Version 3.2.1**

June 2018

**Part 3a. Acknowledgement of Status (continued)**

- 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.
- ASV scans are being completed by the PCI SSC Approved Scanning Vendor Clone Systems, Inc.

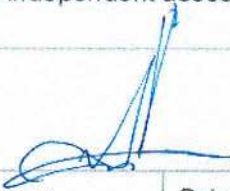
**Part 3b. Service Provider Attestation**



Signature of Service Provider Executive Officer ↑	Date: 25, February 2021
Service Provider Executive Officer Name: Andrey Zinoviev	Title: Director

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

If a QSA was involved or assisted with this assessment, describe the role performed:	QSA independent assessment
--	----------------------------



Signature of Duly Authorized Officer of QSA Company ↑	Date: 25, February 2021
Duly Authorized Officer Name: Andrey Konyahin	QSA Company: Compliance Control Ltd.

**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:	Not applicable
---	----------------

<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.