

Attestation of Compliance, SAQ D—Service Provider Version

Instructions for Submission

The service provider must complete this Attestation of Compliance as a declaration of the service provider's compliance status with the *Payment Card Industry Data Security Standard (PCI DSS) Requirements and Security Assessment Procedures*. Complete all applicable sections and refer to the submission instructions at "PCI DSS Compliance – Completion Steps" in this document.

Part 1. Service Provider and Qualified Security Assessor Information

Part 1a. Service Provider Organization Information

| | | | | | |
|-------------------|------------------------|----------|--------------------------|------|-------|
| Company Name: | 911 Software, INC | DBA(s): | | | |
| Contact Name: | Zorrik Voldman | Title: | President | | |
| Telephone: | 561-392-9606 x 701 | E-mail: | zvoldman@911software.com | | |
| Business Address: | 265 S Federal HWY #353 | City: | Deerfield Beach | | |
| State/Province: | FL | Country: | USA | Zip: | 33441 |
| URL: | http://911software.com | | | | |

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

| | | | | | |
|------------------------|--------------------|----------|------------------|------|--|
| Company Name: | 403 Labs, INC | | | | |
| Lead QSA Contact Name: | Kevin Eaton | Title: | Lead QSA rep | | |
| Telephone: | 877-403-5227 | E-mail: | info@403labs.com | | |
| Business Address: | | City: | | | |
| State/Province: | | Country: | | Zip: | |
| URL: | http://403Labs.com | | | | |

Part 2. PCI DSS Assessment Information

Part 2a. Services Provided that WERE INCLUDED in the Scope of the PCI DSS Assessment (check all that apply)

| | | |
|--|---|---|
| <input type="checkbox"/> 3-D Secure Hosting Provider | <input type="checkbox"/> Hosting Provider – Hardware | <input type="checkbox"/> Payment Processing – ATM |
| <input type="checkbox"/> Account Management | <input type="checkbox"/> Hosting Provider – Web | <input checked="" type="checkbox"/> Payment Processing – MOTO |
| <input type="checkbox"/> Authorization | <input type="checkbox"/> Issuer Processing | <input type="checkbox"/> Payment Processing – Internet |
| <input type="checkbox"/> Back Office Services | <input type="checkbox"/> Loyalty Programs | <input checked="" type="checkbox"/> Payment Processing – POS |
| <input type="checkbox"/> Billing Management | <input type="checkbox"/> Managed Services | <input type="checkbox"/> Prepaid Services |
| <input type="checkbox"/> Clearing and Settlement | <input type="checkbox"/> Merchant Services | <input type="checkbox"/> Records Management |
| <input type="checkbox"/> Data Preparation | <input type="checkbox"/> Network Provider/Transmitter | <input type="checkbox"/> Tax/Government Payments |
| <input type="checkbox"/> Fraud and Chargeback Services | <input type="checkbox"/> Payment Gateway/Switch | |
| <input type="checkbox"/> Others (please specify): | | |

List facilities and locations included in PCI DSS review: N/A

Part 2b. If any services listed are provided by the service provider but *WERE NOT INCLUDED* in the Scope of the PCI DSS Assessment, please check them below:

- | | | |
|--|---|--|
| <input type="checkbox"/> 3-D Secure Hosting Provider | <input type="checkbox"/> Hosting Provider – Hardware | <input type="checkbox"/> Payment Processing – ATM |
| <input type="checkbox"/> Account Management | <input type="checkbox"/> Hosting Provider – Web | <input type="checkbox"/> Payment Processing – MOTO |
| <input type="checkbox"/> Authorization | <input type="checkbox"/> Issuer Processing | <input type="checkbox"/> Payment Processing – Internet |
| <input type="checkbox"/> Back Office Services | <input type="checkbox"/> Loyalty Programs | <input type="checkbox"/> Payment Processing – POS |
| <input type="checkbox"/> Billing Management | <input type="checkbox"/> Managed Services | <input type="checkbox"/> Prepaid Services |
| <input type="checkbox"/> Clearing and Settlement | <input type="checkbox"/> Merchant Services | <input type="checkbox"/> Records Management |
| <input type="checkbox"/> Data Preparation | <input type="checkbox"/> Network Provider/Transmitter | <input type="checkbox"/> Tax/Government Payments |
| <input type="checkbox"/> Fraud and Chargeback Services | <input type="checkbox"/> Payment Gateway/Switch | |
| <input type="checkbox"/> Others (please specify): | | |

Part 2c. Relationships

Does your company have a relationship with one or more third-party service providers (for example, gateways, web-hosting companies, airline booking agents, loyalty program agents, etc.)? ☐ Yes ☒ No

Part 2d. Transaction Processing

How and in what capacity does your business store, process and/or transmit cardholder data? N/A - Software module sold to others

| <u>Payment Application in Use</u> | <u>Version Number</u> | <u>Last Validated according to PABP/PA-DSS</u> |
|-----------------------------------|-----------------------|--|
| CreditLine | 4.1 | 04/12 |
| | | |

Please provide the following information regarding the Payment Applications your organization uses:

Part 3. PCI DSS Validation

Based on the results noted in the SAQ D dated (*completion date of SAQ*), (*Service Provider Company Name*) asserts the following compliance status (check one):

☒ **Compliant:** All sections of the PCI SAQ are complete, and all questions answered “yes”, resulting in an overall **COMPLIANT** rating; **and** a passing scan has been completed by a PCI SSC Approved Scanning Vendor (ASV), thereby (*Service Provider Company Name*) has demonstrated full compliance with the PCI DSS.

☐ **Non-Compliant:** Not all sections of the PCI SAQ are complete, or some questions are answered “no”, resulting in an overall **NON-COMPLIANT** rating, **or** a passing scan has not been completed by a PCI SSC Approved Scanning Vendor (ASV), thereby (*Service Provider Company Name*) has not demonstrated full compliance with the PCI DSS.

Target Date for Compliance:

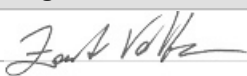
An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. *Check with your acquirer or the payment brand(s) before completing Part 4, since not all payment brands require this section.*

Part 3a. Confirmation of Compliant Status

Service Provider confirms:

| | |
|-------------------------------------|--|
| <input checked="" type="checkbox"/> | Self-Assessment Questionnaire D, Version 2, was completed according to the instructions therein. |
| <input checked="" type="checkbox"/> | All information within the above-referenced SAQ and in this attestation fairly represents the results of my assessment. |
| <input checked="" type="checkbox"/> | I have read the PCI DSS and I recognize that I must maintain full PCI DSS compliance at all times. |
| <input checked="" type="checkbox"/> | No evidence of magnetic stripe (i.e., track) data ⁵ , CAV2, CVC2, CID, or CVV2 data ⁶ , or PIN data ⁷ storage after transaction authorization was found on ANY systems reviewed during this assessment. |

Part 3b. Service Provider Acknowledgement

| | |
|---|------------|
|  | 08/14/2012 |
| Signature of Service Provider Executive Officer ↑ | Date ↑ |
| Zorrik Voldman | President |
| Service Provider Executive Officer Name ↑ | Title ↑ |
| 911 Software, INC | |
| Service Provider Company Represented ↑ | |

Part 4. Action Plan for Non-Compliant Status

Please select the appropriate "Compliance Status" for each requirement. If you answer "NO" to any of the requirements, you are required to provide the date Company will be compliant with the requirement and a brief description of the actions being taken to meet the requirement. *Check with your acquirer or the payment brand(s) before completing Part 4, since not all payment brands require this section.*

⁵ 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 magnetic-stripe data after transaction authorization. The only elements of track data that may be retained are account number, expiration date, and name.

⁶ The three- or four-digit value printed on or to the right of the signature panel or on the face of a payment card used to verify card-not-present transactions.

⁷ Personal Identification Number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.