S³

Security Professional Services:

*2018 Payment Card
Industry Data Security Assessment
Attestation of Compliance for Onsite Assessments –
Service Provider*

Prepared For:
Working Solutions, LLC

Provided By:
Specialized Security Services, Inc.

October 30, 2018

PCi Security Standards Council ®

Version 3.2 April 2016

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:	Working Solutions, LLC	DBA (doing business as):	WSOL, LLC
Contact Name:	Billy West	Title:	VP, IT Operations and Infrastructure
Telephone:	972-964-4800 Ext. 205	E-mail:	bwest@workingsol.com
Business Address:	19111 North Dallas Pkwy Suite 180	City:	Dallas
State/Province:	TX	Country: USA	Zip: 75287
URL:	www.workingsolutions.com		

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

Company Name:	Specialized Security Services, Inc.		
Lead QSA Contact Name:	Albert Rwehumbiza	Title:	Director, Security Services
Telephone:	972-378-5554 Ext. 418	E-mail:	arwehumbiza@s3security.com
Business Address:	4975 Preston Park Blvd., West Tower Suite 510	City:	Plano
State/Province:	TX	Country: USA	Zip: 75093
URL:	www.s3security.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:	Remote and local customer care/call center services

Type of service(s) assessed:

Hosting Provider:
- ☐ Applications / software
- ☐ Hardware
- ☐ Infrastructure / Network
- ☐ Physical space (co-location)
- ☐ Storage
- ☐ Web
- ☐ Security services
- ☐ 3-D Secure Hosting Provider
- ☐ Shared Hosting Provider
- ☐ Other Hosting (specify):

Managed Services (specify):
- ☐ Systems security services
- ☐ IT support
- ☐ Physical security
- ☐ Terminal Management System
- ☐ Other services (specify):

Payment Processing:
- ☐ POS / card present
- ☐ Internet / e-commerce
- ☒ MOTO / Call Center
- ☐ ATM
- ☐ 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): None

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:	N/A

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): None

Provide a brief explanation why any checked services were not included in the assessment:	N/A

Part 2b. Description of Payment Card Business

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	Working Solutions, LLC offers customer care/call center services by providing agents, Customer Service Representatives (CSRs), both local and remote.
	The CSR local agents connect to their customers over private MPLS circuits. VOIP phones are configured to automatically connect to their customer's networks. Firewalls and routers that allow only network traffic which is considered necessary and required for business are located between each call center environment and Working Solutions, LLC customers.
	Remote agents connecting over the Internet use Microsoft's Multi-factor authentication (MFA) which is hosted within Azure. Once authenticated, all VPN traffic is routed internally to the customer's networks. Working Solutions, LLC does not store, process or transmit cardholder data in any form.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	Working Solutions, LLC does not have the ability to impact the security of cardholder data because agents connect directly to their customer's internal networks (merchants) prior to any interaction with cardholder data. Working Solutions, LLC does not process, transmit or store 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):
Corporate Headquarters	1	Dallas, TX, USA
Equinix Data Center	1	Dallas, TX, 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)
N/A	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. *For example:*	Specialized Security Services, Inc. included the website, internal network segments, external network segments, server room, corporate facility, and the data center. The agents connect through private MPLS circuits back to the

• *Connections into and out of the cardholder data environment (CDE).* • *Critical system components within the CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.*	customer's secure hosted payment pages. Working Solutions, LLC does not store, process, or transmit any cardholder data.

Does your business use network segmentation to affect the scope of your PCI DSS environment? *(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? If Yes: Name of QIR Company: QIR Individual Name: Description of services provided by QIR:	☐ Yes ☒ No
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:**
None	N/A

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:	Remote and local customer care/call center services.

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:	☐	☒	☐	1.3.6 – Working Solutions, LLC does not store any CHD in their environment.
Requirement 2:	☐	☒	☐	2.1.1 (ALL) – Working Solutions, LLC does not have any wireless network connected to CDE. 2.6 – Working Solutions, LLC is not a shared hosting provider.
Requirement 3:	☐	☐	☒	3.1, 3.2, 3.3, 3.4, 3.5, 3.6, 3.7 – Working Solutions, LLC does not store cardholder data.
Requirement 4:	☐	☐	☒	4.1 (ALL), 4.2 (ALL), 4.3 (ALL) – Working Solutions, LLC does not store, process or transmit cardholder data.
Requirement 5:	☒	☐	☐	
Requirement 6:	☐	☒	☐	6.3 (ALL) – Working Solutions, LLC does not develop applications that process, store or transmit cardholder data. 6.4.1 (ALL), 6.4.2 (ALL) 6.4.3, 6.4.4 – Working Solutions, LLC does not store, process or transmit cardholder data. 6.4.5.3 (b) – Working Solutions, LLC does not develop applications that store, process or transmit cardholder data. 6.5 (ALL) - Working Solutions, LLC does not develop applications that store, process or transmit cardholder.

		☐	☐	6.6 (ALL) - Working Solutions, LLC does not develop web applications that store, process or transmit cardholder.
Requirement 7:	☒	☐	☐	
Requirement 8:	☐	☒	☐	8.1.6 (a & b) – Working Solutions, LLC does not currently have non-consumer customers in their environment.
				8.2.1 (d & e) - Working Solutions, LLC does not currently have non-consumer customers in their environment.
				8.2.3 (b) - Working Solutions, LLC does not currently have non-consumer customers in their environment.
				8.2.4 (b) - Working Solutions, LLC does not currently have non-consumer customers in their environment.
				8.5.1 - Working Solutions, LLC does not currently have non-consumer customers in their environment
				8.7 **-** Working Solutions, LLC does not store cardholder data.
Requirement 9:	☐	☒	☐	9.5 (ALL) - Working Solutions, LLC does not store cardholder data in any media format.
				9.6 (ALL) - Working Solutions, LLC does not store cardholder data in any media format.
				9.7 (ALL) - Working Solutions, LLC does not store cardholder data in any media format.
				9.8 (ALL) - Working Solutions, LLC does not store cardholder data in any media format.
				9.9 (ALL) – Working Solutions, LLC does not have any PED devices.
				9.10 (ALL) – Working Solutions, LLC does not store cardholder data in their environment.
Requirement 10:	☐	☒	☐	10.2.1 – Working Solutions, LLC does not store any cardholder data.
Requirement 11:	☒	☐	☐	
Requirement 12:	☐	☒	☐	12.8 (ALL)– Working Solutions, LLC does not store, process or transmit cardholder data and thus does not share cardholder data with any service providers.
				12.9 (ALL)- Working Solutions, LLC does not store, process or transmit cardholder data and thus does not share cardholder data with any service providers.
Appendix A1:	☐	☒	☐	A1 (ALL) – Working Solutions, LLC is not a shared hosting provider.
Appendix A2:	☐	☒	☐	A2.3 - Working Solutions, LLC does not store, process or transmit cardholder data.

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:	October 13, 2018.	
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 *October 13, 2018.*

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 *Working Solutions, LLC* 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* 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 (3728-01-13).

Part 3b. Service Provider Attestation

Signature of Service Provider Executive Officer ↑

Service Provider Executive Officer Name: Billy West

Date: 10-22-18

Title: VP, IT Operations and Infrastructure

Part 3c. QSA Acknowledgement (if applicable)

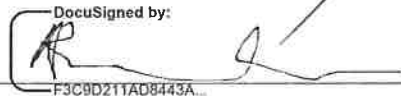| If a QSA was involved or assisted with this assessment, describe the role performed:	Specialized Security Services, Inc. performed the security assessment and prepared the PCI Report on Compliance in accordance with the PCI DSS v3.2 guidelines.

Signature of QSA's Executive Officer ↑

Date: 10 / 29 / 2018

QSA's Executive Officer Name: M. K. Mitchelle Schanbaum

QSA Company: Specialized Security Services, Inc.

DocuSigned by:

F3C9D211AD8443A...

Signature of QSA ↑

Date: 10/29/2018 8:28:22 AM PDT

QSA Name: Albert Rwehumbiza

QSA Company: Specialized Security Services, 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.