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:	Quality Contact Solutions, Inc.	DBA (doing business as):	Not Applicable
Contact Name:	Dean Garfinkel	Title:	Vice President
Telephone:	(866) 963-2889	E-mail:	Dean.Garfinkel@qualitycontactsolutions.com
Business Address:	102 Grant Street	City:	Aurora
State/Province:	NE	Country: US	Zip: 68818
URL:	https://www.qualitycontactsolutions.com		

Part 1b. Qualified Security Assessor Company Information (if applicable)					
Company Name:	CompliancePoint, Inc.				
Lead QSA Contact Name:	Kameko Hancock	Title:	Senior, Security Consultant		
Telephone:	4400 River Green Parkway, Suite 100	E-mail:	khancock@compliancepoint.com		
Business Address:	(770) 255-1100	City:	Duluth		
State/Province:	GA	Country:	US	Zip:	30096
URL:	http://www.compliancepoint.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:	Call Center Operations

Type of service(s) 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): Outsourced Telemarketing (outbound)

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:	Not Applicable - All services were reviewed during this assessment

Type of service(s) not 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):

Provide a brief explanation why any checked services were not included in the assessment:	Not Applicable. All services were reviewed during this assessment.

Part 2b. Description of Payment Card Business

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	Quality Contact Solutions (QCS) is a completely virtual environment in which its agents work from home (WFH). QCS does not store cardholder data (CHD). Using a PCI compliant hosting service provider with a secure payment Interactive Voice Response (IVR) process, QCS WFH agents process customer orders without accessing cardholder information. Customers enter the CHD via DTMF tones.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	QCS provides a full range of software and transaction processing services which allow merchants to service their customers. QCS functions as a service provider. The application, which a compliant third-party service provider application, provides store and forward functionality for credit/debit card processing for loan merchants directly into their merchant acquiring account. Processing occurs through a 3rd party payment gateway with an acquiring bank; QCS does not have access to CHD at any time.

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*
Corporate Headquarters	1	Aurora, NE
Remote Employee Workstations	43	Various remote locations

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)
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	

Part 2e. Description of Environment

Provide a **_high-level_** description of the environment covered by this assessment.	QCS provides call center services to its clients. All call center agents are remote and connect to other PCI certified service providers to process calls for their customers. Customers enter their CHD via the IVR.
For example: • *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.*	

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?	☐ Yes ☒ No

If Yes:

Name of QIR Company:	
QIR Individual Name:	
Description of services provided by QIR:	

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:
Noble Systems	Dialer hosting services
Revenue Advantage	Interactive voice response (IVR)
TLC and Associates	Outsourced call center
Agility Marketing	Outsourced call center

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:	Call Center Operations

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:	☐	☒	☐	QCS is a virtual company and does not have administrative control over firewalls or routers, or network components within the CDE. (1.1.1.b – 1.1.1.c, 1.1.4 - 1.1.7,1.2 – 1.4) QCS does not store CHD in their environment (1.3.6)
Requirement 2:	☐	☐	☒	QCS is a virtual company and does not have administrative control over network components in the CDE. (2.1, 2.2, 2.2.1 - 2.2.5, 2.3, 2.4, 2.5) QCS does not use wireless technology within the CDE. (2.1.1) QCS is not classified as a shared hosting provider. (2.6)
Requirement 3:	☐	☒	☐	QCS does not accept or process card present transactions. (3.2.1) QCS does not accept or process card not present transactions. (3.2.2) QCS does not accept or process debit/PIN transactions. (3.2.3) QCS does not have access to primary account numbers. (3.3) QCS does not store cardholder data on removable media. (3.4.c)

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.)
				QCS does not use full disk encryption within the CDE. (3.4.1) QCS does not store cardholder data. (3.4, 3.5, 3.5.1 – 3.5.4, 3.6.1 - 3.6.8)
Requirement 4:	☐	☐	☒	QCS does not maintain externally facing websites, services or applications that process cardholder data. (4.1) QCS does not use wireless technology within the CDE. (4.1.1) QCS does not use end user messaging technologies to transmit cardholder data. (4.2)
Requirement 5:	☐	☐	☒	QCS is a virtual company and does not have administrative control over network components in the CDE. (5.1, 5.1.1, 5.2, 5.3)
Requirement 6:	☐	☐	☒	QCS is a virtual company and does not have administrative control over network components in the CDE. (6.1, 6.2) QCS does not support or perform software development. (6.3 – 6.3.2, 6.4 – 6.4.6, 6.5 – 6.5.10) QCS does not maintain externally facing websites, services or applications that process cardholder data. (6.6)
Requirement 7:	☐	☒	☐	QCS' network is not in-scope. They do not provision accounts. This is accomplished by their PCI compliant Service Provider. (7.1 – 7.1.4, 7.2 – 7.2.3)
Requirement 8:	☐	☐	☒	QCS does not maintain or administer non-consumer accounts within the CDE. (8.1 - 8.1.8, 8.2 - 8.2.6, 8.3 – 8.3.2, 8.4, 8.5, 8.6) QCS does not provide remote support or have access to customer environments. (8.5.1) QCS does not store any cardholder data. (8.7)
Requirement 9:	☐	☐	☒	QCS is a virtual company and does not control physical access to CDE locations. (9.1 – 9.4.4) QCS is a virtual company and does not have administrative control over components in the CDE. (9.5) QCS does not transfer cardholder data to physical media. (9.6 - 9.6.3, 9.7.1) QCS does not store cardholder data on hard copy materials or electronically. (9.8 - 9.8.2) QCS does not use or support Point of Sale devices within the CDE. (9.9 – 9.9.3)

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 10:	☐	☐	☒	QCS is a virtual company and does not have administrative control over components in the CDE. (10.1 – 10.8.1)
Requirement 11:	☐	☐	☒	QCS is a virtual company and does not have administrative control over components in the CDE. (11.1 – 11.5.1)
Requirement 12:	☐	☒	☐	QCS is a virtual company and does not have administrative control over components in the CDE. (12.3.3 – 12.3.10, 12.5.4 – 12.6, 12.11, 12.11)
Appendix A1:	☐	☐	☒	QCS is not classified as a shared hosting provider. (A1.1, A1.2, A1.3, A1.4)
Appendix A2:	☐	☐	☒	QCS does not use early versions of the TLS protocol to transmit cardholder data. (A2.1, A2.2 A2.3) QCS does not use or support Point of Sale devices within the CDE. (A2.1)

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:	*May 23, 2020*	
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 May 23, 2020.

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 *Quality Contact Solutions, 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)

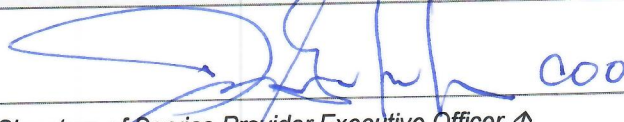|	
☒	The ROC was completed according to the *PCI DSS Requirements and Security Assessment Procedures*, Version *3.2.1*, and was completed according to the instructions therein.
☒	All information within the above-referenced ROC and in this attestation fairly represents the results of my assessment in 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)

☒ 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 – None. QCS is a virtual environment and their network is not in-scope.
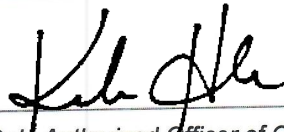
Part 3b. Service Provider Attestation

COO

Signature of Service Provider Executive Officer ↑	*Date:* May 23, 2020
Service Provider Executive Officer Name: Dean Garfinkel	*Title:* ~~Vice President~~ *COO*

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 assisted with the identification of in-scope and out of scope locations, networks, and systems. The QSA reviewed policies, procedures and verified system configurations and processes are following PCI 3.2.1 standards.

Signature of Duly Authorized Officer of QSA Company ↑	*Date:* May 23, 2020
Duly Authorized Officer Name: Kameko Hancock	*QSA Company:* CompliancePoint, 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:	Not Applicable. No ISA was involved or assisted with this assessment.

---

[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	☐	☐	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	☐	☐	