



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

---

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

**Version 3.1**

April 2015

## 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:	Charge Anywhere LLC	DBA (doing business as):	
Contact Name:	Thami Smires	Title:	CTO
ISA Name(s) (if applicable):	N/A	Title:	N/A
Telephone:	(732) 417-4447	E-mail:	tsmires@chargeanywhere.com
Business Address:	4041B Hadley Road	City:	South Plainfield
State/Province:	NJ	Country:	USA
		Zip:	07080
URL:	<a href="http://www.chargeanywhere.com">http://www.chargeanywhere.com</a>		

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

Company Name:	CompliancePoint, Inc.		
Lead QSA Contact Name:	David R. Grow	Title:	Manager, Compliance Services
Telephone:	(678) 252-1064	E-mail:	<a href="mailto:dgrow@compliancepoint.com">dgrow@compliancepoint.com</a>
Business Address:	440 River Green Parkway Suite 100	City:	Duluth
State/Province:	GA	Country:	USA
		Zip:	30096
URL:	<a href="http://www.compliancepoint.com">www.compliancepoint.com</a>		

## 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: Payment Gateway – Production Environment		
Type of service(s) assessed:		
<b>Hosting Provider:</b> <input type="checkbox"/> Applications / software <input type="checkbox"/> Hardware <input type="checkbox"/> Infrastructure / Network <input type="checkbox"/> Physical space (co-location) <input type="checkbox"/> Storage <input type="checkbox"/> Web <input type="checkbox"/> Security services <input type="checkbox"/> 3-D Secure Hosting Provider <input type="checkbox"/> Shared Hosting Provider <input type="checkbox"/> Other Hosting (specify):	<b>Managed Services (specify):</b> <input type="checkbox"/> Systems security services <input type="checkbox"/> IT support <input type="checkbox"/> Physical security <input type="checkbox"/> Terminal Management System <input type="checkbox"/> Other services (specify):	<b>Payment Processing:</b> <input checked="" type="checkbox"/> POS / card present <input checked="" type="checkbox"/> Internet / e-commerce <input checked="" type="checkbox"/> MOTO / Call Center <input type="checkbox"/> ATM <input checked="" type="checkbox"/> Other processing (specify): Pin Pass-through, PIN Translation
<input type="checkbox"/> Account Management	<input type="checkbox"/> Fraud and Chargeback	<input checked="" type="checkbox"/> Payment Gateway/Switch
<input type="checkbox"/> Back-Office Services	<input type="checkbox"/> Issuer Processing	<input type="checkbox"/> Prepaid Services
<input checked="" type="checkbox"/> Billing Management	<input type="checkbox"/> Loyalty Programs	<input checked="" type="checkbox"/> Records Management
<input checked="" type="checkbox"/> Clearing and Settlement	<input type="checkbox"/> Merchant Services	<input type="checkbox"/> Tax/Government Payments
<input type="checkbox"/> Network Provider		
<input type="checkbox"/> Others (specify):		

**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.



**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 assessed

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:

## Part 2b. Description of Payment Card Business

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.

Charge Anywhere, LLC ("Charge Anywhere") is an electronic payment solution provider, operator of the ComsGate Payment Gateway, and creator of Charge Anywhere POS Software Solution. In addition to Gateway Services, Charge Anywhere provides a suite a POS applications to enable merchants to capture payments including, credit, debit and EMV, in Retail, Restaurant, ecommerce and MOTO environments.

Charge Anywhere provides payment processing services for its clients and partners. Card-not-present transactions are initiated via the web or private frame relay. Transaction data includes PAN, CVV2, CAV2, CVC2, CID and PIN information. No sensitive authentic data is retained within any Charge Anywhere systems. The PAN is redacted and encrypted and then stored in an AES-256 encrypted MS SQL database. Transaction data is sent to third party processors to complete the authorization and settlement process via dedicated and secure connections.

Charge Anywhere receives cardholder data via card present and card-not-present transactions from customers, via e-commerce, POS systems. Charge Anywhere transmits, stores, and processes payment cardholder data to third party processors.

CHARGE Anywhere also handles encryption and decryption for end to end encrypted devices such as IDTECH Audio Jack Reader and Miura Mobile Devices.

Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.

None

## 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):
<i>Example: Retail outlets</i>	3	Boston, MA, USA
Data Center	1	South Plainfield, NJ
Corporate Headquarters	1	South Plainfield, NJ



## 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)
Not applicable			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	

## Part 2e. Description of Environment

Provide a **high-level** description of the environment covered by this assessment.

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.

Charge Anywhere provides payment processing services to its clients. Card-not-present transactions are initiated via the web or private link. Transaction data includes PAN, CVV2, CAV2, CVC2, CID and PIN information. No sensitive authentication data (SAD) is retained within Charge Anywhere's systems. The PAN is stored in a MS SQL database. The PAN is encrypted with an AES-256 bit encryption key. Transaction data is sent to third party processors to complete authorization and settlement processes via dedicated secure connections.

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 one or more third-party service providers (for example, 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:

Type of service provider:	Description of services provided:
Chase Payment Tech	Payment Processor
Elavon	Payment Processor
Euronet	Payment Processor
Evertec	Payment Processor
EVO	Payment Processor
First Data	Payment Processor
Global Payments	Payment Processor
Heartland	Payment Processor
Jetpay	Payment Processor
Merchant e-Solutions	Payment Processor
Moneris	Payment Processor
Paypal	Payment Processor
RBM	Payment Processor
TSYS	Payment Processor
VACP (Visa Accelerated Connection Platform)	Payment Processor
Bank of America	Offsite Storage Location of Backup tapes

**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:** Payment Gateway

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:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1.4 Personal firewalls are not applicable as workstations are out of scope
Requirement 2:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	2.1 No wireless in CDE; 2.2 No insecure protocols, services or daemons
Requirement 3:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 4:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 5:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 6:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 7:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 8:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	8.5 No terminated employees during the past 6 months
Requirement 9:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	9.3 No terminated employees during the past 6 months; 9.9 No POS devices in use in the environment
Requirement 10:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 11:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	11.1 No authorized wireless access points in CDE
Requirement 12:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Appendix A:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	

## 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:	<i>March 17, 2016</i>	
Have compensating controls been used to meet any requirement in the ROC?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Were any requirements in the ROC identified as being not applicable (N/A)?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
Were any requirements not tested?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Were any requirements in the ROC unable to be met due to a legal constraint?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No



## Section 3: Validation and Attestation Details

### Part 3. PCI DSS Validation

Based on the results noted in the ROC dated *March 17, 2016* 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 as of *March 17, 2016*: (**check one**):

- ☒ **Compliant:** All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby (*Service Provider Company Name*) 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)

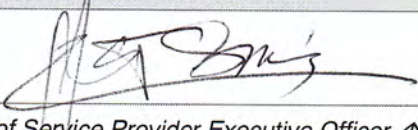
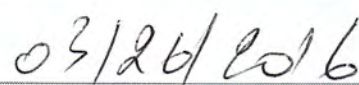
- ☒ The ROC was completed according to the *PCI DSS Requirements and Security Assessment Procedures*, Version (*version number*), and was completed according to the instructions therein.
- ☒ All information within the above-referenced ROC and in this attestation fairly represents the results of my assessment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

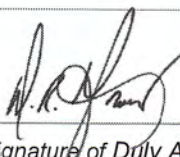
**Part 3b. Service Provider Attestation**

			
Signature of Service Provider Executive Officer ↑		Date:	
Service Provider Executive Officer Name: <b>Thami Smires</b>		Title: <b>CTO</b>	

**Part 3c. QSA Acknowledgement (if applicable)**

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

The QSA provided assistance 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 in accordance with the PCI 3.1 standards.

			
Signature of Duly Authorized Officer of QSA Company ↑		Date: <i>March 17, 2016</i>	
Duly Authorized Officer Name: <i>David R. Grow (QSA #203-541)</i>		QSA Company: <i>CompliancePoint, Inc.</i>	

**Part 3d. ISA Acknowledgement (if applicable)**

If an ISA was involved or assisted with this assessment, describe the role performed:

N/A

Signature of ISA ↑		Date:	
ISA Name: <i>N/A</i>		Title:	

<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.



#### 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	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3	Protect stored cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
4	Encrypt transmission of cardholder data across open, public networks	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
5	Protect all systems against malware and regularly update anti-virus software or programs	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6	Develop and maintain secure systems and applications	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
7	Restrict access to cardholder data by business need to know	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8	Identify and authenticate access to system components	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9	Restrict physical access to cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10	Track and monitor all access to network resources and cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
11	Regularly test security systems and processes	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12	Maintain a policy that addresses information security for all personnel	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

