



# **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:	WEX, Inc. (PWS)	DBA (doing business as):	3Delta Systems (3DSI)		
Contact Name:	Paul Jones	Title:	Manager, Information Security Management		
Telephone:	(703) 677-9526	E-mail:	Paul.jones@wexinc.com		
Business Address:	14151 Newbrook Drive, Suite 200	City:	Chantilly		
State/Province:	VA	Country:	United States	Zip:	20151
URL:	www.wexinc.com				

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

Company Name:	Drummond Group, LLC				
Lead QSA Contact Name:	Samuel P. Hinson	Title:	Business Unit Leader, PCI & Technical Risk Services		
Telephone:	(240) 575-7455	E-mail:	samuel.hinson@drummondgroup.com		
Business Address:	5303 Spectrum Dr., Ste. A	City:	Frederick		
State/Province:	Maryland	Country:	United States	Zip:	21703
URL:	www.drummondgroup.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:		Payment WorkSuite (PWS)
Type of service(s) assessed:		
<b>Hosting Provider:</b> <input checked="" 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 type="checkbox"/> Other processing (specify):
<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 type="checkbox"/> Billing Management	<input type="checkbox"/> Loyalty Programs	<input type="checkbox"/> Records Management
<input 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.

**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:**

- 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**

<p>Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.</p>	<p>WEX, Inc. Payment WorkSuite (PWS)'s business and technical capabilities are primarily focused on business-to-business, card-not-present (CNP) transactions and have been designed with the ability to process government and corporate purchase cards with Level-3 line-item detail. Level-3 line-item detail was designed to support business-to-business (B2B) and business-to-government (B2G) credit card use and includes specific purchase information, such as item description, quantity, unit of measure, price, and more. WEX/3Delta payment services also accommodate consumer cards, business cards, and purchase cards. WEX/3Delta provides merchants with a choice of interfaces/services through which credit card data flows. These interfaces are as follows: EC-Zone: Web application transaction processing via a browser; EC-Linux: Web service transaction processing (HTTPS POST method and SOAP web service); EC-Batch: File-based transaction processing (FTP-based processing); and CardVault: Data tokenization services. PWS provides additional capabilities, which include: EC-Sentry: Policy validation engine for fraud and misuse management; EC-Navigator: Non-transactional command and control functions for client management.</p>
<p>Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.</p>	<p>PWS stores the primary account number (PAN) in an encrypted format on behalf of its customers. This is a requirement because of the repeat-biller/repeat-customer nature of B2B relationships. Hence, PWS has the ability to impact the security of cardholder data.</p>

**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	<i>Boston, MA, USA</i>
Corporate Office	1	Chantilly, VA, USA
Colocation Data Center	1	Ashburn, VA, 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)
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<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.*

Web application transaction processing, web service transaction processing, file-based transaction processing, data tokenization services, internal network segments, DMZ segments, processor connections, firewalls, load balancers, intrusion detection, and physical and virtual servers.

Does your business use network segmentation to affect the scope of your PCI DSS environment?

Yes  No

*(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation)*

**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:
WEX, Inc. (EnCompass)	Separately assessed WEX business line - provides various managed services of the CDE and system components therein
Equinix	Colocation data center hosting provider

**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 WorkSuite (PWS)		
PCI DSS Requirement	Details of Requirements Assessed			Justification for Approach (Required for all “Partial” and “None” responses. Identify which sub-requirements were not tested and the reason.)
	Full	Partial	None	
Requirement 1:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1.2.2: Routers are not in use within the PWS cardholder data environments. 1.2.3: Wireless networks/technologies are not in use within the PWS cardholder data environments.
Requirement 2:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	2.1.1: Wireless networks/technologies are not in use within the PWS cardholder data environments. 2.6: WEX (PWS) is not a shared hosting provider.
Requirement 3:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	3.2.a, 3.2.b: PWS does not support issuing services. 3.4.1: Disk encryption is not used within the PWS environment. 3.6.a: WEX (PWS) does not share keys with its customers for the purpose of transmission or storage of cardholder data. 3.6.2: Cryptographic keys are not distributed. 3.6.6: Clear-text key management is not in use.
Requirement 4:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	4.1.1: Wireless networks and systems are not in use within the PWS cardholder data environments.
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"/>	8.1.5: Vendors are not allowed access to the PWS cardholder data environments. 8.5.1: WEX (PWS) does not have remote access to customer premises.
Requirement 9:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	9.1.2: There are no publicly accessible network jacks within the PWS cardholder data environment at the Equinix co-location facility. 9.6, 9.6.2, 9.6.3: There is no internal or external distribution of any kind of media. 9.8.1: Hard-copy media is not in use. 9.9, 9.9.1, 9.9.2, 9.9.3: WEX (PWS) does not utilize devices that capture payment card data via direct physical interaction with the card.
Requirement 10:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 11:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	11.1.1: There are no authorized wireless access points within the WEX (PWS) cardholder data environments.
Requirement 12:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	12.3.9: WEX/3Delta does not allow vendor access to the PWS/ARX cardholder data environments.
Appendix A1:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	A1.1-A1.4: WEX (PWS) is not a shared hosting provider.
Appendix A2:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	A2.1-A2.3: WEX (PWS) does not use POS POI terminals or SSL/early TLS.

## 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 8 ,2020
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

This AOC is based on results noted in the ROC dated May 8, 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**):

<input checked="" type="checkbox"/>	<p><b>Compliant:</b> All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall <b>COMPLIANT</b> rating; thereby WEX, Inc. (PWS) has demonstrated full compliance with the PCI DSS.</p>						
<input type="checkbox"/>	<p><b>Non-Compliant:</b> Not all sections of the PCI DSS ROC are complete, or not all questions are answered affirmatively, resulting in an overall <b>NON-COMPLIANT</b> rating, thereby (<i>Service Provider Company Name</i>) has not demonstrated full compliance with the PCI DSS.</p> <p><b>Target Date</b> for Compliance:</p> <p>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. <i>Check with the payment brand(s) before completing Part 4.</i></p>						
<input type="checkbox"/>	<p><b>Compliant but with Legal exception:</b> 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.</p> <p><i>If checked, complete the following:</i></p> <table border="1" style="width: 100%;"> <thead> <tr> <th style="width: 35%;">Affected Requirement</th> <th>Details of how legal constraint prevents requirement being met</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> </tbody> </table>	Affected Requirement	Details of how legal constraint prevents requirement being met				
Affected Requirement	Details of how legal constraint prevents requirement being met						

### Part 3a. Acknowledgement of Status

Signatory(s) confirms:

(**Check all that apply**)

<input checked="" type="checkbox"/>	The ROC was completed according to the <i>PCI DSS Requirements and Security Assessment Procedures</i> , Version 3.2.1, and was completed according to the instructions therein.
<input checked="" type="checkbox"/>	All information within the above-referenced ROC and in this attestation fairly represents the results of my assessment in all material respects.
<input type="checkbox"/>	I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
<input checked="" type="checkbox"/>	I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
<input checked="" type="checkbox"/>	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 Qualys (3728-01-14)

**Part 3b. Service Provider Attestation**



<i>Signature of Service Provider Executive Officer</i> ↑	<i>Date:</i> May 8, 2020
<i>Service Provider Executive Officer Name:</i> Michael Leonhirth	<i>Title:</i> CISO

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

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



<i>Signature of Duly Authorized Officer of QSA Company</i> ↑	<i>Date:</i> 5-8-20
<i>Duly Authorized Officer Name:</i> Samuel P. Hinson	<i>QSA Company:</i> Drummond Group, LLC

**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:	
---	--

<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.