



Payment Card Industry (PCI) Data Security Standard

Attestation of Compliance for Onsite Assessments – Service Providers

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:	US Bank		DBA (doing business as):	Corporate Payment Systems (CPS)		
Contact Name:	Thoralf Symreng		Title:	VP, Information Security Services		
Telephone:	612-973-7137		E-mail:	Thoralf.symreng@usbank.com		
Business Address:	1 Meridian Crossing		City:	Richfield		
State/Province:	MN	Country:	USA		Zip:	55423
URL:	http://www.usbank.com					

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

Company Name:	Verizon Business Services				
Lead QSA Contact Name:	Mike Zhang	Title:	Senior Security Consultant		
Telephone:	434-282-4677	E-mail:	Haomin.Zhang@verizon.com		
Business Address:	22001 Loudon County Parkway	City:	Ashburn		
State/Province:	VA	Country:	USA	Zip:	20147
URL:	http://www.verizonenterprises.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: Corporate Payment Systems (CPS)

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): Closed Loop and Fleet cards

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

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.

Corporate Payment Systems (CPS) is a procurer, manager, and processor of corporate cards and an issuer of closed-loop fleet cards for corporate customers. Among the corporate cards that it processes are branded aviation-industry cards, private-label cards, and bank cards. The data elements transmitted to CPS business units includes primary account numbers (PAN), expiration dates, card security codes, and full track data. The data stored consists of full PAN (in an encrypted state) and expiration dates, as well as truncated PAN. For authorization and settlement, payment card data will be kept either internally or sent to an issuing partner or to US Bank – Elavon.

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

Not Applicable

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 Offices	1	Richfield, MN, USA *Please note: US Bank CPS utilizes services provided by US Bank's internal service provider, Shared PCI Assets (SPA). All applicable onsite reviews, observations, and requirements for US Bank CPS were performed as part of the US Bank SPA PCI assessment. Verizon validated that all onsite controls are in place under the US Bank SPA Report on Compliance dated 12 January 2018. This requirement was tested and validated under the US Bank internal service provider assessment (SPA). Verizon validated that this control is in place under the US Bank SPA Attestation of Compliance dated 12 January 2018 and that it covers the scope of the services used by the US Bank CPS.

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)
Multi Service Aviation (MSA) Auth and Settle	In-House Developed	US Bank	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	
WebPOS	In-House Developed	US Bank	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	
OTR	In-House Developed	US Bank	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	
Voyager	In-House Developed	US Bank	<input type="checkbox"/> Yes <input checked="" 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.

CPS's Access Online business unit uses website, application, and database servers to facilitate the management, procurement, and reporting of corporate cards. Through mobile and desktop user interfaces, cardholder data (CHD) is entered by Access Online consumers and displayed to them. To support this functionality as well as the creation of reports, CHD is stored in an encrypted format in Access Online distributed databases. For the issuing

and processing of corporate cards, Access Online partners with TSYS, via Connect:Direct connections.

Authorization requests from Multi Service Aviation merchants are received either via dial-up connections to MSA application servers or via a secure website gateway, supported by website and application servers. These authorization requests are then transmitted via private, Connect:Direct connections to US Bank – Elavon or other issuing partners. Following an authorization response, PAN is transmitted from the application servers to the MSA database cluster, for storage in an encrypted format. All sensitive authentication data (SAD) collected during the authorization process is retained in volatile memory on the application servers and purged, post-authorization response. Batch settlement files are received from dial-up and WebPOS merchant connections, stored encrypted in settlement servers, and transmitted via private, Connect:Direct connections to US Bank – Elavon or other issuing partners.

OTR works with its business partner, Transcard, to issue OTR fleet cards, by transmitting customer requests and receiving cardholder data, in return, via API. This PAN – card validation codes or values (CVV) are kept by Transcard – is stored, encrypted, on a mid-range computer. Authorization requests are received via VPN from merchant headquarters, payment processors, or US Bank – Elavon. These requests are received by the mid-range computer and either processed internally (for fuel transactions) or sent via API to Transcard, (for pre-paid, non-fuel transactions). Settlement files, including full PAN, are processed in a similar fashion. An Interactive Voice Response system also transmits PAN, via API, to the Fleet Commander Online application, in order to authenticate callers wishing to manage their fleet cards over the phone.

All issuing, authorizing, and servicing of Voyager closed-loop fleet payment cards occurs on a mainframe system. New fuel card requests are received by website applications that transmit the requests to the mainframe. Embossing files, containing PAN, are stored, encrypted, on the mainframe. The HP NonStop Tandem system used by Elan Financial Services receives authorization requests from merchants, and transmits those requests, via Connect:Direct, from its BASE 24 application to Voyager's mainframe application, for processing. CVV, if present, is compared by the Voyager application with the CVV kept in encrypted format on the mainframe. Settlement files do not contain PAN.

	<p>Should a Voyager fleet card not be accepted at a given location, a customer can use a website to request the creation of a MasterCard Single-Use Account (SUA). The Voyager application then calls an Access Online web service to request the SUA and receive the MasterCard PAN, expiration date and CVV for the customer to use. These transactions are authorized through Access Online's partner, TSYS. A nightly sales file is sent to Voyager from TSYS, via Access Online, for reconciliation with the fleet customer's billing statement.</p>
<p>Does your business use network segmentation to affect the scope of your PCI DSS environment?</p> <p><i>(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation)</i></p>	<p><input checked="" type="checkbox"/> Yes <input type="checkbox"/> No</p>

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:
US Bank Shared PCI Assets	Managed Security and Network Services *Please note: US Bank CPS utilizes services provided by US Bank's internal service provider, Shared PCI Assets (SPA). All applicable onsite reviews, observations, and requirements for US Bank CPS were performed as part of the US Bank SPA PCI assessment. Verizon validated that all onsite controls are in place under the US Bank SPA Report on Compliance dated 12 January 2018. This requirement was tested and validated under the US Bank internal service provider assessment (SPA). Verizon validated that this control is in place under the US Bank SPA Attestation of Compliance dated 12 January 2018 and that it covers the scope of the services used by the US Bank CPS.
Elan Financial Services	Payment Gateway
Elavon	Payment Gateway
CDW	AS/400 System Maintenance
TransCard	Issuing Services (OTR)
TSYS	Issuing Services
Giesecke & Devrient	Embossing Services

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:		Corporate Payment Systems (CPS)		
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 checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 2:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	2.1.1.x - Not Applicable - Wireless technologies are used, but are not connected to and does not impact the security of the CDE 2.6 - Not Applicable - CPS is not a shared hosting provider
Requirement 3:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	3.6.a - Not Applicable - CPS does not share encryption keys with their customers
Requirement 4:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	4.1.1 - Not Applicable - Wireless technologies are used, but are not connected to and does not impact the security of the CDE
Requirement 5:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 6:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	6.4.6 – Not Applicable - CPS did not have any significant changes within the past 12 months
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.a, 8.1.5.b – Not Applicable – CPS does not have vendors that remotely access the network
Requirement 9:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	9.8.2 – Not Applicable – CPS does not store PAN data on removable media 9.9, 9.9.1, 9.9.2, 9.9.3 - Not Applicable - CPS does not have any POI terminals in scope
Requirement 10:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 11:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	11.2.3.x – Not Applicable - CPS did not have any significant changes within the past 12 months
Requirement 12:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	12.3.9 – Not Applicable – CPS does not have vendors that remotely access the network
Appendix A1:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Appendix A2:	<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:	13 July 2018	
Have compensating controls been used to meet any requirement in the ROC?	<input checked="" type="checkbox"/> Yes	<input 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 **13 July 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**):

<input checked="" type="checkbox"/>	<p>Compliant: All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall COMPLIANT rating; thereby <i>Corporate Payment Systems</i> has demonstrated full compliance with the PCI DSS.</p>						
<input type="checkbox"/>	<p>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 <i>Corporate Payment Systems</i> has not demonstrated full compliance with the PCI DSS.</p> <p>Target Date 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>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.</p> <p><i>If checked, complete the following:</i></p> <table border="1"> <thead> <tr> <th>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, 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 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.
<input checked="" type="checkbox"/>	ASV scans are being completed by the PCI SSC Approved Scanning Vendor <i>Qualys and Tenable</i>

Part 3b. Service Provider Attestation

Prescott Balch, SVP Business Information Officer
Prescott Balch

Daniel Ratzlaff, VP Global Technology
Daniel Ratzlaff

Signature of Service Provider Executive Officer ↑

Date: 7/13/2018

Service Provider Executive Officer Name:

Title:

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 performed interviews, reviewed evidence, and wrote the Report on Compliance and Attestation of Compliance.

[Signature]
 Eric Jolent

QSA NAME: Mike Zhang

Mike Zhang

Signature of Duly Authorized Officer of QSA Company ↑

Date: July 13, 2018

Duly Authorized Officer Name: Eric Jolent

QSA Company: Verizon Business Services

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:

N/A

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	<input type="checkbox"/>	<input type="checkbox"/>	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	<input type="checkbox"/>	<input type="checkbox"/>	
3	Protect stored cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
4	Encrypt transmission of cardholder data across open, public networks	<input type="checkbox"/>	<input type="checkbox"/>	
5	Protect all systems against malware and regularly update anti-virus software or programs	<input type="checkbox"/>	<input type="checkbox"/>	
6	Develop and maintain secure systems and applications	<input type="checkbox"/>	<input type="checkbox"/>	
7	Restrict access to cardholder data by business need to know	<input type="checkbox"/>	<input type="checkbox"/>	
8	Identify and authenticate access to system components	<input type="checkbox"/>	<input type="checkbox"/>	
9	Restrict physical access to cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
10	Track and monitor all access to network resources and cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
11	Regularly test security systems and processes	<input type="checkbox"/>	<input type="checkbox"/>	
12	Maintain a policy that addresses information security for all personnel	<input type="checkbox"/>	<input type="checkbox"/>	
Appendix A1	Additional PCI DSS Requirements for Shared Hosting Providers	<input type="checkbox"/>	<input type="checkbox"/>	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS	<input type="checkbox"/>	<input type="checkbox"/>	

