DocuSign Envelope ID: FE914F85-7F81-412C-9D8A-B0380A45180C



Payment Card Industry (PCI)
Data Security Standard

Teleperformance Colombia

December 30, 2020

Attestation of Compliance for Onsite Assessments – Service Providers

Version 3.2.1

June 2018

DocuSign Envelope ID: FE914F85-7F81-412C-9D8A-B0380A45180C

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:	Teleperformance Colombia		DBA (doing business as):	Teleperformance Colombia	
Contact Name:	Alvaro Guerrero		Title:	Security Director	
Telephone:	+57 1 4049080		E-mail:	alvaro.guerrero @teleperformance.com	
Business Address:	Av. Calle 26 Num. 92-32 TorreB Piso 6		City:	Bogotá	
State/Province:	Cundinamarca	Country:	Colombia	Zip:	111071
URL:	https://co.teleperformance.com/es-es				

Part 1b. Qualified Security Assessor Company Information (if applicable)					
Company Name:	SecurityMetrics, Inc.				
Lead QSA Contact Name:	Thomas McCrory		Title:	Principal Security Analyst	
Telephone:	+1 801-705-5664		E-mail:	aoc@securitymetrics.com	
Business Address:	1275 West 1600 North		City:	Orem	
State/Province:	Utah	Country:	USA	Zip:	84057
URL:	www.securitymetrics.com				

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

DocuSign Envelope ID: FE914F85-7F81-412C-9D8A-B0380A45180C

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:	Contact Center, TP Wallet, TP Wallet Knox	
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):		

***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.*

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

DocuSign Envelope ID: FE914F85-7F81-412C-9D8A-B0380A45180C

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:	Teleperformance Colombia performs several services for merchants which neither include the storage, processing, or transmission of cardholder data nor impact the security of cardholder data. As such, these services were not included in the assessment.	

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

DocuSign Envelope ID: FE914F85-7F81-412C-9D8A-B0380A45180C

Part 2b. Description of Payment Card Business	
Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	Teleperformance Colombia receives cardholder data via SIP-enabled VoIP phones or through IVR servers which retrieve cardholder data for the TP Wallet and TP Wallet Knox (henceforth collectively referred to as “TP Wallet”) services before normalization, encryption, and storage to Teleperformance Colombia database servers. Depending on the campaign, VoIP payments entering the Teleperformance Colombia systems are processed indirectly through the Teleperformance Colombia clients’ payment applications. VoIP calls coming into the Teleperformance Colombia environment for the purpose of indirect processing do so via a dedicated call manager and are encrypted before storage. Due to the COVID-19 pandemic, some agents work remotely from their homes. These Work-at-Home Home Agents (aka WAHA-HA, or Cloud Campus) connect to the Teleperformance Colombia network via hardened workstations provided by Teleperformance Colombia and using a virtual private network (VPN) secured with a custom Idaptive multi-factor authentication solution.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	Cardholder data is received, stored, and transmitted as part of the TP Wallet and Contact Center business operations.

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*
Contact Center	1	Barranquilla, Colombia • Blue Gardens
Contact Center	14	Bogotá, Colombia • Africa • Americas • Andalucía • Business Center • BTS0 • BTS3 • Cataluña • Europa • Iserra 100 • North Point • Oceania • Pacífico • Puerta del Sol • Textura

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

DocuSign Envelope ID: FE914F85-7F81-412C-9D8A-B0380A45180C

Contact Center	6	Medellín, Colombia • Antioquia • Andes I • Andes II • Barrio Colombia • Habitat Store • Itagüí
Contact Center	1	Tunja, Colombia • Green Hills
Data Center	1	Bogotá, Colombia

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)
TP Wallet Knox2 V2	3.0.0.1	Teleperformance Colombia	☐ Yes ☒ No	Not Applicable

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.*	The assessment covered all systems used to support card-not-present transaction data received by web servers and IVR systems located at the Teleperformance Contact Centers and the CenturyLink data center in Bogotá, Colombia. This includes: • All connections into and out of the cardholder data environment (CDE). • Critical systems within the CDE, such as firewalls, web servers, database servers, administrator workstations, contact center workstations, a custom Idaptive MFA solution, and people, processes, and technologies that support logging and monitoring. • Secure software development that may impact the security of 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

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

DocuSign Envelope ID: FE914F85-7F81-412C-9D8A-B0380A45180C

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:	Not Applicable	
QIR Individual Name:	Not Applicable	
Description of services provided by QIR:	Not Applicable	
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:**	
CenturyLink	Colocation, physical security	
Note: *Requirement 12.8 applies to all entities in this list.*		

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

DocuSign Envelope ID: FE914F85-7F81-412C-9D8A-B0380A45180C

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:	Contact Centers, TP Wallet, TP Wallet Knox

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:	☐	☒	☐	**1.2.2: N/A – No routers exist within the Teleperformance Colombia CDE.**
Requirement 2:	☐	☒	☐	**2.1.1: N/A – No wireless technologies are in use within the Teleperformance Colombia CDE.** **2.2.3: N/A – No insecure services, protocols, or daemons are in use.** **2.6: N/A – Teleperformance Colombia is not a shared hosting provider.**
Requirement 3:	☐	☒	☐	**3.4.1: N/A – Disk encryption is not used.** **3.6: N/A – Teleperformance Colombia does not share cryptographic keys with customers.** **3.6.6: N/A – Manual clear-text cryptographic key management operations are not used.**
Requirement 4:	☐	☒	☐	**4.1.1: N/A – No wireless technologies are in use.**
Requirement 5:	☒	☐	☐	
Requirement 6:	☐	☒	☐	**6.4.6: N/A – No significant changes have occurred in the previous 12 months.** **6.6: N/A – No public-facing web applications are present.**
Requirement 7:	☒	☐	☐	

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

DocuSign Envelope ID: FE914F85-7F81-412C-9D8A-B0380A45180C

Requirement 8:	☐	☒	☐	**8.1.5: N/A – No third-party accounts are granted access to the Teleperformance Colombia CDE.** **8.5.1: N/A – Teleperformance Colombia does not control access to any third-party or customer systems.**
Requirement 9:	☐	☒	☐	**9.5.1 - 9.7.1: N/A – No cardholder data is stored on removable media.** **9.8.1: N/A – No cardholder data is stored on hard-copy materials.** **9.9 - 9.9.3: N/A – Teleperformance Colombia does not manage any devices that capture cardholder data via direct physical interaction.**
Requirement 10:	☐	☒	☐	**10.5.4: N/A – No external-facing technologies are present.**
Requirement 11:	☐	☒	☐	**11.2.3: N/A – No significant changes have occurred in the previous 12 months.**
Requirement 12:	☐	☒	☐	**12.3.9: N/A – No third-party accounts are granted access to the Teleperformance Colombia CDE.**
Appendix A1:	☐	☒	☐	**A1.1 - A1.4: N/A – Teleperformance Colombia is not a shared hosting provider.**
Appendix A2:	☐	☒	☐	**A2.1 – A2.3: N/A – Teleperformance Colombia does not use SSL or early TLS for POS POI terminal connections.**

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

DocuSign Envelope ID: FE914F85-7F81-412C-9D8A-B0380A45180C

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:	*December 30, 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

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

DocuSign Envelope ID: FE914F85-7F81-412C-9D8A-B0380A45180C

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in the ROC dated *December 30, 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 *Teleperformance Colombia* 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 *Teleperformance Colombia* 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.

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

DocuSign Envelope ID: FE914F85-7F81-412C-9D8A-B0380A45180C

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 *(Tenable.io)*

Part 3b. Service Provider Attestation

DocuSigned by:
Alvaro Guerrero
C928BED28B7C45C...

Signature of Service Provider Executive Officer ↑	*Date:* **January 13, 2021**
Service Provider Executive Officer Name: **Alvaro Guerrero**	*Title:* **Security Director**

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

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

DocuSigned by:
Thomas McCrory
47D3F84EE0B2431...

Signature of Duly Authorized Officer of QSA Company ↑	*Date:* **January 13, 2021**
Duly Authorized Officer Name: **Thomas McCrory**	*QSA Company:* **SecurityMetrics, 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*

[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.

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

DocuSign Envelope ID: FE914F85-7F81-412C-9D8A-B0380A45180C

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	☐	☐	











© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.