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:	First Data International – Deutschland (Germany)		DBA (doing business as):	First Data Deutschland GmbH	
Contact Name:	Bolanle Olowolagba		Title:	Director, Risk and Control	
Telephone:	+44 (0)1268 298327		E-mail:	bolanle.olowolagba@firstdata.com	
Business Address:	Marienbader Platz 1		City:	Bad Homburg v. d. Höhe	
State/Province:	Not Applicable	Country:	Germany	Zip:	61348
URL:	http://www.firstdata.com				

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

Company Name:	Trustwave Holdings Inc.				
Lead QSA Contact Name:	Anthony Baker		Title:	QSA	
Telephone:	+1 (312) 873-7500		E-mail:	abaker@trustwave.com	
Business Address:	70 W. Madison Street, Suite 600		City:	Chicago	
State/Province:	IL	Country:	USA	Zip:	60602
URL:	https://www.trustwave.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:	Authorization, settlement, fraud, chargebacks, issuing	
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): Call center acquiring and issuing, Call Center 24 – Issuing, Customer Service and Business Support, Authorization, Payment Gateway mPOS, Payment Facilitator mPOS, Dynamic Currency Conversion (DCC) Service, 3D Secure Service		

***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:	Not Applicable	

Part 2b. Description of Payment Card Business	
Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	Payment transactions (card-present, PIN/Debit, card-not-present, Telephone Orders) enter (using HTTPS protocol, TLS 1.2 encrypted (AES 128/256-bit} or IPSec (AES-256 or IPSec 3DES-168the First Data Deutschland processing environment from the internet, the card brands, and directly connected network service providers. Card-present and /PIN/debit transactions are received from Visa, JCB, Discover, MasterCard, Diners International, UnionPay International or from the internet. The transactions received from Visa and MasterCard (IPSec 3DES 168-bit) are processed in the Global Authorization Network System (GANS) and Poseidon payment system. The transactions received from the internet that are sent to the GANS system are then forwarded to Visa or MasterCard for upstream processing via a direct-connection. Card-not-present transactions are received from Visa, MasterCard, or directly from the internet. The transactions received by First Data Deutschland directly from the internet are received by the Internet Payment Gateway (IPG) over HTTPS encrypted TLS 1.2 encrypted (AES 128/256-bit)) connections. The card-not-present transactions are routed to the GANS system and then forwarded to VISA and MasterCard for upstream processing. Cardholder data is stored within the First Data Deutschland environment either encrypted (AES-256) or protected using the appropriate compensating controls. First Data Deutschland stores the following cardholder data: - Cardholder data (PAN, Cardholder Name, Expiration date) on the disks and databases encrypted using (AES-256) to provide clients the following services: clearing, settlement, chargeback, fraud monitoring. Tokenized PAN and truncated PAN (first six and last four) are also stored - SAD (full track, EMV Track Equivalent data, PIN block and card security codes) on the disks encrypted using (AES-256) or protected using the appropriate compensating controls to provide clients card production service.
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 All PCI DSS related systems and processes have been included in the scope of review.

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*
Data Center	1	E-Shelter company – Eschborner Landstrasse 100, 60489 Frankfurt, Germany
DR site	1	Equinix company – Kruppstrasse 121-127, 60388 Frankfurt, Germany
Corporate Office, Call Center	1	Marienbader Platz 1, 61348 Bad Homburg v. d. Höhe, Germany
Office	1	Nelson Mandela Platz 18, 90459 Nürnberg, Germany

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)
Poseidon OLTP	4.1	ATOS Worldline	☒ Yes ☐ No	28 Oct 2022
Solon	1.38.06	FDCS	☐ Yes ☒ No	Not Applicable
Madeira	4.0.1.0	FDCS	☐ Yes ☒ No	Not Applicable
FD First Insight	16.07	FDCS	☐ 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.*	This assessment covers GANS (Global Authorization Network System) and the Payment application Poseidon, which process CHD and accepts connections from and to company customers/payment brands was assessed. Firewalls that protect company. The following company's CDE system components were assessed: • OS: Microsoft Windows, *nix (to support payment application and security systems) • Database: to store CHD in encrypted format • Network equipment(firewalls,switches,routers): to transmit CHD transaction, to encrypt CHD transaction • Payment applications: to process CHD • Supporting systems: FIM solution, virtual technology, backup systems, Domain controllers, antivirus system. • Central Log solution to store security logs

	• IDS: to prevent cyber attacks • Web-servers: to support payment applications • WAF: to protect against cyber attacks • HSMs: for card authorization process The following processor connections were assessed: • MasterCard (direct connection) - Payment Processor for Authorization, Settlement, Clearing, Chargeback. • Arcot Systems Inc (direct connection) - Payment Processor for 3D-Secure Authorization • Gemalto GmbH (direct connection) – Card personalization company • Discover (connection over Telecash) – card brand • VISA (direct connection) - Payment Processor for Authorization, Settlement, Clearing, Chargeback. • American Express (connection over TeleCash) - Payment Processor for Authorization, Settlement, Clearing, Chargeback. • JCB (direct connection) - Payment Processor for Authorization, Settlement, Clearing, Chargeback. • Diners International (direct connection) - Payment Processor for Authorization, Settlement, Clearing, Chargeback.
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:	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:**
Arcot Systems Inc	Payment gateway, 3D-Secure processing
Netcetera	3D-Secure processing
Swisscom	Estatement processing company
Swiss Post Solutions	Paper Statements processing company

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:	Authorization, settlement, fraud, chargebacks, issuing

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:	☒	☐	☐	
Requirement 2:	☐	☒	☐	The following sub-requirements are Not Applicable: 2.1.1 (There is no wireless in the CDE and in the scope of the assessment) 2.6 (Company is not a Shared hosting provider)
Requirement 3:	☒	☐	☐	
Requirement 4:	☐	☒	☐	The following sub-requirements are Not Applicable: 4.1.1 (There is no wireless in the CDE and in the scope of the assessment)
Requirement 5:	☒	☐	☐	
Requirement 6:	☐	☒	☐	The following sub-requirements are Not Applicable: 6.5.3 (Company does not develop cryptographic storage applications.) 6.5.4 (Company does not develop communication mechanisms.)
Requirement 7:	☒	☐	☐	
Requirement 8:	☐	☒	☐	The following sub-requirements are Not Applicable: 8.1.3 (There are no terminated users in the past six months),

				8.1.5 (Company does not have any vendor accounts for remote access), 8.5.1 (Company does not provide customers access to cardholder data)
Requirement 9:	☐	☒	☐	The following sub-requirements are Not Applicable: 9.9 (Company does not have POI-devices that capture payment card data.)
Requirement 10:	☒	☐	☐	
Requirement 11:	☒	☐	☐	
Requirement 12:	☐	☒	☐	The following sub-requirements are Not Applicable: 12.3.9 (Vendors and business partners do not have access to CDE)
Appendix A1:	☐	☐	☒	Not Applicable. Company is not a Shared Hosting Provider
Appendix A2:	☐	☐	☒	Not Applicable.

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:	*October 17, 2019*	
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 *October 17, 2019.*

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 *First Data International - Deutschland (Germany)* 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 *Trustwave*

[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 3b. Service Provider Attestation

Signature of Service Provider Executive Officer ↑	*Date: October 17, 2019*
Service Provider Executive Officer Name: Kristina Rossi	*Title:* Director Risk and Control

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

If a QSA was involved or assisted with this assessment, describe the role performed:	*Anthony Baker QSA performed assessment and prepared the Report on Compliance.* *James Sawyer QSA assisted assessment on-site with interviews*

Signature of Duly Authorized Officer of QSA Company ↑	*Date: October 17, 2019*
Duly Authorized Officer Name: Anthony Baker	*QSA Company:* Trustwave Holdings, 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*

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	☒	☐