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:	Worldline SA France		DBA (doing business as):	Not Applicable	
Contact Name:	Pierre Poquet		Title:	Security Manager	
Telephone:	+33 (0)2 54 44 74 07		E-mail:	pierre.poquet@worldline.com	
Business Address:	19 rue de la Vallée Maillard		City:	Blois	
State/Province:	N/A	Country:	France	Zip:	41000
URL:	http://www.worldline.com				

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

Company Name:	Trustwave				
Lead QSA Contact Name:	Panagiotis Sklavos		Title:	Senior Security Consultant	
Telephone:	+44 (0) 845-456-9611		E-mail:	PSklavos@trustwave.com	
Business Address:	Westminster Tower 3 Albert Embankment		City:	London	
State/Province:	London	Country:	United Kingdom	Zip:	SE1 7SP
URL:	http://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:	Accor ESM, Sips, SNCF Payment Processing Platform (SIC), Orange IVR, PVOICE IVR, Store Acceptance	
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): Authorization		

***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:	**Managed Services (specify):**	**Payment Processing:**
☐ Applications / software	☐ Systems security services	☐ POS / card present
☐ Hardware	☐ IT support	☐ Internet / e-commerce
☐ Infrastructure / Network	☐ Physical security	☐ MOTO / Call Center
☐ Physical space (co-location)	☐ Terminal Management System	☐ ATM
☐ Storage	☐ Other services (specify):	☐ Other processing (specify):
☐ Web		
☐ Security services		
☐ 3-D Secure Hosting Provider		
☐ Shared Hosting Provider		
☐ Other Hosting (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): Not Applicable		

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.	Worldline specializes in high tech electronic payment solutions and services. Worldline provides services in Europe (Belgium, France, Germany, UK, Spain, Netherlands, Italy), Asia and Latin America. The assessment focuses on the Worldline Regional Business Unit France, Worldline SA (WLSA). The other regional business units are undergoing their own PCI DSS assessments. WLSA maintains several different payment platforms to cater to the needs of its customers and offers several services, through its Merchant Services and Mobility and eTransformation Services divisions (the Financial Services division being held within equensWorldline France, another processing entity with a separate assessment). Outside France, WLSA addresses foreign markets through the other Regional Business Units and local contracts. American Express, Visa, MasterCard, JCB, Diners, and Cartes Bancaires, Bancontact, Bank of China are accepted. WLSA accepts card-present and PIN/Debit transactions over leased lines, and card-not-present transactions over the Internet, over telephone, IVR, and retail location. WLSA receives transactions over leased lines and over the Internet (using TLS 1.2, RSA 2048bit or VPN IPsec AES256bit) and transmits data via leased lines or the Internet (using TLS 1.2 or VPN IPsec AES256bit) to upstream providers, acquirers, issuing banks and the Brands. WLSA stores PANs in encrypted, hashed, truncated forms for reporting, settlement and authorization purposes.
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. WLSA is neither otherwise involved nor has the ability to impact the security of cardholder data.

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):
Worldline SA Data Center	1	Vendome, France
Worldline SA Data Center	2	Seclin, France
Worldline SA Office	1	Blois, France

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)
Accor ESM	2.00.21	Worldline SA France	☐ Yes ☒ No	Not Applicable
Sips	18R2	Worldline SA France	☐ Yes ☒ No	Not Applicable
SNCF SIC	FO 2.6.5 BO MO 3.7.6 BO FI 5.3.17 BO NMP 1.14.2	Worldline SA France	☐ Yes ☒ No	Not Applicable
Orange IVR	3.0.0	Worldline SA France	☐ Yes ☒ No	Not Applicable
PVOICE IVR	0.0.15	Worldline SA France	☐ Yes ☒ No	Not Applicable
Store Acceptance	Casino 2.1.08 Mutu 2.2.05	Worldline SA France	☐ 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 in-scope WLSA logical environments and zones were included in the Worldline data center in Seclin, France and in the Worldline data center in Vendôme, France and all systems and procedures which support these zones. The network connections (private leased lines or IPsec VPNs) for payment processing with 3rd parties were part of the assessment. The following elements were reviewed during the assessment: • Payment applications • Databases • Operating systems • Firewalls • Switches • Intrusion Prevention systems

	• Web application firewalls • Antivirus solutions • FIM
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? If Yes: Name of QIR Company: QIR Individual Name: Description of services provided by QIR:	☐ Yes ☒ No
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:**
equensWorldline France	Payment Processing
Adyen B.V (VI)	Payment Processing
Ingenico e-Commerce Solutions	Payment Processing
Lyra Network	Payment Processing
Monext - Payline	Payment Processing
Verifone Paybox Point Transaction Systems	Payment Processing
equensWorldline GmbH	Payment Processing
equensWorldline Belgium	Payment Processing
COFFISEC	Physical Security Training Provider
EIFFAGE	CCTV & Access Control system in Data Centers
Derichebourg	Media Destruction

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:	Accor ESM, Sips, SNCF Payment Processing Platform (SIC), Orange IVR, PVOICE IVR, Store Acceptance			
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:	☐	☒	☐	Req. 2.1.1 - Not Applicable – WLSA does not have Wireless connected to the in scope environment. Req. 2.6 – Not Applicable – WLSA is not a Shared Hosting Provider.
Requirement 3:	☐	☒	☐	Req. 3.6 – Not Applicable – WLSA does not share keys with customers
Requirement 4:	☐	☒	☐	Req. 4.1.1 - Not Applicable – WLSA does not have Wireless connected to the in scope environment.
Requirement 5:	☒	☐	☐	
Requirement 6:	☒	☐	☐	
Requirement 7:	☒	☐	☐	
Requirement 8:	☐	☒	☐	Req. 8.1.5 – Not Applicable – No vendor access Req. 8.5.1 – Not Applicable - WLSA does not have remote connectivity access to service providers and consumers.
Requirement 9:	☐	☒	☐	Req. 9.6 – Not Applicable – Media is not distributed Req. 9.6.2 – Not Applicable – Media is not distributed Req. 9.6.3 – Not Applicable – Media is not distributed

				Req. 9.8.1 – Not Applicable – No hard copy materials used Req. 9.9 – Not Applicable - WLSA does not operate devices at the point of sale. Req. 9.9.1, 9.9.2, 9.9.3 – Not Applicable - WLSA does not operate devices at the point of sale.
Requirement 10:	☒	☐	☐	
Requirement 11:	☐	☒	☐	Req. 11.2.3 – Not Applicable – No significant changes
Requirement 12:	☐	☒	☐	Req. 12.3.9 – Not Applicable – No Vendor access
Appendix A1:	☐	☐	☒	Appendix A1 – Not Applicable – WLSA is not a Shared Hosting Provider.
Appendix A2:	☒	☐	☐	

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:	September 14, 2018	
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 *September 14, 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):***

☒	**Compliant:** All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby Worldline SA France 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 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:* September 14, 2018
Service Provider Executive Officer Name: Pierre POQUET	*Title:* Security Manager

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

If a QSA was involved or assisted with this assessment, describe the role performed:	Panagiotis Sklavos is the Lead-QSA for this Report on Compliance.

Signature of Duly Authorized Officer of QSA Company ↑	*Date:* September 14, 2018
Duly Authorized Officer Name: Michael Aminzade	*QSA Company:* Trustwave

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	☒	☐