Payment Card Industry
Data Security Standard

Attestation of Compliance for Report on Compliance – Service Providers

Version 4.0

Revision 2

Publication Date: August 2023

PCI DSS v4.0 Attestation of Compliance for Report on Compliance – Service Providers

Entity Name: Worldline Merchant Services

Assessment End Date: 30 Oct 2024

Date of Report as noted in the Report on Compliance: 30 Oct 2024

Section 1: Assessment Information

Instructions for Submission

This Attestation of Compliance (AOC) must be completed as a declaration of the results of the service provider's assessment against the *Payment Card Industry Data Security Standard (PCI DSS) Requirements and Testing Procedures (*"Assessment"). Complete all sections. The service provider is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the entity(ies) to which this AOC will be submitted for reporting and submission procedures.

This AOC reflects the results documented in an associated Report on Compliance (ROC). Associated ROC sections are noted in each AOC Part/Section below.

Capitalized terms used but not otherwise defined in this document have the meanings set forth in the PCI DSS Report on Compliance Template.

Part 1. Contact Information

Part 1a. Assessed Entity (ROC Section 1.1)

Company name:	Worldline Merchant Services
DBA (doing business as):	-
Company mailing address:	1442, Chaussée de Haecht, 1130 Brussels, Belgium
Company main website:	https://www.worldline.com
Company contact name:	Juan José Rabaneda Bueno
Company contact title:	Global Security Assurance Coordinator
Contact phone number:	+34 680 391 961
Contact e-mail address:	juan.rabaneda@worldline.com

Part 1b. Assessor (ROC Section 1.1)

Provide the following information for all assessors involved in the Assessment. If there was no assessor for a given assessor type, enter Not Applicable.

PCI SSC Internal Security Assessor(s)	
ISA name(s):	-
Qualified Security Assessor	
Company name:	usd AG
Company mailing address:	Frankfurter Str. 233, Haus C1, 63263 Neu-Isenburg, Germany
Company website:	https://www.usd.de
Lead Assessor name:	Tobias Weber
Assessor phone number:	+49 6102 8631-325
Assessor e-mail address:	tobias.weber@usd.de
Assessor certificate number:	QSA (204-922)

Part 2. Executive Summary

Part 2a. Scope Verification

Services that were INCLUDED in the scope of the Assessment (select all that apply):

Name of service(s) assessed:	Orange IVR, PVOICE IVR, SIPS, SNCF SIC, Store Acceptance, Xenturion, Ticket Master, OneSource, Order Processing Service (OPS), Tokenization Service, HSM Luna, Online and Offline Payment Connectors, WS2010, Payment Page, Device Rest API, Merchant Batch Processor, Façade API, Tap on Mobile

Type of service(s) assessed:

Hosting Provider:	**Managed Services:**	**Payment Processing:**
☐ Applications / software	☐ Systems security services	☒ POI / 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-hosting services		
☐ Security services		
☐ 3-D Secure Hosting Provider		
☐ Multi-Tenant Service 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): Tokenization		

Note: *These categories are provided for assistance only and are not intended to limit or predetermine an entity's service description. If these categories do not apply to the assessed service, complete "Others." If it is not clear whether a category could apply to the assessed service, consult with the entity(ies) to which this AOC will be submitted.*

Part 2. Executive Summary *(continued)*

Part 2a. Scope Verification *(continued)*

Services that are provided by the service provider but were NOT INCLUDED in the scope of the Assessment (select all that apply):

Name of service(s) not assessed:	None

Type of service(s) not assessed:

Hosting Provider:	**Managed Services:**	**Payment Processing:**
☐ Applications / software	☐ Systems security services	☐ POI / 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-hosting services		
☐ Security services		
☐ 3-D Secure Hosting Provider		
☐ Multi-Tenant Service 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):		

Provide a brief explanation why any checked services were not included in the Assessment:	-

Part 2b. Description of Role with Payment Cards (ROC Section 2.1)

Describe how the business stores, processes, and/or transmits account data.	Acceptance: Payment card transactions originate from POS devices as well as via e-commerce and through connections from processors (card-present, card-not-present transactions). Transactions are received through dedicated connections: • Processors: leased lines or internet via IPsec VPN with strong encryption

	• POS/e-commerce: over direct dial-up, internet protected by strong encryption (TLS 1.2+). Worldline transmits received authorization requests to card acquirers for authorization or to processors/payment card brands for further processing. The transaction data containing PANs and sensitive authentication data is forwarded via VPN or private lines to the card brands and other directly connected parties. Worldline performs data capture from card acceptance devices and processes received financial transactions for clearing and settlement or processes and submits financial transactions to payment card brands for subsequent clearing and settlement. Storage (general description): Worldline stores account data in flat files and databases for further processing as described above. Additionally, cardholder data is stored in log files for reporting, incident management and value-added service provision (such as fraud monitoring, chargeback processing, data warehouse) as well as call recording files (for call center quality monitoring and dispute resolution purpose) encrypted with strong encryption, paper media for chargeback, and call center services provision. All stored cardholder data are protected by applicative, database, file system, disk encryption, and/or compensating controls. Cardholder data are archived on optical disks, on a storage system or as hardcopies. File Transfer (general description): Secure file transfer systems are used to exchange files with cardholder data internally and with brands and customers. Cardholder data are only stored temporarily on this system, which encrypts all data with AES strong cryptography. Worldline is a level 1 service provider with card payment services. Worldline processes debit and credit card transactions from its locations seated in Europe to serve European markets and other geographies such as the US, on behalf of their customers, being merchants, card acquirers and card issuers. Cardholder data are being processed, transmitted and stored during the card payment processing and card issuance as provided services to the Worldline clients. Worldline Merchant Services is made up of the grouping of the legal entities Worldline Sweden AB, Inc, Worldline France and Worldline SA/NV, WL Japan.
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	N/A

Describe system components that could impact the security of account data.	Payment applications

Part 2. Executive Summary *(continued)*

Part 2c. Description of Payment Card 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 POI devices, databases, web servers, etc., and any other necessary payment components, as applicable.* • *System components that could impact the security of account data.*	The assessed environment consists of the applications used to operate the assessed services of Worldline Merchant Services, including the underlying network and infrastructure run by Worldline Europe Central Hosting Provider.
Indicate whether the environment includes segmentation to reduce the scope of the Assessment. (Refer to the "Segmentation" section of PCI DSS for guidance on segmentation)	☒ Yes ☐ No

Part 2d. In-Scope Locations/Facilities (ROC Section 4.6)

List all types of physical locations/facilities (for example, corporate offices, data centers, call centers and mail rooms) in scope for this Assessment.

Facility Type	Total Number of Locations (How many locations of this type are in scope)	Location(s) of Facility (city, country)
Example: Data centers	*3*	*Boston, MA, USA*
Office	1	Bezons, France
Office	1	Blois, France
Office + data center	1	Seclin La Pointe, France
Data center	1	Seclin Dassault, France
Office + data center	1	Vendôme, France
Office	1	Stockholm, Sweden
Data center	1	Bromma, Sweden
Data center	1	Sköndal, Sweden
Office + data center	1	Brussels, Belgium
Office	1	São Paulo, Brazil
Office	1	Tokyo, Japan

Part 2. Executive Summary *(continued)*

Part 2e. PCI SSC Validated Products and Solutions (ROC Section 3.3)

Does the entity use any item identified on any PCI SSC Lists of Validated Products and Solutions♦?

☐ Yes ☒ No

Provide the following information regarding each item the entity uses from PCI SSC's Lists of Validated Products and Solutions:

Name of PCI SSC-validated Product or Solution	Version of Product or Solution	PCI SSC Standard to which Product or Solution Was Validated	PCI SSC Listing Reference Number	Expiry Date of Listing
-	-	-	-	-

♦ For purposes of this document, "Lists of Validated Products and Solutions" means the lists of validated products, solutions, and/or components appearing on the PCI SSC website (www.pcisecuritystandards.org)—for example, 3DS Software Development Kits, Approved PTS Devices, Validated Payment Software, Payment Applications (PA-DSS), Point to Point Encryption (P2PE) solutions, Software-Based PIN Entry on COTS (SPoC) solutions, and Contactless Payments on COTS (CPoC) solutions.

Part 2f. Third-Party Service Providers **(ROC Section 4.4)**	
For the services being validated, does the entity have relationships with one or more third-party service providers that:	
• Store, process, or transmit account data on the entity's behalf (for example, payment gateways, payment processors, payment service providers (PSPs, and off-site storage))	☒ Yes ☐ No
• Manage system components included in the entity's Assessment (for example, via network security control services, anti-malware services, security incident and event management (SIEM), contact and call centers, web-hosting companies, and IaaS, PaaS, SaaS, and FaaS cloud providers)	☒ Yes ☐ No
• Could impact the security of the entity's CDE (for example, vendors providing support via remote access, and/or bespoke software developers).	☒ Yes ☐ No

If Yes:

Name of Service Provider:	**Description of Services Provided:**
Worldline Europe Central Hosting Provider	Hosting, System Security Services, IT Support, Network Provider, Infrastructure Service, File Transfer Service, HSM and Key Management Services, Risk Management, Vulnerability Management, Security Incident Management, HR Management, Security Awareness Training, Secure Coding Training, Media Handling
Equinix, Inc.	Housing
Amazon Web Services, Inc.	Cloud services
ACI Worldwide (Germany) GmbH – Pay.On	Payment Processing
ACI Worldwide Corp and Affiliates	Fraud and Chargeback services

Note: *Requirement 12.8 applies to all entities in this list.*

Part 2. Executive Summary *(continued)*

Part 2g. Summary of Assessment (ROC Section 1.8.1)

Indicate below all responses provided within each principal PCI DSS requirement.

For all requirements identified as either "Not Applicable" or "Not Tested," complete the "Justification for Approach" table below.

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: Orange IVR, PVOICE IVR, SIPS, SNCF SIC, Store Acceptance, Xenturion, Ticket Master, OneSource, Order Processing Service(OPS), Tokenization Service, HSM Luna, Online and Offline Payment Connectors, WS2010, Payment Page, Device Rest API, Merchant Batch Processor, Tap on Mobile

PCI DSS Requirement	Requirement Finding More than one response may be selected for a given requirement. Indicate all responses that apply.				Select If Below Method(s) Was Used	
	In Place	Not Applicable	Not Tested	Not in Place	Customized Approach	Compensating Controls
Requirement 1:	☒	☐	☐	☐	☐	☐
Requirement 2:	☒	☐	☐	☐	☐	☐
Requirement 3:	☒	☒	☐	☐	☐	☐
Requirement 4:	☒	☒	☐	☐	☐	☐
Requirement 5:	☒	☐	☐	☐	☐	☐
Requirement 6:	☒	☐	☐	☐	☐	☐
Requirement 7:	☒	☒	☐	☐	☐	☐
Requirement 8:	☒	☒	☐	☐	☐	☐
Requirement 9:	☒	☐	☐	☐	☐	☐
Requirement 10:	☒	☐	☐	☐	☐	☐
Requirement 11:	☒	☒	☐	☐	☐	☐
Requirement 12:	☒	☒	☐	☐	☐	☐
Appendix A1:	☐	☒	☐	☐	☐	☐
Appendix A2:	☐	☒	☐	☐	☐	☐

Justification for Approach

For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.	3.3.2: SAD is never stored electronically. 3.3.3, 3.4.2, 4.2.1.1, 7.2.4, 7.2.5, 8.4.2, 8.6.1 – 8.6.3, 11.4.7, 11.6.1, 12.3.1, 12.3.3, 12.3.4, 12.5.2.1, 12.5.3, 12.6.2, 12.6.3.1, 12.6.3.2, 12.10.4.1, 12.10.7: Requirement is best practice until 31 Mar 2025. 4.2.1.2: No wireless networks in use that transport PAN data or that are connected to the CDE. 4.2.2: No end user messaging technologies are in scope of this assessment 8.2.3: The assessed entity is not a service provider with access to customer premises. 8.2.7: There are no third parties with access to or accounts on the systems or applications of the assessed entity. 12.3.2: The entity does not use the customized approach for any of the applicable PCI DSS requirements. Req. A1: The assessed entity is not a multi-tenant service provider. Req. A2: No early SSL/TLS POS devices.
For any Not Tested responses, identify which sub-requirements were not tested and the reason.	none

Section 2 Report on Compliance

(**ROC Sections 1.2 and 1.3.2**)

Date Assessment began: ***Note:*** *This is the first date that evidence was gathered, or observations were made.*			01 May 2024
Date Assessment ended: ***Note:*** *This is the last date that evidence was gathered, or observations were made.*			30 Oct 2024
Were any requirements in the ROC unable to be met due to a legal constraint?			☐ Yes ☒ No
Were any testing activities performed remotely? If yes, for each testing activity below, indicate whether remote assessment activities were performed:			☒ Yes ☐ No
• Examine documentation	☒ Yes	☐ No	
• Interview personnel	☒ Yes	☐ No	
• Examine/observe live data	☒ Yes	☐ No	
• Observe process being performed	☒ Yes	☐ No	
• Observe physical environment	☐ Yes	☒ No	
• Interactive testing	☒ Yes	☐ No	
• Other:	☐ Yes	☒ No	

Section 3 Validation and Attestation Details

Part 3. PCI DSS Validation (ROC Section 1.7)

This AOC is based on results noted in the ROC dated 30 Oct 2024.

Indicate below whether a full or partial PCI DSS assessment was completed:

☒ **Full Assessment** – All requirements have been assessed and therefore no requirements were marked as Not Tested in the ROC.

☐ **Partial Assessment** – One or more requirements have not been assessed and were therefore marked as Not Tested in the ROC. Any requirement not assessed is noted as Not Tested in Part 2g above.

Based on the results documented in the ROC noted above, each signatory identified in any of Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document *(select one)**:***

☒	**Compliant:** All sections of the PCI DSS ROC are complete, and all assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall **COMPLIANT** rating; thereby Worldline Merchant Services has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above.
☐	**Non-Compliant:** Not all sections of the PCI DSS ROC are complete, or one or more requirements are marked as Not in Place, resulting in an overall **NON-COMPLIANT** rating; thereby *(Service Provider Company Name)* has not demonstrated compliance with PCI DSS requirements. **Target Date** for Compliance: *YYYY-MM-DD* An entity submitting this form with a Non-Compliant status may be required to complete the Action Plan in Part 4 of this document. Confirm with the entity to which this AOC will be submitted before completing Part 4.
☐	**Compliant but with Legal exception:** One or more assessed requirements in the ROC are marked as Not in Place due to a legal restriction that prevents the requirement from being met and all other assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall **COMPLIANT BUT WITH LEGAL EXCEPTION** rating; thereby *(Service Provider Company Name)* has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above or as Not in Place due to a legal restriction. This option requires additional review from the entity to which this AOC will be submitted. *If selected, complete the following:*

Affected Requirement	Details of how legal constraint prevents requirement from being met

Part 3. PCI DSS Validation *(continued)*

Part 3a. Service Provider Acknowledgement

Signatory(s) confirms:
(Select all that apply)

☒	The ROC was completed according to *PCI DSS*, Version 4.0 and was completed according to the instructions therein.
☒	All information within the above-referenced ROC and in this attestation fairly represents the results of the Assessment in all material respects.
☒	PCI DSS controls will be maintained at all times, as applicable to the entity's environment.

Part 3b. Service Provider Attestation

Ondertekend door:
Geert van de Wielle
C37A810CD86148F...

Signature of Service Provider Executive Officer ↗	Date: 30 Oct 2024
Service Provider Executive Officer Name: Geert van de Wielle	Title: Head of Security / CISO

Part 3c. Qualified Security Assessor (QSA) Acknowledgement

If a QSA was involved or assisted with this Assessment, indicate the role performed:	☒ QSA performed testing procedures.
	☐ QSA provided other assistance. If selected, describe all role(s) performed: -

DocuSigned by:
T. Weber
1D3519071EC24C8...

Signature of Lead QSA ↗	Date: 30 Oct 2024
Lead QSA Name: Tobias Weber	

DocuSigned by:
Torsten Schlotmann
9366AA034EE04CE...

Signature of Duly Authorized Officer of QSA Company ↗	Date: 30 Oct 2024
Duly Authorized Officer Name: Torsten Schlotmann	QSA Company: usd AG

Part 3d. PCI SSC Internal Security Assessor (ISA) Involvement

If an ISA(s) was involved or assisted with this Assessment, indicate the role performed:	☐ ISA(s) performed testing procedures.
	☐ ISA(s) provided other assistance. If selected, describe all role(s) performed: -

Part 4. Action Plan for Non-Compliant Requirements

Only complete Part 4 upon request of the entity to which this AOC will be submitted, and only if the Assessment has Non-Compliant results noted in Section 3.

If asked to complete this section, select the appropriate response for "Compliant to PCI DSS Requirements" for each requirement below. For any "No" responses, include the date the entity expects to be compliant with the requirement and provide a brief description of the actions being taken to meet the requirement.

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 network security controls	☐	☐	
2	Apply secure configurations to all system components	☐	☐	
3	Protect stored account data	☐	☐	
4	Protect cardholder data with strong cryptography during transmission over open, public networks	☐	☐	
5	Protect all systems and networks from malicious software	☐	☐	
6	Develop and maintain secure systems and software	☐	☐	
7	Restrict access to system components and cardholder data by business need to know	☐	☐	
8	Identify users and authenticate access to system components	☐	☐	
9	Restrict physical access to cardholder data	☐	☐	
10	Log and monitor all access to system components and cardholder data	☐	☐	
11	Test security systems and networks regularly	☐	☐	
12	Support information security with organizational policies and programs	☐	☐	
Appendix A1	Additional PCI DSS Requirements for Multi-Tenant Service Providers	☐	☐	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	☐	☐