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:	Visa Europe Limited	DBA (doing business as):	Visa Europe		
Contact Name:	Jason Miles-Wynter-Pink	Title:	Lead Internal Security Assessor		
Telephone:	+44 (0) 207 795 5158	E-mail:	mileswpj@visa.com		
Business Address:	1 Sheldon Square	City:	London		
State/Province:	Not Applicable	Country:	United Kingdom	Zip:	W26TT
URL:	www.visa.co.uk				

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

Company Name:	Trustwave				
Lead QSA Contact Name:	Fotios Tsifountidis	Title:	Security Consultant - QSA		
Telephone:	+44 (0) 845-456-9611	E-mail:	ftsifountidis@trustwave.com		
Business Address:	Trustwave	City:	London		
State/Province:	Not Applicable	Country:	United Kingdom	Zip:	SE1 7SP
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:	Payment Processing	
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): Manual entry - card not present
☒ 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.*

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:	Internet/e-commerce, MOTO/call center, ATM, Back-Office Services, Billing Management, Fraud and Chargeback, Prepaid Services, Records Management, Tax/Government Payments, Tokenization

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): Tokenization

Provide a brief explanation why any checked services were not included in the assessment:	All services listed above are either managed or performed by Visa Inc. with systems, applications and solutions hosted in environments outside the United Kingdom, UK (i.e. in OCC, OCE, OCW and KC2 Datacentres in US and Singapore) not controlled or managed by Visa Europe. These environments, processes, services and solutions as well as their connections, security controls and all protection aspects of cardholder data (in transit/at rest) are covered in a separate PCI DSS Visa Inc. assessment with their AoC v3.2.1 dated 04/06/2020.

Part 2b. Description of Payment Card Business

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	Visa Europe is a Level 1 Service Provider engaged in operating a retail electronic payments network. Visa Europe. accepts card-present, card-not-present transaction data in the course of conducting their business. Visa Europe transmits cardholder data to payment processors as part of the authorization process. In the settlement process, Visa Europe processes cardholder data to payment processors. Visa Europe stores cardholder data as part of its business processes. Cardholder data is stored encrypted with strong encryption (AES 128/256) or truncated with the first 6/4 and last 4, or last 4 digits only of the PAN visible. All data storage, processing and transmission is in secure networks located within its main processing datacenter in Basingstoke (OCB). Visa Europe maintains connections with approximately 500 entities within Europe (member banks and processors). Visa Europe transmits cardholder data using secure protocols primarily over private MPLS networks using AES 128 and RSA 2048bits but also over the internet utilizing HTTPS TLS 1.2 AES 256-bits. Visa Europe is involved in the card issuing process, in which cardholder data is stored in the databases encrypted using AES 128/256 bits.
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):
Example: Retail outlets	*3*	*Boston, MA, USA*
Headquarters and Datacentre	1	London, United Kingdom
Main Datacentre (OCB)	1	Basingstoke, United Kingdom
Offices and Datacentre	1	Reading, United Kingdom

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)
Not Applicable	Not Applicable	Not Applicable	☐ 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 Visa Europe networks reviewed and included in-scope for the PCI assessment were the Commercial, Corporate and Extranet Networks. The networks are further broken into Perimeter, Business and Restricted zones which are segregated using Cisco ASA, Palo Alto and Checkpoint firewalls. Visa Europe is one of the main processing networks to which all-major processors connect. Relationships with all processors and clients that connect to the Visa Europe and amount to approximately 500 entities. Connections between Visa Europe and their clients are primarily via private MPLS links using AES 128 and RSA 2048bits, while a subset of connections is via internet utilizing HTTPS TLS 1.2 AES 256-bits. . The critical and CDE supporting systems included in the assessment were: • Firewalls/Routers/Switches • Middleware and mainframe that support payment processing • Servers to support the receipt of cardholder data and the transmission of cardholder data to processors • Hardware Security Solutions (HSM) for key management and key management functionality • Intrusion Detection Systems • Personal Firewalls • Remote Access Software • Anti-Virus software • Log aggregation using centralized monitoring solutions • File integrity monitoring

	- Change Management solutions - Data Loss Prevention (DLP) solutions - Virtualization solutions - Application code scanning solutions - Wireless controllers - Web application firewalls, web monitoring solutions, content filtering solutions - Critical applications including VEPPS, DRP, VEF, VAU, VIP

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:**
Collinson Group	Concierge/Airport lounge payments
Carlson Wagonlit Travel	Corporate travel booking system
Iron Mountain	Offsite media storage
Optile	Merchant marketplace service offerings

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:	Payment Processing

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:	□	☒	□	2.2.3 was not applicable as Visa Europe does not have any insecure services, protocols or daemons in their environment. 2.6 was not applicable as Visa Europe is not a shared hosting provider
Requirement 3:	□	☒	□	3.6.6 was not applicable as Visa Europe does not engage in manual clear text key management.
Requirement 4:	☒	□	□	
Requirement 5:	☒	□	□	
Requirement 6:	☒	□	□	
Requirement 7:	☒	□	□	
Requirement 8:	□	☒	□	8.1.5 was not applicable as Visa Europe does not provide vendors with access. 8.5.1 was not applicable as Visa Europe has no remote access to customer managed systems/sites.
Requirement 9:	□	☒	□	9.9 was not applicable as Visa Europe does not have any devices with direct physical interaction with cardholder data.

				9.9.1 was not applicable as Visa Europe does not have any devices with direct physical interaction with cardholder data. 9.9.2 was not applicable as Visa Europe does not have any devices with direct physical interaction with cardholder data. 9.9.3 was not applicable as Visa Europe does not have any devices with direct physical interaction with cardholder data.
Requirement 10:	☒	□	□	
Requirement 11:	□	☒	□	11.3.4 was not applicable as Visa Europe does not isolate their environment. The entire environment was reviewed as part of the assessment. 11.3.4.1 was not applicable as Visa Europe does not isolate their environment. The entire environment was reviewed as part of the assessment.
Requirement 12:	☒	□	□	
Appendix A1:	□	□	☒	Not applicable. Visa Europe is not a shared hosting provider
Appendix A2:	□	□	☒	Not applicable. Visa Europe does not have POS POI terminals (and the SSL/TLS termination points to which they connect) use SSL and/or early TLS.

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:	*August 31, 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

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in the ROC dated *August 31, 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 *Visa Europe Limited* 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 *Qualys*

[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

Ilaiy Elangovan

Signature of Service Provider Executive Officer ↑	*Date:* 9/1/2020
Service Provider Executive Officer Name: Ilaiy Elangovan	*Title:* Chief Information Security Officer

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

If a QSA was involved or assisted with this assessment, describe the role performed:	Fotios Tsifountidis QSA – Reviewed evidence, performed the assessment and Visa Europe interviews, participated in Visa Inc. interviews and completed the Report on Compliance for Visa Europe. Pablo Gomezsolis QSA – Conducted the Visa Inc. interviews and Visa Inc. assessment.

FTsifountidis

Signature of Duly Authorized Officer of QSA Company ↑	*Date: August 31, 2020*
Duly Authorized Officer Name: Fotios Tsifountidis	*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:	Jason Miles-Wynter-Pink - Lead ISA. Reviewed, gathered, provided supporting evidence and managed the assessment for Visa Europe.

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	☒	□	