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:	GlobalCollect Services BV		DBA (doing business as):	GlobalCollect Services USA; Global Collect Services, Ingenico ePayments	
Contact Name:	Karel Koster		Title:	Head of Information Security Management	
Telephone:	+31 (0) 23 567 1500		E-mail:	karel.koster@ingenico.com	
Business Address:	Planetenweg 43-59		City:	Hoofddorp	
State/Province:	Not applicable	Country:	The Netherlands	Zip:	2132 HM
URL:	http://www.ingenico.com/epayments				

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

Company Name:	Trustwave				
Lead QSA Contact Name:	Bernhard Weichs		Title:	Security Consultant	
Telephone:	+44 (0) 845 456 9611		E-mail:	bweichs@trustwave.com	
Business Address:	Westminster Tower 3 Albert Embankment		City:	London	
State/Province:	Not applicable	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:	Internet eCommerce payment processing, fraud and chargeback services, hardware and infrastructure hosting, managed services, software development

Type of service(s) 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): Software Development

***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):

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.	GlobalCollect Services BV is a level 1 payment service provider that processes card-not-present credit card transactions received via its WebCollect and Ingenico Connect payment applications. These applications provide integrated APIs or hosted redirect payment pages to their merchants. The web servers receive cardholder data including PAN, cardholder name, expiration date and card security numbers (CVV2/CVC2/CID/CAV2) via HTTPS connections and forwards authorization request to their service providers and upload processors via VPN tunnels or private lines. GlobalCollect Services BV stores cardholder data for settlement, chargeback and reporting purposes.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	GlobalCollect Services BV offers hardware and network hosting as well as managed services and software development services for other PCI compliant Ingenico Group members. This includes the hosting and management of an e-Commmerce payment platform and corresponding network and security infrastructure for the Ingenico Group members Ogone GmbH. This payment platform is in scope and subject to the PCI DSS assessment of Ogone GmbH, but the hardware is hosted and the systems are managed on an operating system level by GlobalCollect Service BV. All applicable PCI DSS controls on operating system level are managed by GlobalCollect Services BV. GlobalCollect Services BV further provides software development of out-of-the-box software packages and plug-ins for Ingenico Group applications.

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):
Head office	1	Planetenweg 43-59, Hoofddorp 2132 HM, The Netherlands
Data Center	1	Equinix: 4 Luttenbergerweg, 1101 EC Amsterdam-Zuidoost, The Netherlands
Data Center	1	Verizon: 99 Northeast 8th Street, Miami, Florida 33132, United States of America

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)
WebCollect	7.7.3	GlobalCollect Services BV	☐ Yes ☒ No	Not applicable
Ingenico Connect	20170426.02	Ingenico Payment Services LLC	☐ 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 the entire PCI DSS scope and all involved systems and components via samples of: ▪ Connections into the CDE o HTTPS connections using TLS1.0/1.1/1.2 and AES 128-bit or stronger keys ▪ Connections out of the CDE o HTTPS connections using TLS1.2 and AES 128-bit or bigger keys o IPSEC VPN o Private lines ▪ Critical system components within the CDE: o Firewalls o Networking components (Switches, Routers, Load Balancers) o Security appliances (SIEM, FIM, IDS) o Webservers o Databases o Applications and application servers o Logical access controls o Physical access controls
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:**
Atos	Transaction Processing
Barclays	Transaction Processing
Braspag Brazil	Transaction Processing
Braspag Colombia	Transaction Processing
Braspag Mexico	Transaction Processing
Catella	Transaction Processing
CBA (commweb)	Transaction Processing
CobreBem Chile	Transaction Processing
CT-Payment	Transaction Processing
Cybersource	Transaction Processing
Elavon (EuroConex)	Transaction Processing
First Data	Transaction Processing
HSBC	Transaction Processing
INICIS (Korea)	Transaction Processing
IPS (China)	Transaction Processing
It Recycling	Media Destruction
Little	Transaction Processing
Merchant Solutions	Transaction Processing
PayVision	Transaction Processing
Realex Payments	Transaction Processing
Retail Decisions	Fraud Checks
RS2 Bankworks	Transaction Processing
SEB Euroline (Bambora)	Transaction Processing

Societe Generale	Transaction Processing
Sub1 Argentina	Transaction Processing
Wells Fargo	Transaction Processing
Western Union	Transaction Processing
CVOkay	HR Background Checks

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:	Internet eCommerce payment processing, fraud and chargeback services, hardware and infrastructure hosting, managed services, software development

	Details of Requirements Assessed			
PCI DSS Requirement	**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: GCS does neither uses wireless networks to transmit CHD, nor do they have wireless networks connected to their CDE.
Requirement 3:	☐	☒	☐	Req. 3.4.1: GCS does not use disk encryption to protect stored CHD. Req. 3.5.1: Not in place yet (Best practice until January 31st, 2018) Req. 3.6: GCS does not share cryptographic keys with any third parties. Req. 3.6.6: GCS does not perform any clear-text key-management operations.
Requirement 4:	☐	☒	☐	Req. 4.1.1: GCS does neither uses wireless networks to transmit CHD, nor do they have wireless networks connected to their CDE.
Requirement 5:	☒	☐	☐	
Requirement 6:	☒	☐	☐	
Requirement 7:	☒	☐	☐	

Requirement 8:	☐	☒	☐	Req. 8.1.5: GCS does not allow third parties to connect into their environment. Req. 8.3.1: Not in place yet (Best practice until January 31st, 2018) Req. 8.5.1: GCS does not have access to their customer's premises.
Requirement 9:	☐	☒	☐	Req. 9.5.1: GCS does not use removable backup media. Req. 9.6: GCS does not distribute any media. Req. 9.6.2: GCS does not distribute any media. Req. 9.6.3: GCS does not distribute any media. Req. 9.9: GCS does not maintain any POS/POI devices. Req. 9.9.1: GCS does not maintain any POS/POI devices. Req. 9.9.2: GCS does not maintain any POS/POI devices. Req. 9.9.3: GCS does not maintain any POS/POI devices.
Requirement 10:	☐	☒	☐	Req. 10.8: Not in place yet (Best practice until January 31st, 2018) Req. 10.8.1: Not in place yet (Best practice until January 31st, 2018)
Requirement 11:	☐	☒	☐	Req. 11.3.4.1: Not in place yet (Best practice until January 31st, 2018)
Requirement 12:	☐	☒	☐	Req. 12.3.9: GCS does not allow third parties to connect into their environment. Req. 12.4.1: Not in place yet (Best practice until January 31st, 2018) Req. 12.11: Not in place yet (Best practice until January 31st, 2018) Req. 12.11.1: Not in place yet (Best practice until January 31st, 2018)
Appendix A1:	☐	☐	☒	GCS is not a shared hosting provider
Appendix A2:	☐	☒	☐	A 2.1: GCS does not maintain any POS/POI devices

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 11, 2017*	
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 11, 2017.*

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 *GlobalCollect Services BV* 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 12, 2017
Service Provider Executive Officer Name: Karel Koster	*Title:* Head of Information Security

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

If a QSA was involved or assisted with this assessment, describe the role performed:	Bernhard Weichs – Lead QSA ▪ Performed the assessment ▪ Reviewed documentation and compensating controls ▪ Prepared the Report on Compliance ▪ Prepared the Attestation of Compliance

Signature of Duly Authorized Officer of QSA Company ↑	*Date: September 11, 2017*
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	☒	☐	