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:	Global Collect Services B.V.		DBA (doing business as):	Global Collect Services USA, Global Collect Services, Ingenico ePayments	
Contact Name:	Geert van de Wielle		Title:	Chief Information Security Officer	
Telephone:	+31 (0) 23 567 1500		E-mail:	ICT.Security.Management@epay.ingenico.com	
Business Address:	Neptunesstraat 41		City:	Hoofddorp	
State/Province:	Not applicable	Country:	The Netherlands	Zip:	2132 JA
URL:	www.globalcollect.com				

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

Company Name:	SecureTrust				
Lead QSA Contact Name:	Bernhard Reus		Title:	Security Consultant	
Telephone:	+1 (312) 873-7500		E-mail:	breus@securetrust.com	
Business Address:	70 W Madison St, Ste 600		City:	Chicago	
State/Province:	Illinois	Country:	United States of America	Zip:	60602
URL:	www.securetrust.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 Gateway/Switch, Fraud and Chargeback, Clearing and Settlement, Back-Office Services, Merchant Services	
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):		

***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.	Global Collect Services B.V. (GCS) provides merchants with an integrated API or a redirect payment page to transfer their payment requests. The web servers of GCS receive the CHD including PAN, cardholder name, expiration date, and card security codes via a HTTPS (TLS v1.2 with AES 128-bit or AES 256-bit) connection. The received CHD is forwarded to external upload processors to authorize transactions. During the upload, the CHD (PAN, expiration date, and card security codes) is protected by HTTPS (TLS v1.2, AES 128-bit or AES 256-bit), IPSEC based VPN (AES 128-bit or AES 256-bit), SFTP (SSHv2 with PGP encrypted (RSA 2048-bit or AES 256-bit) files) or encrypted with the processor's own AES 256-bit certificates. In specific cases, the received PAN is forwarded to the service provider Axis and their tokenization engine service via TLS v1.3 (AES 256-bit). The returned Token will be used for all further internal processing in the BSP application and after processing stored instead of encrypted PAN. GCS stores CHD (PAN, expiration date and cardholder name): For settlement, dispute handling, fraud detection and reporting purposes, in an Oracle database using AES 256-bit, salted SHA 256 hash and truncation (no digits saved, all 16 digits are changed to asterisks). Cardholder data and sensitive authentication data is held in a temporary table during the entire authorization process on the front-office Oracle database. In import/export files for transaction processing as well as clearing files and customer reports (AES 256-bit, truncation and masked (last 4 digits)) for settlement and reporting purposes to external processors. GCS's payment application produces truncated PAN (first 6 digits) of the PAN in the Ingress database. For settlement, GCS sends clearing files to defined external processors. The following card brands are accepted by GCS: Visa MasterCard

	American Express Discover JCB Diners Club Carte Bancaire Union Pay
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. GCS is not otherwise involved nor can 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):
Data Center	4	Miami, Florida, United States of America Amsterdam-Zuidoost, The Netherlands Paris, France Magny-les-Hameaux, France
Headquarter	1	Hoofddorp, The Netherlands
Dispute Management center	1	Hoofddorp, The Netherlands

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)
WDL (WebCollect)	20.02.0.0	GCS	☐ Yes ☒ No	Not applicable
WPL (WebCollect)	20.01.0.0	GCS	☐ Yes ☒ No	Not applicable
ORB (WebCollect)	20.1.0.0	GCS	☐ Yes ☒ No	Not applicable
HPP (WebCollect)	18.9.0.0	GCS	☐ Yes ☒ No	Not applicable
CCA (WebCollect)	19.1.0.00	GCS	☐ Yes ☒ No	Not applicable
EPB (WebCollect)	19.1.2.0	GCS	☐ Yes ☒ No	Not applicable
EMA (WebCollect)	1903.02.00 (18.6)	GCS	☐ Yes ☒ No	Not applicable
WPC (WebCollect)	1904.03.00	GCS	☐ Yes ☒ No	Not applicable

Ingenico Connect	20190409	GCS	☐ Yes ☒ No	Not applicable
Ogone Connect	20190409	GCS	☐ Yes ☒ No	Not applicable
ah-bambora-service-app	2002.00.00	GCS	☐ Yes ☒ No	Not applicable
ah-rbs-client-app	1910.00.00	GCS	☐ Yes ☒ No	Not applicable
aibapacs30-service-app	1908.00.00	GCS	☐ Yes ☒ No	Not applicable
aib-service-app	1908.00.00	GCS	☐ Yes ☒ No	Not applicable
amex-service-app	2004.00.00	GCS	☐ Yes ☒ No	Not applicable
atos-ws-service-app	18.6.0.0	GCS	☐ Yes ☒ No	Not applicable
barclays-iso-service-app	2004.00.00	GCS	☐ Yes ☒ No	Not applicable
barclays-service-app	2004.00.00	GCS	☐ Yes ☒ No	Not applicable
braspag-cc-service-app	18.7.0.0	GCS	☐ Yes ☒ No	Not applicable
cba-service-app	18.10.0.0	GCS	☐ Yes ☒ No	Not applicable
ecvv-service-app	18.17.0.0	GCS	☐ Yes ☒ No	Not applicable
elavon-service-app	18.7.0.0	GCS	☐ Yes ☒ No	Not applicable
firstdata-service-app	18.6.0.1	GCS	☐ Yes ☒ No	Not applicable
iin-service-app	1908.00.00	GCS	☐ Yes ☒ No	Not applicable
jcb-service-app	18.6.0.9	GCS	☐ Yes ☒ No	Not applicable
litle-service-app	18.10.0.0	GCS	☐ Yes ☒ No	Not applicable
mpi-service-app	1907.03.00	GCS	☐ Yes ☒ No	Not applicable
payment-engine-app	2004.02.00	GCS	☐ Yes ☒ No	Not applicable
payment-management-app	18.12.0.0	GCS	☐ Yes ☒ No	Not applicable
realex-service-app	18.5.5.2	GCS	☐ Yes ☒ No	Not applicable
sub1-cc-service-app	2001.00.00	GCS	☐ Yes ☒ No	Not applicable
bnp-offline-app	2105.00.00	GCS	☐ Yes ☒ No	Not applicable
sberbank-offline-app	2103.03.00	GCS	☐ Yes ☒ No	Not applicable
vtb-offline-app	2104.00.00	GCS	☐ Yes ☒ No	Not applicable
alfabank-offline-app	2103.01.00	GCS	☐ Yes ☒ No	Not applicable
fuiou-offline-app	2006.00.00	GCS	☐ Yes ☒ No	Not applicable

boleto-offline-app	2004.09.00	GCS	☐ Yes ☒ No	Not applicable
molpay-realtime-offline-app	2007.01.00	GCS	☐ Yes ☒ No	Not applicable
sofort-offline-app	2007.01.00	GCS	☐ Yes ☒ No	Not applicable
crypto-service-app	2106.01.00	GCS	☐ Yes ☒ No	Not applicable
wcm-web-app	2104.00.00	GCS	☐ Yes ☒ No	Not applicable
configuration-service-app	2105.02.00	GCS	☐ Yes ☒ No	Not applicable
unionpay-service-app	2010.00.00	GCS	☐ Yes ☒ No	Not applicable
fraud-fraugster-adaptor-app	1905.00.00	GCS	☐ Yes ☒ No	Not applicable
fraugster-status-service-app	1905.00.00	GCS	☐ Yes ☒ No	Not applicable
retaildecisions-service-app	18.17.0.0	GCS	☐ Yes ☒ No	Not applicable
CCP	4.0	GCS	☐ Yes ☒ No	Not applicable
BSP	2.0.9-R38.2	GCS	☐ Yes ☒ No	Not applicable
DMA	4.036.00	GCS	☐ 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, all involved systems and components: ▪ Connections into the CDE o HTTPS connections using TLS v1.2 o sFTP connections (with strong encryption) ▪ Connections out of the CDE o HTTPS connections using TLS v1.2 o HTTPS connections using TLS v1.3 o sFTP connection (with strong encryption) ▪ IPSEC VPN (with strong encryption)Critical system components within the CDE o GCS Payment Applications o Databases

	○ Operating Systems ○ Network Devices ○ Security Devices ○ Virtualization Technologies ○ File-Integrity Monitoring ○ Anti-Virus ○ Intrusion Detection System ○ Web-Application Firewall ○ Storage Area Network ○ Web Applications ○ Key Management ○ Crypto Processing Devices ○ Wireless Scanning ○ Administrative Laptops ○ Console Firmware ○ Log Management ○ Vulnerability Management
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:**
Equinix EMEA	Co-location hosting
Equinix Americas	Co-location hosting
Telehouse	Co-location hosting
Fraugster	Fraud detection
ACI Worldwide (Formerly Retail Decision)	Fraud detection
Aquire HUB is under Axis	Transmission to acquirer networks
Axis	Tokenization
Okta	MFA Solution

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 Gateway/Switch, Fraud and Chargeback, Clearing and Settlement, Back-Office Services, Merchant Services

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:	☐	☒	☐	Req. 1.2.3: GCS does not maintain wireless network in scope of PCI DSS
Requirement 2:	☐	☒	☐	Req. 2.1.1: GCS does not use wireless networks to transmit CHD, nor do they have wireless networks connected to the CDE Req. 2.2.3: GCS does not use any insecure services, daemons or protocols Req. 2.6: GCS is not a shared hosting provider
Requirement 3:	☐	☒	☐	Req. 3.4.1: GCS does not use disk encryption to protect stored CHD Req. 3.6: GCS does not share cryptographic keys with any third parties Req. 3.6.2: GCS does not distribute cryptographic keys Req. 3.6.6: GCS does not perform clear-text key-management operations
Requirement 4:	☐	☒	☐	Req. 4.1.1: GCS does not use wireless networks to transmit CHD, nor do they have wireless networks connected to the CDE
Requirement 5:	☐	☒	☐	Req. 5.1.2: GCS deploys anti-virus software to all systems

Requirement 6:	☐	☒	☐	Req. 6.4.6: GCS did not perform significant changes to their environment
Requirement 7:	☒	☐	☐	
Requirement 8:	☐	☒	☐	Req. 8.1.5: GCS does not allow third parties to connect into their environment Req. 8.5.1: GCS does not have access to their customer's premises
Requirement 9:	☐	☒	☐	Req. 9.5.1: GCS does not use removeable backup media Req. 9.6.2: GCS does not distribute any media Req. 9.6.3: GCS does not distribute any media Req. 9.7.1: GCS does not use removeable media Req. 9.8.1: GCS does not use hard-copy 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:	☒	☐	☐	
Requirement 11:	☐	☒	☐	Req. 11.1.1: GCS does not maintain wireless network in scope of PCI DSS Req. 11.2.3: GCS did not perform significant changes to their environment
Requirement 12:	☐	☒	☐	Req. 12.3.9: GCS does not allow third parties to connect into their environment
Appendix A1:	☐	☐	☒	A1: GCS is not a shared hosting provider
Appendix A2:	☐	☐	☒	A2.1: GCS does not maintain any POS/POI devices A2.2: GCS does not use SSL or early TLS versions

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 7, 2021*	
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 7, 2021.*

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 *Global Collect Services B.V.* 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 *SecureTrust*

[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:* 08. 10. 2021
Service Provider Executive Officer Name: VAN DE WIELE Geert	*Title:* CISO

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

If a QSA was involved or assisted with this assessment, describe the role performed:	Bernhard Reus – Lead QSA • System Tests • Evidence Review • Documentation Review • Process Review • Preparation of Report on Compliance • Preparation of Attestation of Compliance

Signature of Duly Authorized Officer of QSA Company	*Date:* October 7, 2021
Duly Authorized Officer Name: Bernhard Reus	*QSA Company:* SecureTrust

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	☒	☐	