Payment Card Industry
Data Security Standard

Attestation of Compliance for Report on Compliance – Service Providers

Version 4.0.1

Publication Date: August 2024

PCI DSS v4.0.1 Attestation of Compliance for Report on Compliance – Service Providers

Entity Name: Trust Payments (UK) Ltd (formerly Secure Trading Limited)

Date of Report as noted in the Report on Compliance: 2025-03-28

Date Assessment Ended: 2025-03-27

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:	Trust Payments (UK) Ltd (formerly Secure Trading Limited)
DBA (doing business as):	Trust Payments
Company mailing address:	1 Royal Exchange, Royal Exchange Avenue, London, EC3V 3DG, United Kingdom
Company main website:	https://www.trustpayments.com/
Company contact name:	Dariusz Synowiec
Company contact title:	Information Security Officer
Contact phone number:	01248 672000
Contact e-mail address:	dariusz.synowiec@trustpayments.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):	N/a
Qualified Security Assessor	
Company name:	OmniCyber Security Limited
Company mailing address:	Grosvenor House, 11 St Paul's Square, Birmingham, B3 1RB, United Kingdom
Company website:	https://www.omnicybersecurity.com/
Lead Assessor name:	Jason McWhirr
Assessor phone number:	0121 709 2526
Assessor e-mail address:	jmcwhirr@omnicybersecurity.com

Assessor certificate number:	203-779

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:	TruConnect Hosted Payment Pages & Payment Platform and TruPOS

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		Merchant payment processing is covered by the 'Payment Gateway/Switch' selection below
☐ 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):		

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:	N/a

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:	N/a

Part 2b. Description of Role with Payment Cards (ROC Sections 2.1 and 3.1)

Describe how the business stores, processes, and/or transmits account data.	Trust Payments UK Ltd (Trust Payments) operates as a payment service provider, acting as a payment gateway between merchants and acquiring banks. The company operates a payment platform (referred to as TruConnect (ex-STPP)) which predominantly processes Cardholder-Not-Present (CNP) data (although cardholder-present transactions are processed with one acquirer), and TruPOS, which is a payment switch platform for merchant point of sale systems. Trust Payments also accepts and processes Mail Order/Telephone Order (MOTO) transactions on behalf of its merchant clients. Some merchants accept

	MOTO transactions and send these transactions to Trust Payments via TruConnect payment interfaces. Trust Payments does not accept MOTO transactions directly and does not have a call centre for such payments. Consumer account data, track data, and PIN are also passed through the gateway for card-present transactions taken by customer (merchant) POS solutions. Account data is stored for only as long as is required (e.g., processing, and recurring transactions) as per the PCI DSS standard, with retention times enforced to maintain compliance. Transmission: Trust Payments transmits account data for the purpose of transaction authorisation, fraud checks, tokenisation, and settlement. Processing: Trust Payments processes account data for the purpose of transaction authorisation between the merchant and the acquirer. Trust Payments processes account data for the purpose of settlement services between TruPOS and the acquirer. Storage: Trust Payments stores encrypted PAN for the purpose of transaction authorisation and settlement.
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	Transmission, storage, and processing of account data is performed by the payment gateway and POS systems, so Trust Payments could potentially impact the security of its merchants' consumer account data.
Describe system components that could impact the security of account data.	FaaS, IaaS, and SaaS cloud services, network security controls, computers, servers, remote access.

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.*	TruConnect Merchant account data is transmitted to the payment gateway DMZ webservers located in the Amazon Web Services (AWS) hosted environment. The DMZ is protected by; Web Application Firewall (WAF), Network Load Balancer (NLB), Intrusion Prevention Solution (IPS), and DDoS protection. All other systems and databases are located in the internal zone. Segmentation techniques are used to isolate the cardholder data environment (CDE) from out-of-scope systems and functions. IT administrator access (locally and remotely) is via Jumpservers that require multi-factor authentication. Trust Payments has connections to multiple processing entities with mutually agreed connectivity standards and systems to protect the transmission of cardholder data and maintain PCI DSS requirements. A cloud Hardware Security Module (HSM) is used for key encryption and decryption for TruPOS. An Internet-facing portal is used for merchant back-office services, but only provides a truncated PAN to merchants for transaction referencing. TruPOS Authorisation requests are sent to TruPOS using a PCI DSS PTS compliant payment terminal and the TruPOS Point-of-Sale (POS) client (used in merchant locations) over the Internet to the Amazon Web Services (AWS) hosted environment. TruPOS performs settlement on behalf of merchants with acquirers by using the TruConnect payment gateway and provides reporting services for merchants using only truncated PAN data. All in-scope system components are FaaS (Function as a Service) and SaaS (Software as a Service) solutions provided by AWS and hosted in the European region of AWS.
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*
Datacentre	2	AWS, EU
Datacentre	1	Bangor, UK
Home Office	Many	UK

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
XAC xCL_RP-10	5.x	PTS	4-80032	2026-04-30

* 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, Point to Point Encryption (P2PE) solutions, Software-Based PIN Entry on COTS (SPoC) solutions, Contactless Payments on COTS (CPoC) solutions), and Mobile Payments on COTS (MPoC) products.

Part 2. Executive Summary *(continued)*

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:
Elavon, First Data Merchant Services (dba. Payspring, Paypoint, Payeezy, Acculynk), First Data - Secure Transport (Datawire), Fiserv Solutions Europe Limited (formerly OmniPay), Millenium Digital, TNS Global Connectivity & TNSPay Mobile	Transaction processing & settlement services
Fexco, Currency Select PTY Ltd	Currency conversion services
ACI Worldwide/RED, Cardinal Commerce Corp, Mastercard Payment Gateway Services, Feedzai, FraudControl2	Fraud checking services
AWS	FaaS, IaaS, SaaS, & security services
Cloudflare, Futurex, Lacework, Microsoft, Qualys, Sophos	Communication, encryption, & security services
Xebia	Third-party software development services
XAC	Payment Terminal Supplier

AEVI, AIB, Alipay, AMEX, ANZ, Apple Pay, ATA, Bank of America, Barclays, Cardinal, Cardnet, Citibank, Deutsche Bank, Elavon, EMS, FDMS, FDMS Canada, FEXCO, Google Pay, HBOS, HSBC, Lloyds, Metabank, MobilePay, PayPal, Paysafe, Payvision PNC Bank, Santander, STFS, Streamline, Suntrust, TransFirst, Travelex, Travelex Cuscal, VISA Token, Wells Fargo	Acquirers

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: TruConnect Hosted Payment Pages & Payment Platform and TruPOS

PCI DSS Requirement	Requirement Finding More than one response may be selected for a given requirement. Indicate all responses that apply.				Select If a Compensating Control(s) Was Used
	In Place	Not Applicable	Not Tested	Not in Place	
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.	1.2.6, 2.2.5 - No insecure services, protocols, ports, or daemons in scope. 1.3.3, 2.3.1, 2.3.2, 4.2.1.2 - No wireless networks in scope. 3.3.3 - The assessed entity is not an issuer. 3.5.1.2, 3.5.1.3 - No use of disk-level or partition level encryption. 3.7.9 - No sharing of cryptographic keys with customers. 4.2.2 - PAN not shared over end-user messaging technologies. 5.2.3.1 - Anti-malware software installed on all in-scope systems. 5.3.3 - USB devices are blocked for all in-scope devices, 6.4.3, 11.6.1, 12.5.3 - Future dated requirements. 6.5.2, 11.3.1.3, 11.3.2.1 - No significant changes. 6.5.5 - Live PANs not used in pre-production environments. 8.2.3 - No remote access to customer premises. 8.2.7 - No third party remote access to in-scope systems. 8.3.9 - Passwords are not the only authentication factor. 8.3.10, 8.3.10.1 - No customer access to cardholder data. 9.4.6 - No hard-copy materials containing cardholder data. 9.5.1-9.5.1.3b, A2.1.1, A2.1.2 - No POS POI devices in scope. 10.4.2, 10.4.2.1 - All system components are monitored (as per requirement 10.4.1). 11.4.7, A1.x - Not a multi-tenant service provider. 12.3.2 - No use of the Customised Approach. A3.x - Not a designated entity.
For any Not Tested responses, identify which sub-requirements were not tested and the reason.	N/a

Section 2 Report on Compliance

(**ROC Sections 1.2 and 1.3**)

Date Assessment began: ***Note:*** *This is the first date that evidence was gathered, or observations were made.*	2025-03-03
Date Assessment ended: ***Note:*** *This is the last date that evidence was gathered, or observations were made.*	2025-03-28
Were any requirements in the ROC unable to be met due to a legal constraint?	☐ Yes ☒ No
Were any testing activities performed remotely?	☒ 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 *(Date of Report as noted in the ROC 2025-03-28)*.

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 Trust Payments (UK) Ltd (formerly Secure Trading Limited) 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 N/a has not demonstrated compliance with PCI DSS requirements. **Target Date** for Compliance: N/a 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 N/a 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 4.0.1 and was completed according to the instructions therein.
☒	All information within the above-referenced ROC and in this attestation fairly represents the results of 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

Ian Hughes

Signature of Service Provider Executive Officer ↗	Date: 2025-04-01
Service Provider Executive Officer Name: Ian Hughes	Title: CTO

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:

J McWhirr

Signature of Lead QSA ↗	Date: 2025-04-01
Lead QSA Name: Jason McWhirr	

J McWhirr

Signature of Duly Authorized Officer of QSA Company ↗	Date: 2025-04-01
Duly Authorized Officer Name: Jason McWhirr	QSA Company: OmniCyber Security Limited

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	☐	☐	

Note: The PCI Security Standards Council is a global standards body that provides resources for payment security professionals developed collaboratively with our stakeholder community. Our materials are accepted in numerous compliance programs worldwide. Please check with your individual compliance accepting organization to ensure that this form is acceptable in their program. For more information about PCI SSC and our stakeholder community please visit: https://www.pcisecuritystandards.org/about_us/

CERTIFICATE *of* SIGNATURE

REF. NUMBER
UYBPI-JVURB-AN8Z5-HPBMN

DOCUMENT COMPLETED BY ALL PARTIES ON
01 APR 2025 15:16:22 UTC

SIGNER	TIMESTAMP	SIGNATURE
JASON MCWHIRR EMAIL JMCWHIRR@OMNICYBERSECURITY.COM	SENT 01 APR 2025 14:48:31 UTC SIGNED 01 APR 2025 14:48:31 UTC	 IP ADDRESS 104.28.243.161 LOCATION MANCHESTER, UNITED KINGDOM
IAN HUGHES EMAIL IAN.HUGHES@TRUSTPAYMENTS.COM	SENT 01 APR 2025 14:48:31 UTC VIEWED 01 APR 2025 15:15:58 UTC SIGNED 01 APR 2025 15:16:22 UTC	 IP ADDRESS 104.28.214.205 LOCATION READING, UNITED KINGDOM

RECIPIENT VERIFICATION

EMAIL VERIFIED
01 APR 2025 15:15:58 UTC