WorldNet TPS Ltd.

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:	WorldNet TPS Ltd.		DBA (doing business as):	WorldNet	
Contact Name:	Simon Cruise		Title:	Chief Technology Officer	
Telephone:	+353 1 524 1099		E-mail:	simon.cruise@worldnettps.com	
Business Address:	1st Floor Cherrywood Business & Technology Park Hibernia House Cherrywood Loughlinstown		City:	Dublin	
State/Province:	N/A	Country:	Republic of Ireland	Zip:	D18 E440
URL:	https://www.worldnettps.com				

Part 1b. Qualified Security Assessor Company Information (if applicable)					
Company Name:	Online Enterprises Inc. dba Online Business Systems				
Lead QSA Contact Name:	Chris Ince		Title:	Senior Security Consultant	
Telephone:	+44 07857851666		E-mail:	pcirocs@obsglobal.com	
Business Address:	200-115 Bannatyne Ave		City:	Winnipeg	
State/Province:	MB	Country:	Canada	Zip:	R3B 0R3
URL:	https://www.obsglobal.com/				

PCi Security Standards Council ®

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:	WorldNet TPS Payment Gateway

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):

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.

PCi Security Standards Council ®

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:	N/A

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:	N/A

Part 2b. Description of Payment Card Business

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	WorldNet TPS Ltd. (hereafter WorldNet) is a multichannel payment gateway, enabling payments from web sites, mobile apps, social media, and POS. Merchants send HTTPS API calls to worldnettps.com. HTTPS connections are secured with TLS 1.2. Merchant messages reach an Apache web server where they are decrypted. Inspection on layer 7 for possible web application attacks is done via GCP Cloud Armor. Only when traffic has passed the inspection, is a new TLS session established from GCP Cloud Armor to the Apache web server. The HTTPS session is then forwarded to the proper web server where the traffic is terminated. A web application server processes cardholder data in memory. Once the transaction is processed, the answer is sent back through the same flow (and same encryption tunnels) to the merchants. As a service provider, WorldNet transmits payment card transactions between acquirers and merchants using its own cardholder data environment (CDE). Transactional data, including some elements of cardholder data (encrypted PAN, cardholder name, expiry date) is stored as per WorldNet's retention policy within the NetTraxion application database. There is no storage of sensitive authentication data post-authorization within the organization. WorldNet also develops its web applications (Payment and NetTraxion) for e-commerce card-not-present transactions.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	Cardholder data, including sensitive authentication data for card-not-present transactions, is transmitted to the acquirers for authorization. Post-authorization, WorldNet stores some of the elements of cardholder data (encrypted PAN, cardholder name and expiry date) for reporting purposes. These records are retained and securely disposed of as per WorldNet's retention and disposal policy. WorldNet also provides the gateway functionality to third party call centers so that they can take payments either via an integrated or virtual terminal. During calls, no cardholder data is transferred, and no calls are recorded.

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*
Corporate Offices	1	Dublin, Republic of Ireland

Call Centre	1	Dublin, Republic of Ireland
Data Centre	1	Dublin, Republic of Ireland
Data Centre	1	Carlow, Republic of Ireland

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)
Worldnet NetTraxion	7.5	WorldNet TPS	☐ Yes ☒ No	N/A
WorldNet Payment	7.5	WorldNet	☐ Yes ☒ No	N/A
GoChip SDK	N/A	WorldNet	☐ Yes ☒ No	N/A

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.*	WorldNet processes and transmits Internet based card-not-present (e-commerce) and card-present (GoChip SDK) transactions between merchants and acquirers. Sensitive authentication data from the website (CVV2/CVC2) is transmitted via WorldNet's servers to the acquiring banks for authorization and is not stored in any form. In the case of successful authorisation, the PAN is stored in encrypted format. For the GoChip SDK service, once the transaction has been authorized, WorldNet stores the PANin encrypted format. Only the GoChip SDK back-end payment processes and infrastructure are in scope, with the responsibility for the management of POS terminals utilizing GoChip SDK is the responsibility of each individual merchant offering this facility. All critical devices within the CDE, such as web servers, application servers, database servers, firewalls and switches were included in the scope of this assessment

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:	N/A	
QIR Individual Name:	N/A	
Description of services provided by QIR:	N/A	

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 Telecity DB1	Data Center Hosting, co-location.
Google Cloud Platform (GCP)	Provides Cloud Platform.
Blacknight Internet Solutions Ltd.	Data Center Hosting, co-location.
ACH Jack Henry	Payment Processing
AIB Merchant Services	Payment Processing
Authorize.Net	Payment Processing
Bancomer	Payment Processing
Barclaycard	Payment Processing
Beanstream	Payment Processing
Braintree	Payment Processing
CardFlex	Payment Processing
CashFlows	Payment Processing
ChinaUnionPay Server Hosted solution	Payment Processing
Credorax	Payment Processing
CT Payments	Payment Processing
CyberSource	Payment Processing
CyberSourceSoap	Payment Processing
DigitalRiver	Payment Processing
DirectPay	Payment Processing
Elavon	Payment Processing
Elavon POS	Payment Processing
FDRC DW	Payment Processing

FDRC PTCP	Payment Processing
FDRC TCP	Payment Processing
First Citizens	Payment Processing
FirstData GGe4	Payment Processing
FiServ	Payment Processing
FlapWS	Payment Processing
Global Payroll Gateway	Payment Processing
GlobalCollect	Payment Processing
GlobalCollect Mexico	Payment Processing
HSBCIris	Payment Processing
HSBCMigs	Payment Processing
HSBCUK	Payment Processing
Ingenico	Payment Processing
IntegraPay	Payment Processing
KICC	Payment Processing
Litle	Payment Processing
Maxconnect	Payment Processing
Moneris	Payment Processing
Moneris US	Payment Processing
NCB	Payment Processing
NETAXCEPT	Payment Processing
NICE	Payment Processing
NMI	Payment Processing
Pagos	Payment Processing
Payconex	Payment Processing
PayFlowPro	Payment Processing
Paymentech Orbital	Payment Processing
PayPal	Payment Processing
Paysafe	Payment Processing
PayULatam	Payment Processing
Payvision	Payment Processing
PayvisionV2	Payment Processing
PayvisionV2 JSON	Payment Processing
PesoPay	Payment Processing
PrismPay	Payment Processing
ProPay	Payment Processing

ProtectPay	Payment Processing
RBS WorldPay	Payment Processing
RBS WorldPay UK	Payment Processing
RealEx	Payment Processing
SAGE	Payment Processing
SecurePay	Payment Processing
TNSPAY	Payment Processing
TSYS	Payment Processing
TSYS Saratoga	Payment Processing
USAePay	Payment Processing
VACP	Payment Processing
VACP G2G	Payment Processing
WorldPay	Payment Processing

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:	Provides payment 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:	☐	☒	☐	Requirement 1.2.2 - There are no routers in scope for this assessment. Requirement 1.2.3 - There are no wireless networks in scope for this assessment.
Requirement 2:	☐	☒	☐	Requirement 2.1.1 - There are no wireless networks in scope for this assessment. Requirement 2.2.3 - There are no services, protocols, or daemons that are considered to be insecure. Requirement 2.6 - WorldNet is not a shared hosting provider.
Requirement 3:	☐	☒	☐	Requirement 3.4.1 - Disk encryption is not used. Requirement 3.6 - No keys are shared with customers. Requirement 3.6.6 – No manual clear-text cryptographic key-management operations are used.
Requirement 4:	☐	☒	☐	Requirement 4.1.1 - There are no wireless networks in scope for this assessment.
Requirement 5:	☐	☒	☐	Requirement 5.1, 5.1.1, 5.3 – There are no systems commonly affected by malicious software.
Requirement 6:	☐	☒	☐	Requirement 6.4.6 - There was no significant change in the past 12 months.
Requirement 7:	☒	☐	☐	

PCI Security Standards Council®

Requirement 8:	☐	☒	☐	Requirement 8.1.5 - There are no vendors providing remote management services to WorldNet. Requirement 8.2.6 – Keys are used for Linux systems. Requirement 8.5.1 - WorldNet does not have access to its customers' premises.
Requirement 9:	☐	☒	☐	Requirement 9.5 – 9.5.1 - WorldNet does not generate any media with cardholder data or store cardholder data in any form. Requirement 9.6 – 9.6.3, 9.7, 9.7.1, 9.8 - 9.8.2 – There is no media containing cardholder data in scope for this assessment. Requirement 9.9 - 9.9.3 - WorldNet does not own any point-of-sale systems and is not responsible for the point-of-sale systems owned by customers at their sites.
Requirement 10:	☒	☐	☐	
Requirement 11:	☐	☒	☐	Requirement 11.2.3 - No re-scans were required.
Requirement 12:	☐	☒	☐	Requirement 12.3.9 - No vendors or business partners have access to production systems.
Appendix A1:	☐	☐	☒	A1.1 - A1.4 – WorldNet is not a shared hosting provider.
Appendix A2:	☐	☐	☒	A2.1 - A2.3 – WorldNet does not use SSL/early TLS.

PCI Security Standards Council ®

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:	*08 July 2022*	
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 08 July 2022.

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 *WorldNet TPS Ltd. (DBA WorldNet)* 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 – *Sysnet Global Solutions.*

Part 3b. Service Provider Attestation

DocuSigned by:

Simon Cruise

0D2AF07F890B47E...

Signature of Service Provider Executive Officer ↑	*Date:* 7/8/2022
Service Provider Executive Officer Name: Simon Cruise	*Title:* Chief Technology Officer

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

If a QSA was involved or assisted with this assessment, describe the role performed:	*The QSA Chris Ince, (certificate number 205-825), performed a full assessment of the PCI DSS requirements applicable to the environment, in accordance with the PCI DSS v3.2.1 testing procedures.*

DocuSigned by:

Chris Ince

BCE77ACD99C6409...

Signature of Duly Authorized Officer of QSA Company ↑	*Date:* 7/8/2022
*Duly Authorized Officer Name: **Chris Ince***	*QSA Company:* **Online Enterprises Inc. dba Online Business Systems**

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:	N/A

---

[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.

PCi Security Standards Council ®

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	☐	☐	