Payment Card Industry (PCI)

Data Security Standard

Attestation of Compliance for Onsite Assessments – Service Providers

Version 3.1

April 2015

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:	John Clarke		Title:	Head of Product Innovation	
ISA Name(s) (if applicable):	N/A		Title:	N/A	
Telephone:	+353 1 524 2252		E-mail:	john.clarke@worldnettps.com	
Business Address:	Block AA, Cherrywood Science and Technology Park, Loughlinstown		City:	Dublin	
State/Province:	Dublin	Country:	Ireland	Zip:	
URL:	www.worldnettps.com				

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

Company Name:	Sysnet Global Solutions				
Lead QSA Contact Name:	Bogdan Bondar		Title:	Information Security Consultant	
Telephone:	+48 662 395 468		E-mail:	bogdan.bondar@sysnetgs.com	
Business Address:	4th Floor, The Herbert Building, The Park, Carrickmines		City:	Dublin	
State/Province:	N/A	Country:	Ireland	Zip:	18
URL:	www.sysnetgs.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:		
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.

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: ☐ 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):		
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 is a multichannel payment gateway, enabling payments from web sites, mobile apps and social media. WorldNet also provides managed services to its customers and card-present transactions captured using a mobile Point-of-sale (mPOS).
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	No other services involved in or has the ability to impact the security cardholder data were indicated.

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 office	1	Ireland, Dublin, Cherrywood Techno Park
Technical Office	1	Ukraine, Crimea, Simferopol
Data Center "TeleCity Group"	1	Ireland, Dublin, U7 Kilcarbery Park

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)
Nettraxion	v3.6.1.2	WorldNet TPS	☐ Yes ☒ No	N/A
			☐ Yes ☐ No	
			☐ Yes ☐ No	

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 TPS process and transmit internet based card-not-present (eCommerce) and card-present (mPOS solution) transactions between merchants and acquirers. The scope of this assessment is limited to the mPOS back end payment processing processes and infrastructure. For the mPOS service, PIN data is not received by WorldNet TPS as local authentication is performed on the PED device. After transactions are authorized WorldNet TPS stores encrypted PAN. WorldNet TPS transmits data for authorization and settlement processing. The WorldNet TPS webserver uses a TLS certificate issued by VeriSign CA. Sensitive authentication data from the website (CVV2/CVC2) is transmitted via WorldNet TPS servers to acquiring banks for authorization and are not stored in local databases or in any other form. If the authorization is successful, the PAN is encrypted using an 3DES 192 bits. WorldNet TPS hosts their CDE components in PCI compliant Data Center "TelecityGroup".

	Critical devices within CDE such as application servers, database servers, firewalls, routers and switches were included in the scope.

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 one or more third-party service providers (for example, 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:

Type of service provider:	Description of services provided:
WorldPay	Provides payment gateway services
Barclaycard	Provides payment gateway services
Cashflows	Provides payment gateway services
CT Payments	Provides payment gateway services
Elavon	Provides payment gateway services
First Atlantic Commerce	Provides payment gateway services
First Data Latvia	Provides payment gateway services
Pivotal Payments	Provides payment gateway services
TSYS	Provides payment gateway services
Data Center "TeleCity Group"	PCI DSS compliant service provider. Physical Hosting.

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:	WorldNet TPS Ltd. is a multichannel payment gateway

	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:	☐	☒	☐	**1.2.3 - No wireless environments connected to the CDE**
Requirement 2:	☐	☒	☐	**2.1.1 - No wireless environments connected to the CDE** **2.2.3 - No insecure services, protocols, or daemons found.** **2.6 - Entity is not a shared hosting provider.**
Requirement 3:	☐	☒	☐	**3.2 - Entity is not an issuer** **3.4.1 – No disk encryption is used.** **3.6 - Assessed entity does not share keys with their customers for transmission and storage of cardholder data.**
Requirement 4:	☐	☒	☐	**4.1.1 - No wireless environments connected to the CDE**
Requirement 5:	☒	☐	☐	
Requirement 6:	☒	☐	☐	
Requirement 7:	☒	☐	☐	
Requirement 8:	☐	☒	☐	**8.1.5 - No vendor accounts or vendor remote access is allowed to the CDE.**

Requirement 9:	☐	☒	☐	**9.5.1-9.8 - There is no usage of media for CHD processing, storage or transmission.**
Requirement 10:	☒	☐	☐	
Requirement 11:	☒	☐	☐	
Requirement 12:	☐	☒	☐	**12.3.8-12.3.10 – There is no remote access to the CDE for business partners, and/or vendors.**
Appendix A:	☐	☐	☒	**Assessed entity is not a Shared Hosting Provider**

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:	*15 July 2015*	
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

PCI Security Standards Council

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

Based on the results noted in the ROC dated *15 July 2015*, 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 as of *15 July 2015*: (***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.* 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 *3.1*, 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.

PCI Security Standards Council

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, (ref 3937-01-10)*

Part 3b. Service Provider Attestation

Signature of Service Provider Executive Officer ↑	*Date:* **15 July 2015**
Service Provider Executive Officer Name: **John Clarke**	*Title:* **Head of Product Innovation**

Part 3c. QSA Acknowledgement (if applicable)

If a QSA was involved or assisted with this assessment, describe the role performed:	*Conduct formal assessment of compliance for WorldNet TPS.*

Signature of Duly Authorized Officer of QSA Company ↑	*Date: 15 July 2015*
Duly Authorized Officer Name: Bogdan Bondar	*QSA Company:* Sysnet Global Solutions

Part 3d. ISA Acknowledgement (if applicable)

If an ISA was involved or assisted with this assessment, describe the role performed:	*Not Applicable*

Signature of ISA ↑	*Date:*
ISA Name:	*Title:*

[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 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	☒	☐	