PCi Security Standards Council ®

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:	WorldNet TPS Ltd.	DBA (doing business as):	WorldNet
Contact Name:	Kevin Pattison	Title:	Chief Infrastructure Officer
Telephone:	+353 1 5242252	E-mail:	kevin.pattison@worldnettps.com
Business Address:	WorldNet TPS Ltd. Hibernian Building, Cherrywood Technology Park, Loughlinstown	City:	Dublin

State/Province:	N/A	Country:	Republic of Ireland	Zip:	D18 E440

URL:	www.worldnettps.com

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

Company Name:	Sysnet Global Solutions		
Lead QSA Contact Name:	Robert Calka	Title:	Senior Information Security Consultant
Telephone:	+48 513 153 242	E-mail:	robert.calka@sysnetgs.com
Business Address:	Global Operatioms Centre - 3rd Floor, Block 71a, The Plaza, Park West	City:	Dublin

State/Province:	N/A	Country:	Republic of Ireland Ireland	Zip:	D12 X9F9

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:	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.

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:
- ☐ 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:	Not Applicable

Part 2b. Description of Payment Card Business

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	WorldNet TPS is a multichannel payment gateway, enabling payments from web sites, mobile apps and social media.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	As an Internet Service Provider WorldNet TPS transmits payment card transactions between acquirers and merchants using its own cardholder data environment (CDE). In addition, mPOS transactions are processed using the WorldNet payment gateway, and authorised via third-party acquirers.

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	Dublin, Republic of Ireland

Technical Office	1	Crimea, Ukraine
Data Centre: Equinix Telecity DB1	1	Dublin, Republic of Ireland
Data Centre: Blacknight Internet Solutions	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)
Nettraxion	N/A	WorldNet TPS	☐ Yes	☒ No	N/A
			☐ Yes	☐ No	
			☐ Yes	☐ No	
			☐ Yes	☐ No	
			☐ Yes	☐ No	
			☐ Yes	☐ No	
			☐ Yes	☐ No	
			☐ Yes	☐ No	

Part 2e. Description of Environment

Provide a **_high-level_** description of the environment covered by this assessment.	WorldNet TPS processes and transmits 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, once transactions are authorized, WorldNet TPS stores the encrypted PAN. WorldNet TPS transmits data for authorization and settlement processing. 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. Critical devices within the CDE such as application servers, database servers, firewalls, and switches were in scope.
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.*	
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:

QIR Individual Name:

Description of services provided by QIR:

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:
AIB Merchant Services	Provides Payment Services
Barclaycard	
WorldPay	
Elavon	
Cashflow	
TSYS	
First Data Latvia	
TSYS Saratoga	
CT Payment	
Valitor	
ELAVON POS	
VACP	
CREDORAX	
Rietumu	
Sage	
NMI	
Authorise Net	
Payconex	
FDRC TCP	
First Citizens	
ProPay	
PayVision	
PayVision V2 JSON	
Global Connect	
Global Connect Mexico	
Ingenico	
Moneris	
Moneris US	
RBS Worldpay	

RBS Worlpay UK PrismPay PesoPay China Unionpay	
Equinix Telecity DB1	Physical Hosting
Blacknight Internet Solutions Ltd	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 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:	☐	☒	☐	**Req. 1.2.2 is not applicable because there are no routers within the CDE.** **Req. 1.2.3 is not applicable because there are no wireless networks connected to the CDE.**
Requirement 2:	☐	☒	☐	**Req. 2.1.1 is not applicable because there are no wireless networks connected to the CDE.** **Req. 2.6 is not applicable because the entity is not a shared hosting provider..**
Requirement 3:	☐	☒	☐	**Req. 3.4.1 is not applicable because disk encryption is not used.** **Req. 3.6.a is not applicable because the entity does not share keys with their customers for transmission and storage of cardholder data.**
Requirement 4:	☐	☒	☐	**Req. 4.1.1 is not applicable because there are no wireless networks connected to the CDE.**
Requirement 5:	☒	☐	☐	
Requirement 6:	☐	☒	☐	**Req. 6.4.6 is not applicable this is a best practice until 31 January 2018.**
Requirement 7:	☒	☐	☐	

Requirement 8:	☐	☒	☐	Req. 8.1.5 is not applicable because there are no vendor accounts or vendor remote access allowed to the CDE. Req 8.3.1 is not applicable because this is a best practice until 31 January 2018. Req. 8.5.1 is not applicable because WorldNet TPS does not have access to its customers' premises.
Requirement 9:	☐	☒	☐	Req. 9.5.1 is not applicable because there is no electronic or physical backup media stored. Req. 9.6-9.6.3, 9.7-9.7.1 are not applicable because there is no media that contains cardholder data. Req. 9.8.1- 9.8.2 are not applicable because there are no cardholder data stored on media. Req. 9.9-9.9.3 are not applicable because the entity does not manage devices that capture payment card data via direct physical interaction (clients' responsibility).
Requirement 10:	☐	☒	☐	Req. 10.8.1 is not applicable because this is a best practice until 31 January 2018.
Requirement 11:	☐	☒	☐	Req. 11.1.1 is not applicable because there are no wireless devices permitted in the CDE. Req. 11.3.4.1 is not applicable this is a best practice until 31 January 2018.
Requirement 12:	☐	☒	☐	Req. 12.4.1 is not applicable because this is a best practice until 31 January 2018. Req. 12.11-12.11.1 are not applicable because this is a best practice until 31 January 2018.
Appendix A1:	☐	☐	☒	WorldNet TPS is not ashared service provider.
Appendix A2:	☐	☒	☐	A2.1 is not applicable because there are no POS terminals in scope for this assessment.

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:	*17 July 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 *17 July 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 *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
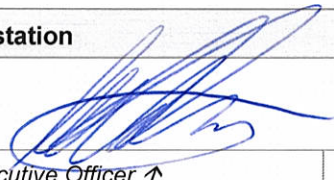
Signatory(s) confirms:

(Check all that apply)

☒	The ROC was completed according to the *PCI DSS Requirements and Security Assessment Procedures*, Version *3.2*, 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 - *Sysnet Global Solutions*.

Part 3b. Service Provider Attestation

Signature of Service Provider Executive Officer ↑	*Date:* 17 July 2017
Service Provider Executive Officer Name: Kevin Pattison	*Title:* Chief Infrastructure 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 performed a full on-site assessment of the PCI DSS requirements applicable to the environment and in accordance with the PCI DSS testing procedures.*
Signature of Duly Authorized Officer of QSA Company ↑	*Date:* 17 July 2017
Duly Authorized Officer Name: Robert Calka	*QSA Company:* Sysnet Global Solutions

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*

---

[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	☒	☐	
Appendix A1	Additional PCI DSS Requirements for Shared Hosting Providers	☒	☐	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS	☒	☐	