



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 TPS Ltd.		
Contact Name:	Kevin Pattison	Title:	Security Officer		
Telephone:	+ 353 1 524 2252	E-mail:	kevin.pattison@worldnettps.com		
Business Address:	WorldNet TPS Ltd. 1 st Floor Cherrywood Business & Technology Park, Hibernia House, Loughlinstown	City:	Dublin		
State/Province:	N/A	Country:	Republic of Ireland	Zip:	D18E440
URL:	www.worldnettps.com				

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

Company Name:	Sysnet Global Solutions				
Lead QSA Contact Name:	Tomasz Mechliński	Title:	QSA		
Telephone:	+353 (0) 1 495 1300	E-mail:	tomasz.mechlinski@sysnetgs.com		
Business Address:	HQ: 1st/3rd Floor Core A Block 71 The Plaza Park West Avenue Park West Business Park	City:	Dublin 12		
State/Province:	N/A	Country:	Republic of Ireland	Zip:	D12 Y4C0
URL:	https://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: <input type="checkbox"/> Applications / software <input type="checkbox"/> Hardware <input type="checkbox"/> Infrastructure / Network <input type="checkbox"/> Physical space (co-location) <input type="checkbox"/> Storage <input type="checkbox"/> Web <input type="checkbox"/> Security services <input type="checkbox"/> 3-D Secure Hosting Provider <input type="checkbox"/> Shared Hosting Provider <input type="checkbox"/> Other Hosting (specify):	Managed Services (specify): <input type="checkbox"/> Systems security services <input type="checkbox"/> IT support <input type="checkbox"/> Physical security <input type="checkbox"/> Terminal Management System <input type="checkbox"/> Other services (specify):	Payment Processing: <input checked="" type="checkbox"/> POS / card present <input checked="" type="checkbox"/> Internet / e-commerce <input type="checkbox"/> MOTO / Call Center <input type="checkbox"/> ATM <input type="checkbox"/> Other processing (specify):	
<input type="checkbox"/> Account Management	<input type="checkbox"/> Fraud and Chargeback	<input checked="" type="checkbox"/> Payment Gateway/Switch	
<input type="checkbox"/> Back-Office Services	<input type="checkbox"/> Issuer Processing	<input type="checkbox"/> Prepaid Services	
<input type="checkbox"/> Billing Management	<input type="checkbox"/> Loyalty Programs	<input type="checkbox"/> Records Management	
<input checked="" type="checkbox"/> Clearing and Settlement	<input type="checkbox"/> Merchant Services	<input type="checkbox"/> Tax/Government Payments	
<input type="checkbox"/> Network Provider			
<input type="checkbox"/> 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: <input type="checkbox"/> Applications / software <input type="checkbox"/> Hardware <input type="checkbox"/> Infrastructure / Network <input type="checkbox"/> Physical space (co-location) <input type="checkbox"/> Storage <input type="checkbox"/> Web <input type="checkbox"/> Security services <input type="checkbox"/> 3-D Secure Hosting Provider <input type="checkbox"/> Shared Hosting Provider <input type="checkbox"/> Other Hosting (specify):	Managed Services (specify): <input type="checkbox"/> Systems security services <input type="checkbox"/> IT support <input type="checkbox"/> Physical security <input type="checkbox"/> Terminal Management System <input type="checkbox"/> Other services (specify):	Payment Processing: <input type="checkbox"/> POS / card present <input type="checkbox"/> Internet / e-commerce <input type="checkbox"/> MOTO / Call Center <input type="checkbox"/> ATM <input type="checkbox"/> Other processing (specify):
<input type="checkbox"/> Account Management	<input type="checkbox"/> Fraud and Chargeback	<input type="checkbox"/> Payment Gateway/Switch
<input type="checkbox"/> Back-Office Services	<input type="checkbox"/> Issuer Processing	<input type="checkbox"/> Prepaid Services
<input type="checkbox"/> Billing Management	<input type="checkbox"/> Loyalty Programs	<input type="checkbox"/> Records Management
<input type="checkbox"/> Clearing and Settlement	<input type="checkbox"/> Merchant Services	<input type="checkbox"/> Tax/Government Payments
<input type="checkbox"/> Network Provider		

Others (specify):

Provide a brief explanation why any checked services were not included in the assessment:

Part 2b. Description of Payment Card Business

<p>Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.</p>	<p>WorldNet TPS Ltd. (thereafter WorldNet) is a multichannel payment gateway, enabling payments from web sites, mobile apps and social media.</p> <p>Merchant sends HTTPS API call to worldnettps.com. HTTPS connection is secured with TLS 1.2. Merchant message reaches Apache web server where it is decrypted. Inspection on layer 7 for possible Web Application attacks is done on Imperva. Once traffic is inspected and passed, new TLS session is established from Imperva to Apache web server via firewall SonicWall HA. SonicWall works in "pass through" mode. HTTPS session is forwarded to the proper web server where HTTPS traffic is terminated. Web application server processes cardholder data in memory. Once transaction is processed, the answer is sent back through the same flow (and same encryption tunnels) to the merchant.</p> <p>As a Service Provider, WorldNet transmits payment card transactions between the acquirers and the merchants using its own cardholder data environment (CDE).</p> <p>Transactional data, including some elements of cardholder data (encrypted PAN, cardholder name, expiry date) is stored as per the WorldNet's retention policy within the NetTraxion application database. There is no storage of sensitive authentication data post-authorization within the organization.</p>
<p>Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.</p>	<p>WorldNet is a Service Provider who processes card transactions on behalf of merchants, who can make use of the WorldNet's payment platform in a number of ways, including online e-commerce integrations, mobile payments, virtual terminals or mPOS.</p> <p>Cardholder data, in some cases including sensitive authentication data (for card-not-present transactions) is transmitted to the acquirers for authorization.</p> <p>Post-authorization, WorldNet stores some of the elements of cardholder data (encrypted PAN, cardholder name, expiry date) for reporting purposes. These records are retained and securely disposed of as per WorldNet's retention and disposal policy.</p>

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):
<i>Example: Retail outlets</i>	3	<i>Boston, MA, USA</i>
<i>Corporate office</i>	1	<i>Dublin, Ireland</i>

Technical Office	1	Crimea, Ukraine
Data Centre – Equinix Telecity DB1	1	Dublin, Ireland
Data Centre – Blacknight Internet Solutions Ltd.	1	Carlow, 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	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> 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 (mPOS) transactions between merchants and acquirers. Sensitive authentication data from the website (CVV2/CVC2) is transmitted via WorldNet's servers to the acquiring banks for authorisation and is not stored in any form. In case of successful authorization, the PAN is stored in an encrypted format. For the mPOS service, once transaction is authorised, WorldNet stores the encrypted PAN. For this service, only the mPOS back-end payment processing processes and infrastructure are in scope. The responsibility for management of mPOS terminals is with 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:	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:
AIB Merchant Services	Provides payment services.
Barclaycard	Provides payment services.
Elavon	Provides payment services.
Cashflow	Provides payment services.
TSYS	Provides payment services.
CT Payment	Provides payment services.
Valitor	Provides payment services.
Elavon POS	Provides payment services.
CredoRax	Provides payment services.
Rietumu	Provides payment services.
Sage	Provides payment services.
NMI	Provides payment services.
Authorise Net	Provides payment services.
Payconex	Provides payment services.
FDRC TCP	Provides payment services.
First Citizens	Provides payment services.
ProPay	Provides payment services.
PayVision	Provides payment services.
PayVision V2 JSON	Provides payment services.
Global Connect	Provides payment services.
Global Connect Mexico	Provides payment services.
Ingenico	Provides payment services.
Moneris	Provides payment services.
Moneris US	Provides payment services.
VACP	Provides payment services.

TSYS Saratoga	Provides payment services.
PrismPay	Provides payment services.
PesoPay	Provides payment services.
China Unionpay	Provides payment services.
First Data Latvia	Provides payment services.
Equinix Telecity DB1	Data Center Hosting.
Blacknight Internet Solutions Ltd.	Data Center Hosting.
Worldpay, Inc.	Provides payment services.

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		
PCI DSS Requirement	Details of Requirements Assessed			Justification for Approach (Required for all “Partial” and “None” responses. Identify which sub-requirements were not tested and the reason.)
	Full	Partial	None	
Requirement 1:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1.2.2 - There are no routers in scope for this assessment. 1.2.3 - There are no wireless networks in the scope of this assessment.
Requirement 2:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	2.1.1 - There are no wireless networks in the scope of this assessment. 2.2.3 - There are no services, protocols, or daemons that are considered to be insecure. 2.6 - WorldNet is not a shared hosting provider.
Requirement 3:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	3.4.1 - Disk encryption is not used. 3.6 - No keys are shared with customers.
Requirement 4:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	4.1.1 - There are no wireless networks in the scope of this assessment.
Requirement 5:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	5.1, 5.1.1, 5.2, 5.3 – There are no systems commonly affected by malicious software.
Requirement 6:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	6.4.6 - There was no significant change in the past 12 months.
Requirement 7:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Requirement 8:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	8.1.5 - There are no vendors providing remote management services to WorldNet. 8.5.1 - WorldNet does not have access to customer premises.
Requirement 9:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	9.6 – 9.6.3, 9.7, 9.7.1, 9.8, 9.8.1, 9.8.2– there is no media containing cardholder data in the scope of this assessment. 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:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 11:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	11.2.3 - No re-scans were required.
Requirement 12:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	12.3.9 - No vendors or business partners have access to production systems.
Appendix A1:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	A1.1 - A1.4 – WorldNet is not a shared hosting provider.
Appendix A2:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	A2.1 - A2.3 – WorldNet does not use SSL/early TLS.

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:	23 July 2019	
Have compensating controls been used to meet any requirement in the ROC?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Were any requirements in the ROC identified as being not applicable (N/A)?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
Were any requirements not tested?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Were any requirements in the ROC unable to be met due to a legal constraint?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in the ROC dated 23th July 2019.

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*):

<input checked="" type="checkbox"/>	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.				
<input type="checkbox"/>	<p>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 (<i>Service Provider Company Name</i>) has not demonstrated full compliance with the PCI DSS.</p> <p>Target Date for Compliance:</p> <p>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. <i>Check with the payment brand(s) before completing Part 4.</i></p>				
<input type="checkbox"/>	<p>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.</p> <p><i>If checked, complete the following:</i></p> <table border="1" data-bbox="316 1084 1370 1187"> <thead> <tr> <th>Affected Requirement</th> <th>Details of how legal constraint prevents requirement being met</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> </tbody> </table>	Affected Requirement	Details of how legal constraint prevents requirement being met		
Affected Requirement	Details of how legal constraint prevents requirement being met				

Part 3a. Acknowledgement of Status

Signatory(s) confirms:

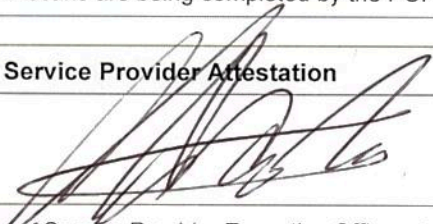
(*Check all that apply*)

<input checked="" type="checkbox"/>	The ROC was completed according to the <i>PCI DSS Requirements and Security Assessment Procedures</i> , Version 3.2.1, and was completed according to the instructions therein.
<input checked="" type="checkbox"/>	All information within the above-referenced ROC and in this attestation fairly represents the results of my assessment in all material respects.
<input type="checkbox"/>	I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
<input checked="" type="checkbox"/>	I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
<input checked="" type="checkbox"/>	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 data¹, CAV2, CVC2, CID, or CVV2 data², or PIN data³ 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: 29/7/2019
Service Provider Executive Officer Name: KEVIN PATTISON	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:	<i>The QSAs, Tomasz Mechliński (certificate number 205-514) and Krzysztof Olejniczak (certificate number 203-393), performed a full assessment of the PCI DSS requirements applicable to the environment, in accordance with the PCI DSS v3.2.1 testing procedures.</i>
--------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------



Signature of Duly Authorized Officer of QSA Company ↑	Date: 23 July 2019
Duly Authorized Officer Name: James Devoy	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	<input type="checkbox"/>	<input type="checkbox"/>	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	<input type="checkbox"/>	<input type="checkbox"/>	
3	Protect stored cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
4	Encrypt transmission of cardholder data across open, public networks	<input type="checkbox"/>	<input type="checkbox"/>	
5	Protect all systems against malware and regularly update anti-virus software or programs	<input type="checkbox"/>	<input type="checkbox"/>	
6	Develop and maintain secure systems and applications	<input type="checkbox"/>	<input type="checkbox"/>	
7	Restrict access to cardholder data by business need to know	<input type="checkbox"/>	<input type="checkbox"/>	
8	Identify and authenticate access to system components	<input type="checkbox"/>	<input type="checkbox"/>	
9	Restrict physical access to cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
10	Track and monitor all access to network resources and cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
11	Regularly test security systems and processes	<input type="checkbox"/>	<input type="checkbox"/>	
12	Maintain a policy that addresses information security for all personnel	<input type="checkbox"/>	<input type="checkbox"/>	
Appendix A1	Additional PCI DSS Requirements for Shared Hosting Providers	<input type="checkbox"/>	<input type="checkbox"/>	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	<input type="checkbox"/>	<input type="checkbox"/>	

