



# 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:	WorldNet TPS Ltd. Hibernian Building Cherrywood Technology Park, Loughlinstown, Dublin, Ireland	City:	Dublin
State/Province:	Dublin	Country:	Ireland
URL:	www.worldnettps.com		
		Zip:	

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

Company Name:	Sysnet Global Solutions		
Lead QSA Contact Name:	Jason Cookes	Title:	Managing Information Security Consultant
Telephone:	+353 (0)1 495 1300	E-mail:	jason.cookes@systnetgs.com
Business Address:	4th Floor, The Herbert Building, The Park, Carrickmines	City:	Dublin
State/Province:	N/A	Country:	Ireland
URL:	www.systnetgs.com		
		Zip:	18

## 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:		
<b>Hosting Provider:</b> <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):	<b>Managed Services (specify):</b> <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):	<b>Payment Processing:</b> <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 checked="" 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 type="checkbox"/> Clearing and Settlement	<input checked="" 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.

**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:		
<b>Hosting Provider:</b> <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):	<b>Managed Services (specify):</b> <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):	<b>Payment Processing:</b> <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		
<input type="checkbox"/> 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.
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 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):
<i>Example: Retail outlets</i>	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
Data Center Blacknight Internet Solutions Ltd	1	Unit 12A, Barrowside Business Park Sleaty Road, Graiguecullen, 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	v3.6	WorldNet TPS	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	N/A
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> 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, 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 COMODO. 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 [REDACTED]

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 Barclaycard Valitor Elevon First Atlantic CT Payments Credorax AIB Merchant Services CashFlows Pivotal Payments	Provides Payment Services
Telecity Group DC (Blacknight Solutions)	Physical Hosting.
Blacknight Solutions	Phyiscial 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.

<b>Name of Service Assessed:</b>		WorldNet TPS Payment Gateway		
<b>PCI DSS Requirement</b>	<b>Details of Requirements Assessed</b>			<b>Justification for Approach</b> (Required for all “Partial” and “None” responses. Identify which sub-requirements were not tested and the reason.)
	<b>Full</b>	<b>Partial</b>	<b>None</b>	
Requirement 1:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1.2.3 - No wireless environments connected to the CDE
Requirement 2:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	2.1.1 - No wireless environments connected to the CDE 2.2.3 No insecure services 2.6 - Entity is not a shared hosting provider.
Requirement 3:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	3.2 - Entity is not an issuer 3.4.1 – Disk encryption is not used. 3.6.a - Assessed entity does not share keys with their customers for transmission and storage of cardholder data.
Requirement 4:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	4.1.1 - No wireless environments connected to the CDE
Requirement 5:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	5.1 - 5.1.1, 5.2 - 5.4 No systems in use that are commonly affected by malicious software
Requirement 6:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
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 - No vendor accounts or vendor remote access is allowed to the CDE.

				8.5.1 WorldNet does not have access to client environments
Requirement 9:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	9.5.1 There is no electronic or physical backup media stored. 9.6 Media which contains cardholder data is not sent outside the data centres 9.6.2 -9.7.1 Media is not stored outside of the DC's 9.8.1- 9.8.2 No cardholder data is stored on external media. 9.9 Entity does not maintain devices that capture payment card data via direct physical interaction (client responsibility).
Requirement 10:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 11:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 12:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Appendix A:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	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 2016
Have compensating controls been used to meet any requirement in the ROC?	<input checked="" type="checkbox"/> Yes <input 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

Based on the results noted in the ROC dated *15 July 2016*, 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 2016*: (**check one**):

<input checked="" type="checkbox"/>	<p><b>Compliant:</b> All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall <b>COMPLIANT</b> rating; thereby <i>WorldNet TPS Ltd.</i> has demonstrated full compliance with the PCI DSS.</p>						
<input type="checkbox"/>	<p><b>Non-Compliant:</b> Not all sections of the PCI DSS ROC are complete, or not all questions are answered affirmatively, resulting in an overall <b>NON-COMPLIANT</b> rating, thereby (<i>Service Provider Company Name</i>) has not demonstrated full compliance with the PCI DSS.</p> <p><b>Target Date</b> 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><b>Compliant but with Legal exception:</b> 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" style="width: 100%;"> <thead> <tr> <th style="width: 30%;">Affected Requirement</th> <th>Details of how legal constraint prevents requirement being met</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> <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, Version 3.1</i> , 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 checked="" 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 data<sup>1</sup>, CAV2, CVC2, CID, or CVV2 data<sup>2</sup>, or PIN data<sup>3</sup> 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 *Synet Global Solutions*, (ref 3937-01-10)

**Part 3b. Service Provider Attestation**



Signature of Service Provider Executive Officer ↑	Date: 15 July 2016
Service Provider Executive Officer Name: Kevin Pattison	Title: Chief Infrastructure Officer

**Part 3c. QSA Acknowledgement (if applicable)**

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

	
Signature of Duly Authorized Officer of QSA Company ↑	Date: 15 July 2016
Duly Authorized Officer Name: Jason Cookes	QSA Company: Synet 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:

<sup>1</sup> 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.

<sup>2</sup> 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.

<sup>3</sup> 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 checked="" type="checkbox"/>	<input type="checkbox"/>	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3	Protect stored cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
4	Encrypt transmission of cardholder data across open, public networks	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
5	Protect all systems against malware and regularly update anti-virus software or programs	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6	Develop and maintain secure systems and applications	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
7	Restrict access to cardholder data by business need to know	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8	Identify and authenticate access to system components	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9	Restrict physical access to cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10	Track and monitor all access to network resources and cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
11	Regularly test security systems and processes	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12	Maintain a policy that addresses information security for all personnel	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

