



Payment Card Industry (PCI) **Data Security Standard**

Attestation of Compliance for Self-Assessment Questionnaire D – Service Providers

For use with PCI DSS Version 3.2

Revision 1.1

January 2017

Section 1: Assessment Information

Instructions for Submission

This document must be completed as a declaration of the results of the service provider's self-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:	HEMKO Systems Corporation	DBA (doing business as):	
Contact Name:	Harry Hemstreet	Title:	President
Telephone:	970-667-0460	E-mail:	hhemstreet@hemko.com
Business Address:	5560 Stone Church Court	City:	Loveland
State/Province:	Colorado	Country:	USA
		Zip:	80537
URL:	reg.PlanetReg.com		

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

Company Name:	his is a self-assessment completed using tools provided by Trustwave		
Lead QSA Contact Name:		Title:	
Telephone:		E-mail:	
Business Address:		City:	
State/Province:		Country:	
		Zip:	
URL:	www.trustwave.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: PlanetReg

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.

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: <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"/> Back-Office Services <input type="checkbox"/> Billing Management <input type="checkbox"/> Clearing and Settlement <input type="checkbox"/> Network Provider	<input type="checkbox"/> Fraud and Chargeback <input type="checkbox"/> Issuer Processing <input type="checkbox"/> Loyalty Programs <input type="checkbox"/> Merchant Services	<input type="checkbox"/> Payment Gateway/Switch <input type="checkbox"/> Prepaid Services <input type="checkbox"/> Records Management <input type="checkbox"/> Tax/Government Payments
<input type="checkbox"/> Others (specify):		

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

Part 2b. Description of Payment Card Business

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	Cardholder data is collected online and transmitted to payment gateways. Cardholder data is not stored.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	None

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
remote application server	1	Lansing, Michigan

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)
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<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.

The PlanetReg web application resides on a single dedicated server running on MS IIS. The single network connection is to the domain server for internet connection.

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?

If Yes:

Name of QIR Company:

QIR Individual Name:

Description of services provided by QIR:

Yes No

Part 2f. Third-Party Service Providers (Continued)

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:
Authorize.net	PAYMENT_PROCESSING
eProcessing Network, LLC	PAYMENT_PROCESSING
eWay	PAYMENT_PROCESSING
PAY PAL, INC	PAYMENT_PROCESSING
Sage Payment Solutions	PAYMENT_PROCESSING
USA ePay, a Gorcorp Company	PAYMENT_PROCESSING
goEmerchants, LLC	PAYMENT_PROCESSING
Stripe, Inc	PAYMENT_PROCESSING
BluePay	PAYMENT_PROCESSING
Merchant One, Inc.	PAYMENT_PROCESSING
Elavon NA	PAYMENT_PROCESSING
Bluefin Payment Systems	PAYMENT_PROCESSING
First Data - Card Services	PAYMENT_PROCESSING
International	
CardConnect	PAYMENT_PROCESSING
Australia Post	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 were assessed for that Requirement, and no sub-requirements were marked as “Not Tested” or “Not Applicable” in the SAQ.
- Partial – One or more sub-requirements of that Requirement were marked as “Not Tested” or “Not Applicable” in the SAQ.
- None – All sub-requirements of that Requirement were marked as “Not Tested” and/or “Not Applicable” in the SAQ.

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 SAQ
- 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: PlanetReg

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"/>	<p>1.2.3 My organization does not use wireless networks anywhere in the CDE</p> <p>1.3.6 Cardholder data is not stored.</p> <p>1.3.7(b) There is no disclosure of private IP addresses or routing information disclosed to external entities.</p>
Requirement 2:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>2.1.1 (a) My organization does not use wireless networks in the cardholder data environment.</p> <p>2.1.1 (b) My organization does not use wireless networks in the cardholder data environment.</p> <p>2.1.1 (c) My organization does not use wireless networks in the cardholder data environment.</p> <p>2.1.1 (d) My organization does not use wireless networks in the cardholder data environment.</p> <p>2.1.1 (e) My organization does not use wireless networks in the cardholder data environment.</p> <p>2.2.1 (b) virtualization technology is not used</p>

Requirement 3:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>3.1 (a) No card holder data is stored.</p> <p>3.1 (b) No card holder data is stored.</p> <p>3.1 (c) No card holder data is stored.</p> <p>3.1 (d) No card holder data is stored.</p> <p>3.1 (e) No card holder data is stored.</p> <p>3.2 (a) sensitive authentication data is not stored</p> <p>3.2 (b) sensitive authentication data is not stored</p> <p>3.4 PAN is not stored</p> <p>3.4.1 (a) disk encryption is not used</p> <p>3.4.1 (b) cryptographic keys are not used</p> <p>3.4.1 (c) cardholder data is not stored</p> <p>3.5.1 cardholder data is not stored</p> <p>3.5.2 cryptographic keys are not used</p> <p>3.5.3 cryptographic keys are not used, cardholder data is not stored</p> <p>3.5.4 cryptographic keys are not used</p> <p>3.6 (a) cryptographic keys are not used, cardholder data is not stored</p> <p>3.6 (b) cryptographic keys are not used, cardholder data is not stored</p> <p>3.6.1 cryptographic keys are not used</p> <p>3.6.2 cryptographic keys are not used</p> <p>3.6.3 cryptographic keys are not used</p> <p>3.6.4 cryptographic keys are not used</p> <p>3.6.5 (a) cryptographic keys are not used</p> <p>3.6.5 (b) cryptographic keys are not used</p> <p>3.6.5 (c) cryptographic keys are not used</p> <p>3.6.6 manual clear-text key management operations are not used</p> <p>3.6.7 cryptographic keys are not used</p> <p>3.6.8 cryptographic keys are not used</p> <p>3.7 cardholder data is not stored</p>
Requirement 4:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>4.1.1 My organization does not use wireless networks in the cardholder data environment.</p> <p>4.2 (a) PANs are not sent using end-user messaging</p>

				technologies.
Requirement 5:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
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"/>	<p>8.5.1 my organization has no remote access to customer premises.</p> <p>8.7 (a) cardholder data is not stored, no database contains cardholder data</p> <p>8.7 (b) cardholder data is not stored, no database contains cardholder data</p> <p>8.7 (c) cardholder data is not stored, no database contains cardholder data</p>
Requirement 9:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>9.1.3 No wireless handheld devices exist within the cardholder environment.</p> <p>9.5 No media is part of the cardholder environment.</p> <p>9.5.1 No media is part of the cardholder environment.</p> <p>9.6 (a) No media is part of the cardholder environment.</p> <p>9.6.1 No media is part of the cardholder environment.</p> <p>9.6.2 No media is part of the cardholder environment.</p> <p>9.6.3 No media is part of the cardholder environment.</p> <p>9.7 No media is part of the cardholder environment.</p> <p>9.7.1 (a) No media is part of the cardholder environment.</p> <p>9.7.1 (b) No media is part of the cardholder environment.</p> <p>9.8 (a) No media is part of the cardholder environment.</p> <p>9.8 (b) No media is part of the cardholder environment.</p> <p>9.8.1 (a) No media is part of the cardholder environment.</p>

				<p>9.8.1 (b) No media is part of the cardholder environment.</p> <p>9.8.2 No media is part of the cardholder environment.</p> <p>9.9 (a) no devices exist for direct physical interaction with cards</p> <p>9.9 (b) no devices exist for direct physical interaction with cards</p> <p>9.9 (c) no devices exist for direct physical interaction with cards</p> <p>9.9.1 (a) no devices exist for direct physical interaction with cards</p> <p>9.9.1 (b) no devices exist for direct physical interaction with cards</p> <p>9.9.1 (c) no devices exist for direct physical interaction with cards</p> <p>9.9.2 (a) no devices exist for direct physical interaction with cards</p> <p>9.9.2 (b) no devices exist for direct physical interaction with cards</p> <p>9.9.3 (a) no devices exist for direct physical interaction with cards</p> <p>9.9.3 (b) no devices exist for direct physical interaction with cards</p> <p>9.10 cardholder data is not stored, no database contains cardholder data no physical contact with cards occurs</p>
Requirement 10:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>10.2.1 cardholder data is not stored, no database contains cardholder data no physical contact with cards occurs</p> <p>10.4.1 (b) not more than one server</p>
Requirement 11:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>11.1 (a) no wireless access points exist</p> <p>11.1 (b) no wireless access points exist</p>

				<p>11.1 (c) no wireless access points exist</p> <p>11.1 (d) no wireless access points exist</p> <p>11.1.1 no wireless access points exist</p> <p>11.1.2 (a) no wireless access points exist</p> <p>11.1.2 (b) no wireless access points exist</p> <p>11.3.4 (a) segmentation is not used to isolate the CDE, CDE is on a single dedicated server with a single network connection to domain server(internet)</p> <p>11.3.4 (b) segmentation is not used to isolate the CDE, CDE is on a single dedicated server with a single network connection to domain server(internet)</p> <p>11.3.4 (c) segmentation is not used to isolate the CDE, CDE is on a single dedicated server with a single network connection to domain server(internet)</p> <p>11.3.4.1 (a) segmentation is not used to isolate the CDE, CDE is on a single dedicated server with a single network connection to domain server(internet)</p> <p>11.3.4.1 (b) segmentation is not used to isolate the CDE, CDE is on a single dedicated server with a single network connection to domain server(internet)</p> <p>11.3.4.1 (c) segmentation is not used to isolate the CDE, CDE is on a single dedicated server with a single network connection to domain server(internet)</p> <p>11.3.4.1 (d) segmentation is not used to isolate the CDE, CDE is on a single dedicated server with a single network connection to domain server(internet)</p>
Requirement 12:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>12.3.10 (a) cardholder data is not stored, no database contains cardholder data</p> <p>12.3.10 (b) cardholder data is not stored, no database contains</p>

				cardholder data
Appendix A1:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Appendix A2:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	A2.1 no POS/POI terminals are used

Section 2: Self-Assessment Questionnaire D – Service Providers

This Attestation of Compliance reflects the results of a self-assessment, which is documented in an accompanying SAQ.

The assessment documented in this attestation and in the SAQ was completed on:	21 MAY 2018
Have compensating controls been used to meet any requirement in the SAQ?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Were any requirements in the SAQ identified as being not applicable (N/A)?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
Were any requirements in the SAQ identified as being not tested?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Were any requirements in the SAQ 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 SAQ D (Section 2), dated (SAQ completion date).

Based on the results documented in the SAQ D 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"/>	<p>Compliant: All sections of the PCI DSS SAQ are complete, all questions answered affirmatively, resulting in an overall COMPLIANT rating; thereby (Service Provider Company Name) has demonstrated full compliance with the PCI DSS.</p>						
<input type="checkbox"/>	<p>Non-Compliant: Not all sections of the PCI DSS SAQ are complete, or not all questions are answered affirmatively, resulting in an overall NON-COMPLIANT rating, thereby (Service Provide Company Name) 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 “No” 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: 35%;">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:

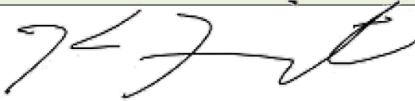
(Check all that apply)

<input checked="" type="checkbox"/>	PCI DSS Self-Assessment Questionnaire D, Version (version of SAQ), was completed according to the instructions therein.
<input checked="" type="checkbox"/>	All information within the above-referenced SAQ 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 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 (*Trustwave*)

Part 3b. Service Provider Attestation



<i>Signature of Service Provider Executive Officer</i> ↑	<i>Date:</i> 01 JUL 2018
<i>Service Provider Executive Officer Name:</i> Ken Dunnington	<i>Title:</i> Security Officer

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

If a QSA was involved or assisted with this assessment, describe the role performed:

<i>Signature of Duly Authorized Officer of QSA Company</i> ↑	<i>Date:</i>
<i>Duly Authorized Officer Name:</i>	<i>QSA Company:</i>

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:

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 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"/>	
Appendix A1	Additional PCI DSS Requirements for Shared Hosting Providers	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

