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:	Vision2Systems, LLC		DBA (doing business as):	N/A	
Contact Name:	Ann Tierney		Title:	Risk and Compliance Officer	
Telephone:	(214) 272-0863		E-mail:	ann.tierney@vision2systems.com	
Business Address:	2130 Commerce Street		City:	Dallas	
State/Province:	TX	Country:	USA	Zip:	75201
URL:	www.vision2systems.com				

Part 1b. Qualified Security Assessor Company Information (if applicable)					
Company Name:	Coalfire Systems, Inc.				
Lead QSA Contact Name:	Avik Mukherjee		Title:	Senior Consultant	
Telephone:	(303) 554-6333		E-mail:	PCIQA@Coalfire.com	
Business Address:	11000 Westmoor Circle, Suite 450		City:	Westminster	
State/Province:	CO	Country:	USA	Zip:	80021
URL:	www.coalfiresystems.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:	Vision2Systems	
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:	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): N/A		
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.	Vison2Systems, LLC (V2S) provides its customers with a secure means of accepting, processing and settling credit card transactions for donation purposes via the Internet, while absorbing most of the PCI compliance burden by ensuring cardholder data never touches the customer's network. Customers subscribing to the V2S platform integrate the V2S API into their web application or mobile application code. At the point when cardholder data is to be captured, the API displays the V2S secure payment online web form. Donors can make one donation at a time or can perform a bulk donation. Once the web form is submitted, a java script (js-encrypt) and a public key from the V2S vault webserver hosted in V2S Cardholder Data Environment (CDE). As the donor enters account data in the V2S payment page the data is encrypted in the donor browser by the js-encrypt using the RSA 4096-bit public key provided by V2S vault webserver. The RSA 4096 public/private key pair used for encrypting the account data is generated by V2S by the vault webserver using Microsoft .NET crypto library and has a validity for 24 hours. The online payment channel is established using at a minimum, TLS 1.0 protocol with AES 128-bit encryption. Encrypted (RSA 4096) CHD consumed includes Permanent Account Number (PAN), Cardholder name, Expiry date and Sensitive Authentication Data (SAD; CAV2/CVC2/CVV2/CID) which is then decrypted by V2S vault application server using the RSA private key and the clear text account data forwarded for payment processing. However, V2S does not store any SAD in its environment. The SAD received is held in .NET data object in volatile memory of the web server before being transmitted for authorization. Once transmitted, the SAD is deleted by releasing the data object programmatically. Cardholder data (CHD) is stored by V2S to enable recurring transactions. CHD is encrypted using the Microsoft .NET Cryptography library and in-house developed process that generates salt values and dynamic encryption keys which are unique for each transaction. The resultant keys used to encrypt the cardholder data for storage use AES 256-bit encryption from the standard Microsoft.NET implementation for cryptography. Credit card numbers consumed for one-time payments and recurring payments are transmitted to CyberSource/FirstData, payment gateway service providers over the Internet (using TLS 1.2 protocol with AES 256-bit encryption) for processing. These transmission channels are maintained by gateway vendors.

Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	V2S, in addition to storing CHD, assigns a pseudo-randomly generated number using .NET random number generator, referred to as a "token", which is also used as the primary key field associated with the encrypted card data. V2S makes use of this token in lieu of credit card numbers for other transactional purposes such as scheduling recurring payments and chargebacks. The tokens are stored in a separate database from the encrypted cardholder data.

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):
Data Center – managed by Armor Defense Inc.	2	Phoenix, AZ, USA and Dallas, TX, USA

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)
Not Applicable.	N/A	N/A	☐ Yes ☐ 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.*	The CHD repository is a MS SQL 2012 database. CHD is encrypted before being stored using Microsoft .NET crypto library using dynamic data encryption keys (AES 256-bit). These databases and other systems that support V2S applications that interact with the CHD are hosted at the Armor Defense Inc (Armor) datacenter in Phoenix, AZ and Dallas, TX. These data centers and the managed services provided by Armor were validated by a PCI Report on Compliance dated May 10, 2016, for PCI DSS v3.1. Coalfire relied on this report for assurance that the physical security controls and management of servers, OS, and Network infrastructure including associated security controls by Armor are in place. Armor uses hypervisor firewalls to isolate the cardholder data environment. All traffic to and from the CHD environment passes through the hypervisor firewalls. V2S in-scope system components includes: • Windows 2008 servers running IIS 7.5 Web servers that accept cardholder information via web application API. • OSSEC File-Integrity monitoring server used to identify integrity of operating system and application files.

	• Microsoft SQL 2012 database servers to store encrypted PAN and masked PAN. Armor management network is used for patch management, logging, anti-virus, and web application firewalls.
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: N/A QIR Individual Name: N/A Description of services provided by QIR: N/A	☐ Yes ☒ No
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:**
Armor Defense, Inc.	Third party service provider providing secure cloud hosting of V2S CDE along with providing managed service for the security of the CDE up to the operating system level
Sumo Logic	Third party service provider providing secure storage of V2S IIS and databases logs along with correlation service
CyberSource	Third party service provider providing payment processing for the payment collected from donor
FirstData Merchant Services	Third party service provider providing payment processing for the payment collected from donor
Gibraltar Loupe	Third party service provider providing secure storage of payment application logs

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:	Vision2Systems

PCI DSS Requirement	**Details of Requirements Assessed**			
	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:	☒	☐	☐	
Requirement 2:	☐	☒	☐	V2S does not maintain any in-scope or connected wireless networks and thus this requirement is Not Applicable: 2.1.1 V2S is not a shared hosting provider and thus this requirement is Not Applicable: Requirement 2.6
Requirement 3:	☐	☒	☐	V2S does not make use of disk encryption and thus this requirement is Not Applicable: Requirement 3.4.1 V2S does store data encrypting keys and this requirement is best practice till January 31, 2016: Requirement 3.5.1 V2S does not store or distribute data encrypting keys and does not have processes that involve any manual clear text key handling and thus these requirements are Not Applicable: Requirement 3.6.2 V2S does not have any manual clear cryptographic practices and thus this requirement is Not Applicable: 3.6.6, 3.6.8
Requirement 4:	☐	☒	☐	V2S does not maintain any in-scope or connected wireless networks and thus this requirement is Not Applicable: Requirement 4.1.1

Requirement 5:	☒	☐	☐	Armor manages AV controls as part of their subscription for the CDE.
Requirement 6:	☐	☒	☐	V2S did not have any significant changes in their CDE in the last 12 months and thus this requirement is Not Applicable: 6.4.6
Requirement 7:	☒	☐	☐	
Requirement 8:	☐	☒	☐	Armor manages controls as part of their subscription: Requirements 8.1.1, 8.1.2, 8.1.3, 8.1.4, 8.1.5, 8.2.1, 8.2.2, 8.3, 8.4, 8.5, 8.6, 8.8 V2S does not grant access to vendors and thus this requirement is Not Applicable: Requirement 8.1.5 This requirement is a best practice until January 31, 2018 and this this requirement is Not Applicable: Requirement 8.3.1. V2S as a service provider does not have remote access to merchant environment and thus this requirement is Not Applicable: Requirement 8.5.1 V2S environment does not make use of any other authentication mechanism than AD credentials and phone factor for two factor authentication and thus this requirement is Not Applicable: Requirement 8.6
Requirement 9:	☐	☒	☐	Armor hosts and manages the virtual infrastructure: Requirements 9.1, 9.2, 9.3, 9.5, 9.8.2, 9.10, 9.1, 9.1.1, 9.1.2, 9.1.3, 9.2, 9.3, and 9.4. V2S does not write any CHD on removable media and thus this requirement in Not Applicable: Requirement 9.5.1, 9.6, 9.6.1, 9.6.2, 9.6.3, 9.7, 9.7.1. V2S does not store CHD in non-digital form and thus this requirement is Not Applicable: Requirement 9.8.1 V2S is a service provider and does not have Point-of-Sale devices and thus these requirements are Not Applicable: Requirement 9.9, 9.9.1, 9.9.2, 9.9.3
Requirement 10:	☐	☒	☐	Armor partially manages controls as part of their subscription: Requirements 10.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3, 10.4, 10.5, 10.6, 10.7 This requirement is best practice until January 31, 2018 and thus is Not Applicable: 10.8

Requirement 11:	☐	☒	☐	Armor manages controls as part of their wireless detection and identification subscription: Requirements 11.1, 11.4, 11.6 V2S has not made significant changes to its cardholder data environment and thus this requirement is Not Applicable: Requirement 11.2.3 This requirement is a best practice until January 31, 2018 and this this requirement is Not Applicable: Requirement 11.3.4.1
Requirement 12:	☐	☒	☐	This requirement is best practice until January 31, 2018 and thus these requirements are Not Applicable: 12.4.1, 12.11
Appendix A1:	☐	☐	☒	V2S is not a shared hosting provider and thus this requirement is Not Applicable: Requirement A.1.1, A.1.2, A.1.3, A.1.4
Appendix A2:	☐	☒	☐	V2S does not have POI devices as part of its CDE and thus requirement A2.1 is Not Applicable

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:	*01/09/2017*	
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 *01/09/2017.*

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 *Vison2Systems, LLC* 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 *Vison2Systems, LLC.* has not demonstrated full compliance with the PCI DSS. **Target Date** for Compliance: N/A 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
N/A	N/A
N/A	N/A

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 *Qualys Inc.*

Part 3b. Service Provider Attestation

Signature of Service Provider Executive Officer ↑	*Date:* 1/18/2017
Service Provider Executive Officer Name: **Ann Tierney**	*Title:* **Risk and Compliance Officer**

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

If a QSA was involved or assisted with this assessment, describe the role performed:	Performed the assessment including all interviews, scope validation exercise, onsite and offsite system component testing, physical location walkthroughs and lead the effort to document the Report on Compliance as the result of the overall assessment.

Signature of Duly Authorized Officer of QSA Company ↑	*Date:* 1/18/2017
Duly Authorized Officer Name: **Avik Mukherjee**	*QSA Company:* **Coalfire Systems, Inc.**

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. No ISAs were involved in the assessment.

[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	☒	☐