



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

---

## **Attestation of Compliance for Onsite Assessments – Merchants**

**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 merchant's assessment with the *Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS)*. Complete all sections: The merchant is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact your acquirer (merchant bank) or the payment brands for reporting and submission procedures.

### Part 1. Merchant and Qualified Security Assessor Information

#### Part 1a. Merchant Organization Information

Company Name:	365 Retail Markets		DBA (doing business as):		
Contact Name:	Robert Hering		Title:	Data Protection Officer	
Telephone:	888.365.7382		E-mail:	robert.hering@365smartshop.com	
Business Address:	1743 Maplelawn		City:	Troy	
State/Province:	MI	Country:	USA	Zip:	48084
URL:	www.365retailmarkets.com				

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

Company Name:	Dara Security				
Lead QSA Contact Name:	Barry Johnson		Title:	President/CEO	
Telephone:	775.622.5386		E-mail:	barryj@darasecurity.com	
Business Address:	10580 N. McCarran Blvd. #115-337		City:	Reno	
State/Province:	NV	Country:	USA	Zip:	89503
URL:	www.darasecurity.com				

### Part 2. Executive Summary

#### Part 2a. Type of Merchant Business (check all that apply)

<input type="checkbox"/> Retailer	<input type="checkbox"/> Telecommunication	<input type="checkbox"/> Grocery and Supermarkets
<input type="checkbox"/> Petroleum	<input type="checkbox"/> E-Commerce	<input type="checkbox"/> Mail order/telephone order (MOTO)
<input checked="" type="checkbox"/> Others (please specify): Self-Service Stand Along Kiosk, Attended and unattended food service terminals and vending machines		

What types of payment channels does your business serve?

- Mail order/telephone order (MOTO)  
 E-Commerce  
 Card-present (face-to-face)

Which payment channels are covered by this assessment?

- Mail order/telephone order (MOTO)  
 E-Commerce  
 Card-present (face-to-face)

**Note:** If your organization has a payment channel or process that is not covered by this assessment, consult your acquirer or payment brand about validation for the other channels.

## Part 2b. Description of Payment Card Business

How and in what capacity does your business store, process and/or transmit cardholder data?

365 Retail Markets designs and implements turnkey, unattended and highly automated MicroMarket self-checkout solutions. The 365 Kiosks and companion application (Valet and V5) are the centerpiece of the growing MicroMarket Industry. Born out of the need for better workplace snack/food options, vending machine operators have quickly gravitated toward offering the open-air, small convenience store model of a MicroMarket. The 365 Kiosk and application allow employees to quickly scan a product they have selected, swipe a credit card and be back at their desks within minutes without leaving the workplace. Operators typically offer around 300 products from bottle beverages to greeting cards. This means that as an employer, you can create a company themed MicroMarket to further emphasize your commitment to providing employees with a market leading alternative to vending machines. At the heart of the 365SmartShop is the 365 SmartHub payment centre where the customer scans and pays for their items. The 365 SmartHub can be configured in multiple ways, including a cash or no-cash dispensing option. The SmartHub can be skinned and branded for any environment.

365 SmartHub is Card-present Point of Sale Application. The 365 SmartHub payment center contains the 365 payment application software. Any payments related to credit card transactions or adding value to a stored-value account with a credit card is handed off to 911 Credit Line payment processing software. OTI card readers are part of an on-going effort to alleviate scope from 365 and consumers for PCI. The OTI card readers offer E2EE (End-to-End Encryption) from swipe to payment resolution.

AirVend is a vending machine with a MSR located on the unit, when a card is swiped the, Track 1 & Track 2 data encrypted in, Track 1 & Track 2 data atomically decrypted and set on data passed through TLS web service to the processor. The track data is only decrypted on the string added to the web service. The copy in memory is still encrypted. The encrypted track data is destroyed.

All devices on the V5 platform including self-service kiosks, nanomarkets™, PicoVend, PicoCooler, ReadyTouch POS, 365Dining, Gen3 Kiosk and Gen3c Kiosk utilize a secure E2EE (End-to-End Encrypted) direct real-time connection to the card processor when items are checked out. The transactions are card present or contactless EMV, with no cardholder data stored for later use. Transactions are needed to complete purchase of items from the self-service, stand-alone, kiosks and mini-retail shops where 365 Retail Markets provide their services. All data is encrypted by the card reader at time of card swipe, 365 Retail Markets does not have access to the encryption keys and cannot decrypt this encrypted cardholder data. This dramatically reduces the scope as 365 Retail Markets does not store, processes and/or transmit (PAN data encrypted during transmission, but 365 Retail Markets does not have access to keys – hence not in scope).

365Pay mobile application utilizes Heartland Payment Systems PCI DSS certified Heartland SecureSubmit backend solution for e-commerce transactions.

### 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	Troy MI USA
Data Center	1	Ayera (Co-Located)
Data Center	1	AWS
Data Center	1	Azure
Data Center	1	Google Cloud

### Part 2d. Payment Application

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)
In-House Developed (Smarthub Kiosk)	2.0.6.3	365 Retail	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	28-Oct-2022
CastlesPay	1.1.x	Castles Technology International	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	28-Oct-2022
			<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.*

Assessment reviewed kiosk deployment, management, and communication. POS application development and communication and interaction with back office support systems.

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 use a Qualified Integrator & Reseller (QIR)?

Yes  No

**If Yes:**

Name of QIR Company:

QIR Individual Name:

Description of services provided by QIR:

Does your company share cardholder data with any 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.)?

Yes  No

**If Yes:**

**Name of service provider:**

**Description of services provided:**

Ayera  
Amazon Web Services

Co-Location Provider

Apriva  
First Data/Bank of America

Processor

Heartland Payment Systems  
Square  
Nayax  
Stripe

Processor

Merchant Link  
USAT  
5th and 3rd bank  
CyberSource

Processor

911 Creditline Software  
Cloud 9 Payment Gateway

Payment Gateway

TrendMicro  
Imperva

Security Services

**Note:** Requirement 12.8 applies to all entities in this list.

## 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:	19-Feb-2021
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 **19-Feb-2021**.

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"/>	<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>365 Retail Markets</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>Merchant 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 your acquirer or 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</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 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)

<input checked="" type="checkbox"/>	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.
<input checked="" type="checkbox"/>	ASV scans are being completed by the PCI SSC Approved Scanning Vendor <i>Clone Systems</i>

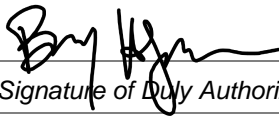
**Part 3b. Merchant Attestation**



<i>Signature of Merchant Executive Officer</i> ↑	<i>Date:</i> 2/24/2021
<i>Merchant Executive Officer Name:</i>	<i>Title:</i> Data Protection Officer

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

If a QSA was involved or assisted with this assessment, describe the role performed:	Level 1 PCI Merchant Review
--	-----------------------------



<i>Signature of Duly Authorized Officer of QSA Company</i> ↑	<i>Date:</i> 19-Feb-2021
<i>Duly Authorized Officer Name:</i> Barry Johnson	<i>QSA Company:</i> Dara Security

**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:	
---	--

<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 your acquirer or the 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 A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

