



# **Payment Card Industry Data Security Standard**

---

## **Attestation of Compliance for Report on Compliance – Service Providers**

**Version 4.0.1**

Publication Date: August 2024

# **PCI DSS v4.0.1 Attestation of Compliance for Report on Compliance – Service Providers**

**Entity Name: 365 Retail Markets**

**Date of Report as noted in the Report on Compliance: 07-Feb-2025**

**Date Assessment Ended: 31-Jan-2025**

## Section 1: Assessment Information

### Instructions for Submission

This Attestation of Compliance (AOC) must be completed as a declaration of the results of the service provider's assessment against the *Payment Card Industry Data Security Standard (PCI DSS) Requirements and Testing Procedures* ("Assessment"). Complete all sections. The service provider is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the entity(ies) to which this AOC will be submitted for reporting and submission procedures.

This AOC reflects the results documented in an associated Report on Compliance (ROC). Associated ROC sections are noted in each AOC Part/Section below.

Capitalized terms used but not otherwise defined in this document have the meanings set forth in the PCI DSS Report on Compliance Template.

#### Part 1. Contact Information

##### Part 1a. Assessed Entity (ROC Section 1.1)

Company name:	365 Retail Markets
DBA (doing business as):	365 Retail Markets LLC
Company mailing address:	1743 Maplelawn Rd. Troy MI 48084
Company main website:	www.365retailmarkets.com
Company contact name:	Syed Umair Azim
Company contact title:	Compliance Officer
Contact phone number:	888.365.6282
Contact e-mail address:	syed.azim@365smartshop.com

##### Part 1b. Assessor (ROC Section 1.1)

Provide the following information for all assessors involved in the Assessment. If there was no assessor for a given assessor type, enter Not Applicable.

##### PCI SSC Internal Security Assessor(s)

ISA name(s):

##### Qualified Security Assessor

Company name:	Certify Audit Services Inc.
Company mailing address:	PO BOX 83752 Gaithersburg MD 20883
Company website:	www.certifyauditservices.com
Lead Assessor name:	Carlette (Letty) Gambrell
Assessor phone number:	775.622.5386
Assessor e-mail address:	carlette@certifyauditservices.com
Assessor certificate number:	206-171

## Part 2. Executive Summary

### Part 2a. Scope Verification

Services that were **INCLUDED** in the scope of the Assessment (select all that apply):

Name of service(s) assessed: MicroMarket, Vending, & Food Service Technology

Type of service(s) assessed:

#### Hosting Provider:

- ☐ Applications / software
- ☐ Hardware
- ☐ Infrastructure / Network
- ☐ Physical space (co-location)
- ☐ Storage
- ☐ Web-hosting services
- ☐ Security services
- ☐ 3-D Secure Hosting Provider
- ☐ Multi-Tenant Service Provider
- ☐ Other Hosting (specify):

#### Managed Services:

- ☐ Systems security services
- ☐ IT support
- ☐ Physical security
- ☐ Terminal Management System
- ☐ Other services (specify):

#### Payment Processing:

- ☒ POI / 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): MicroMarket, Vending, & Food Service Technology

**Note:** These categories are provided for assistance only and are not intended to limit or predetermine an entity's service description. If these categories do not apply to the assessed service, complete "Others." If it is not clear whether a category could apply to the assessed service, consult with the entity(ies) to which this AOC will be submitted.

## Part 2. Executive Summary *(continued)*

### Part 2a. Scope Verification *(continued)*

Services that are provided by the service provider but were **NOT INCLUDED** in the scope of the Assessment (select all that apply):

Name of service(s) not assessed:

Type of service(s) not assessed:

#### Hosting Provider:

- ☐ Applications / software
- ☐ Hardware
- ☐ Infrastructure / Network
- ☐ Physical space (co-location)
- ☐ Storage
- ☐ Web-hosting services
- ☐ Security services
- ☐ 3-D Secure Hosting Provider
- ☐ Multi-Tenant Service Provider
- ☐ Other Hosting (specify):

#### Managed Services:

- ☐ Systems security services
- ☐ IT support
- ☐ Physical security
- ☐ Terminal Management System
- ☐ Other services (specify):

#### Payment Processing:

- ☐ POI / 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):

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

### Part 2b. Description of Role with Payment Cards (ROC Sections 2.1 and 3.1)

Describe how the business stores, processes, and/or transmits account data.

365 Retail Markets (Airvend/V5)

Designs and implements turnkey, unattended and highly automated MicroMarket self-checkout solutions. The 365 Kiosk and companion V5 application is the centerpiece of the growing MicroMarket Industry. Born out of the need for better workplace food service and convenience 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, tap, insert, or swipe a credit card and be back at their desks within minutes

	<p>without leaving the workplace. Operators typically offer around 300 products from bottled 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 MicroMarket is the 365 Kiosk payment center where the customer scans and pays for their items. The 365 Kiosk can be configured in multiple ways, including a cash or no-cash dispensing option. The Kiosk can be branded for any environment.</p> <p>All devices on the V5 platform including the MM6 Kiosk, Gen3 Kiosk, PicoMarket, PicoCooler, PicoVend, PayPlus, and 365Dining POS, utilize a secure E2EE (End-to-End Encrypted) or P2PE (Point-to-Point 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).</p> <p>365Pay mobile application utilizes Heartland Payment Systems PCI DSS certified Heartland SecureSubmit backend solution for e-commerce transactions.</p> <p>The web version of 365Pay is mymarketaccount.net which utilizes the Heartland Payment Systems PCI DSS certified Heartland Portico.</p> <p>Finally, there is support for an e-Commerce webstore that utilizes iFrames from a supported 3rd PCI DSS gateway that allows customers to place orders online.</p>
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	<p>Entity is not exposed to clear-text CHD. For card present transaction, CHD is collected by the POI device deployed within the kiosk and encrypted by the POI device. This information is sent directly to the processor for payment processing. Upon completion of processing the truncated PAN is provided to the entity's backend environment along with results of the transaction request. For card-not-present transactions, CHD is collected through a presented payment page with an integrated iFrame that submits payment card data directly to the processor from the consumer's browser. The entity does not store any CHD within its environment.</p>
Describe system components that could impact the security of account data.	<p>Kiosks and servers supporting the solution.</p>

## Part 2. Executive Summary *(continued)*

### Part 2c. Description of Payment Card 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 POI devices, databases, web servers, etc., and any other necessary payment components, as applicable.*
- *System components that could impact the security of account data.*

Assessment reviewed the overall environment to include the network deployed at the co-location facility, access by entity to the facility from the office locations, and connectivity to and from supported processors. In addition, the development and management of systems and the internal applications were reviewed.

Indicate whether the environment includes segmentation to reduce the scope of the Assessment.

(Refer to the "Segmentation" section of PCI DSS for guidance on segmentation)

☒ Yes ☐ No

### Part 2d. In-Scope Locations/Facilities (ROC Section 4.6)

List all types of physical locations/facilities (for example, corporate offices, data centers, call centers and mail rooms) in scope for this Assessment.

Facility Type	Total Number of Locations (How many locations of this type are in scope)	Location(s) of Facility (city, country)
<i>Example: Data centers</i>	3	<i>Boston, MA, USA</i>
Headquarters	1	Troy MI USA
Data Center	1	AWS USA

## Part 2. Executive Summary *(continued)*

### Part 2e. PCI SSC Validated Products and Solutions (ROC Section 3.3)

Does the entity use any item identified on any PCI SSC Lists of Validated Products and Solutions.\*?

☒ Yes ☐ No

Provide the following information regarding each item the entity uses from PCI SSC's Lists of Validated Products and Solutions:

Name of PCI SSC validated Product or Solution	Version of Product or Solution	PCI SSC Standard to which Product or Solution Was Validated	PCI SSC Listing Reference Number	Expiry Date of Listing
UPT1000F		PCI PTS 5.x	4-80031	30-Apr-2026
UPT1000F		PCI PTS 5.x	4-80051	30-Apr-2026
UPT1000B		PCI PTS 5.x	4-30373	30-Apr-2026
S1U2		PCI PTS 6.x	4-80077	30-Apr-2031
Ux410		PCI PTS 5.x	4-20353	30-Apr-2026
Lane/3600		PCI PTS 6.x	4-30481	30-Apr-2031
Saturn1000-E UPT		PCI PTS 5.x	4-30402	30-Apr-2026
Self/3000		PCI PTS 6.x	4-30510	30-Apr-2031
iUC285		PCI PTS 4.x	4-30161	30-Apr-2024

\* For purposes of this document, "Lists of Validated Products and Solutions" means the lists of validated products, solutions, and/or components, appearing on the PCI SSC website ([www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)) (for example, 3DS Software Development Kits, Approved PTS Devices, Validated Payment Software, Point to Point Encryption (P2PE) solutions, Software-Based PIN Entry on COTS (SPoC) solutions, Contactless Payments on COTS (CPoC) solutions), and Mobile Payments on COTS (MPoC) products.



## Part 2. Executive Summary *(continued)*

### Part 2f. Third-Party Service Providers (ROC Section 4.4)

For the services being validated, does the entity have relationships with one or more third-party service providers that:

• Store, process, or transmit account data on the entity's behalf (for example, payment gateways, payment processors, payment service providers (PSPs, and off-site storage))	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
• Manage system components included in the entity's Assessment (for example, via network security control services, anti-malware services, security incident and event management (SIEM), contact and call centers, web-hosting companies, and IaaS, PaaS, SaaS, and FaaS cloud providers)	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
• Could impact the security of the entity's CDE (for example, vendors providing support via remote access, and/or bespoke software developers).	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No

#### If Yes:

Name of Service Provider:	Description of Services Provided:
True Commerce Inc.	Processor
Heartland Payment Systems	Processor
Apriva LLC	Processor
Adyen	Processor
FreedomPay	Processor
Worldline	Processor
Nayax LLC	Processor
WalleeAG	Processor
Amazon Web Services	Cloud Provider

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

## Part 2. Executive Summary *(continued)*

### Part 2g. Summary of Assessment (ROC Section 1.8.1)

Indicate below all responses provided within each principal PCI DSS requirement.

For all requirements identified as either “Not Applicable” or “Not Tested,” complete the “Justification for Approach” table below.

**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: MicroMarket, Vending, & Food Service Technology

PCI DSS Requirement	Requirement Finding More than one response may be selected for a given requirement. Indicate all responses that apply.				Select If a Compensating Control(s) Was Used
	In Place	Not Applicable	Not Tested	Not in Place	
Requirement 1:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 2:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 3:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 4:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 5:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 6:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 7:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 8:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 9:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 10:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 11:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 12:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Appendix A1:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Appendix A2:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

### Justification for Approach

<p>For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.</p>	<p>1.2.6 &amp; 2.2.5 - No insecure service  1.4.5 - No exposure of internal IP addresses  3.3.3 - Entity not an issuer  3.4.2 &amp; 3.5 - 3.7.9 - Entity does not store CHD.  4.2.1.2 - Wireless not used to transmit CHD  4.2.2 - End-user messaging not used to transmit CHD  6.4.3 &amp; 11.6.1 - Does not support use of payment pages  8.2.3 - Does not have remote access to customer premises  9.4.6 - No hardcopy of CHD  9.5 - 9.5.1.3 - Entity does not maintain POI devices  11.4.5 - 11.4.6 - Segmentation not used  11.4.7 &amp; Appendix A1 - Not a multi-tenant service provide  12.3.2 - Customized approach not utilized  Appendix A2 - Early TLS/SSL not utilized</p>
<p>For any Not Tested responses, identify which sub-requirements were not tested and the reason.</p>	<p>N/A</p>

## Section 2 Report on Compliance

### (ROC Sections 1.2 and 1.3)

Date Assessment began: <b>Note:</b> <i>This is the first date that evidence was gathered, or observations were made.</i>	01-Dec-2024
Date Assessment ended: <b>Note:</b> <i>This is the last date that evidence was gathered, or observations were made.</i>	31-Jan-2025
Were any requirements in the ROC unable to be met due to a legal constraint?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Were any testing activities performed remotely?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No

## Section 3 Validation and Attestation Details

### Part 3. PCI DSS Validation (ROC Section 1.7)

**This AOC is based on results noted in the ROC dated** *(Date of Report as noted in the ROC 07-Feb-2025)*.

Indicate below whether a full or partial PCI DSS assessment was completed:

- ☒ **Full Assessment** – All requirements have been assessed and therefore no requirements were marked as Not Tested in the ROC.
- ☐ **Partial Assessment** – One or more requirements have not been assessed and were therefore marked as Not Tested in the ROC. Any requirement not assessed is noted as Not Tested in Part 2g above.

Based on the results documented in the ROC noted above, each signatory identified in any of Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document *(select one)*:

<input checked="" type="checkbox"/>	<p><b>Compliant:</b> All sections of the PCI DSS ROC are complete, and all assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall <b>COMPLIANT</b> rating; thereby 365 Retail Markets has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above.</p>								
<input type="checkbox"/>	<p><b>Non-Compliant:</b> Not all sections of the PCI DSS ROC are complete, or one or more requirements are marked as Not in Place, resulting in an overall <b>NON-COMPLIANT</b> rating; thereby <i>(Service Provider Company Name)</i> has not demonstrated compliance with PCI DSS requirements.</p> <p><b>Target Date</b> for Compliance: YYYY-MM-DD</p> <p>An entity submitting this form with a Non-Compliant status may be required to complete the Action Plan in Part 4 of this document. Confirm with the entity to which this AOC will be submitted before completing Part 4.</p>								
<input type="checkbox"/>	<p><b>Compliant but with Legal exception:</b> One or more assessed requirements in the ROC are marked as Not in Place due to a legal restriction that prevents the requirement from being met and all other assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall <b>COMPLIANT BUT WITH LEGAL EXCEPTION</b> rating; thereby <i>(Service Provider Company Name)</i> has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above or as Not in Place due to a legal restriction.</p> <p>This option requires additional review from the entity to which this AOC will be submitted.</p> <p><i>If selected, complete the following:</i></p> <table border="1"> <thead> <tr> <th>Affected Requirement</th> <th>Details of how legal constraint prevents requirement from being met</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> </tbody> </table>	Affected Requirement	Details of how legal constraint prevents requirement from being met						
Affected Requirement	Details of how legal constraint prevents requirement from being met								

### Part 3. PCI DSS Validation *(continued)*

#### Part 3a. Service Provider Acknowledgement

**Signatory(s) confirms:**

(Select all that apply)

<input checked="" type="checkbox"/>	The ROC was completed according to <i>PCI DSS</i> , Version 4.0.1 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 the Assessment in all material respects.
<input checked="" type="checkbox"/>	PCI DSS controls will be maintained at all times, as applicable to the entity's environment.

#### Part 3b. Service Provider Attestation

Signature of Service Provider Executive Officer ↑	Date:
Service Provider Executive Officer Name:	Title:

#### Part 3c. Qualified Security Assessor (QSA) Acknowledgement

If a QSA was involved or assisted with this Assessment, indicate the role performed:	<input checked="" type="checkbox"/> QSA performed testing procedures.
	<input type="checkbox"/> QSA provided other assistance. If selected, describe all role(s) performed:

<i>Carlette Gambrell</i>	
Signature of Lead QSA ↑	Date: 07-Feb-2025
Lead QSA Name: Carlette (Letty) Gambrell	

<i>Barry Johnson</i>	
Signature of Duly Authorized Officer of QSA Company ↑	Date: 07-Feb-2025
Duly Authorized Officer Name: Barry Johnson	QSA Company: Certify Audit Services Inc.

#### Part 3d. PCI SSC Internal Security Assessor (ISA) Involvement

If an ISA(s) was involved or assisted with this Assessment, indicate the role performed:	<input type="checkbox"/> ISA(s) performed testing procedures.
	<input type="checkbox"/> ISA(s) provided other assistance. If selected, describe all role(s) performed:

## Part 4. Action Plan for Non-Compliant Requirements

Only complete Part 4 upon request of the entity to which this AOC will be submitted, and only if the Assessment has Non-Compliant results noted in Section 3.

If asked to complete this section, select the appropriate response for “Compliant to PCI DSS Requirements” for each requirement below. For any “No” responses, include the date the entity expects to be compliant with the requirement and provide a brief description of the actions being taken to meet the requirement.

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 network security controls	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2	Apply secure configurations to all system components	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3	Protect stored account data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
4	Protect cardholder data with strong cryptography during transmission over open, public networks	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
5	Protect all systems and networks from malicious software	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6	Develop and maintain secure systems and software	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
7	Restrict access to system components and cardholder data by business need to know	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8	Identify users 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	Log and monitor all access to system components and cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
11	Test security systems and networks regularly	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12	Support information security with organizational policies and programs	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Appendix A1	Additional PCI DSS Requirements for Multi-Tenant Service Providers	<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"/>	

*Note: The PCI Security Standards Council is a global standards body that provides resources for payment security professionals developed collaboratively with our stakeholder community. Our materials are accepted in numerous compliance programs worldwide. Please check with your individual compliance accepting organization to ensure that this form is acceptable in their program. For more information about PCI SSC and our stakeholder community please visit: [https://www.pcisecuritystandards.org/about\\_us/](https://www.pcisecuritystandards.org/about_us/)*