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:	Avanti Market Systems		DBA (doing business as):	Not Applicable	
Contact Name:	Shaun Williams		Title:	Scrum Master/Engineering	
Telephone:	888-937-2826		E-mail:	swilliams@avantimarkets.com	
Business Address:	1217 SW 7th St		City:	Renton	
State/Province:	WA	Country:	USA	Zip:	98057
URL:	https://www.avantimarkets.com				

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

Company Name:	Coalfire Systems, Inc.				
Lead QSA Contact Name:	Lenard Melton		Title:	Security Consultant (QSA)	
Telephone:	303-554-6333		E-mail:	CoalfireSubmission@Coalfire.com	
Business Address:	11000 Westmoor Circle, Suite 450		City:	Westminster	
State/Province:	CO	Country:	USA	Zip:	80021
URL:	https://www.coalfire.com				

Part 2. Executive Summary

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

☒ Retailer	☐ Telecommunication	☒ Grocery and Supermarkets
☐ Petroleum	☐ E-Commerce	☐ Mail order/telephone order (MOTO)
☐ Others (please specify): N/A		

What types of payment channels does your business serve?	Which payment channels are covered by this assessment?
☒ Mail order/telephone order (MOTO)	☒ Mail order/telephone order (MOTO)
☒ E-Commerce	☒ E-Commerce
☒ Card-present (face-to-face)	☒ 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?	Avanti Market Systems (Avanti) is a Level 1 merchant that offers self-service refreshment kiosks to various markets across the United State and international markets. Avanti sells food and beverages through a self-service kiosk for their customers that include private companies, hotels, transportation centers, multi-tenant building and medical centers. Avanti has 250+ market operators as well as 10,000+ market locations throughout the United States and international locations. Avanti accepts cardholder data through their Point of Interaction devices at the kiosks locations as well as through e-Commerce to reload the Avanti MyMarketCard (MMC).

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)
Corporate Office	1	Renton, WA, USA
Kiosk Locations	10,360	Various Locations, USA
Azure Data Center	1	Washington, USA

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)
TransArmor Data Protection	SaaS	First Data	☐ Yes ☒ No	Not Applicable

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.*	**Kiosk Locations:** Avanti Markets (Avanti) accepts card transactions through Ingenico iUC285 devices located at the Avanti kiosks in exchange for food or beverages. The customer will complete payment through swipe, insert or through Near-field Communication Contactless Payment (NFC). Full track or EVM data is encrypted at swipe utilizing the TransArmor Data Protection payment solution and forwarded to Avanti's acquiring bank (Bank of America Merchant Services) for authorization and payment of the transaction. BAMS provides a response back to Avanti which includes first 6 and last 4 of card number, expiration month and year, card type and TransactionID. Avanti stores this response

data within the SQL database "AvantiProduction". Avanti does not have access to encryption keys for the TransArmor Data Protection solution and does not store sensitive authentication data or full card numbers.

E-Commerce/Mobile App:
Avanti offers customers a "My Market Card" where they can load money onto the cards to purchase goods from the Avanti Kiosks. To deposit money into the My Market Card, customers will navigate to "MyMarketCard.com" and select "Add New Payment Option" button. The Avanti customer will then be redirected to a Payeezy screen that is hosted by First Data where they will complete their payment by entering Cardholder Name, Credit Card Number and Expiration Date. After selecting "Pay with your Credit Card" option and waiting for authorization the customer is redirected back to the Avanti page.

- CHD is not processed by Avanti.
- Customer reimbursement service – Payeezy & CyberSource
- Locker delivery service website featuring order/pay ahead functionality utilizing Avanti market cards, Payeezy, and CyberSource
- CHD is collected by either First Data's Payeezy or Visa's CyberSource product. When a consumer uses the My Market Card (MMC) website to reload their MMC, Avanti's application redirects credit card related portions of the screen to either Payeezy or CyberSource. Consumers then enter their CHD directly into the Payeezy or CyberSource web forms.
- All processing of CHD is performed by Payeezy or CyberSource. Global Gateway or CyberSource process the payment and return the transaction details (excluding CHD) to Avanti's MMC website. Return data includes transaction related information along with the first 6 and last 4 of the PAN, but not the full PAN. If the customer requested automatic reloads, a pre-authorization token is returned by Payeezy or CyberSource, which can be used to submit future transactions. The token does not contain clear-text PAN.
- All Authorization is done through the Payeezy or CyberSource systems

	and is not in-scope for the Avanti Platform **Over the Phone Return Process:** Avanti maintains a return process for customers. Customer will complete an online return request form from Avanti (https://www.avantimarkets.com/contact-us) which includes email, issue description, type of issue and priority. Avanti support staff will review the request and determine if a refund is necessary. If found necessary, then an Avanti support staff will set up a call with the customer and call them over a POTs line within a secure room (key and lock) within the Avanti corporate office. Avanti support staff will process the return through a Payeezy screen hosted by First Data and request the following information from the customer for the refund: Order Amount, Card Holder's Name, Credit Card Number and Expiration Date.
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:	Not Applicable
QIR Individual Name:	Not Applicable
Description of services provided by QIR:	Not Applicable
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:**
Microsoft Azure	Hosting of Data Center and E-Commerce Code
First Data Merchant Services	Payment Processing Activities
Payeezy	Outsourced Third Party E-Commerce Payment Page
CyberSource	Outsourced Third Party E-Commerce Payment Page

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:	03/22/2022	
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 *03/22/2022*

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 *Avanti Market Systems* 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 *Not Applicable* 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 your acquirer or 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
Not Applicable	Not Applicable

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 *3.2.1*, 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 Not Applicable

Part 3b. Merchant Attestation

DocuSigned by:
John Reilly
441077197FDE44D...

Signature of Merchant Executive Officer ↑	*Date:* 03/22/2022
Merchant Executive Officer Name: **John Reilly**	*Title:* **President**

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

If a QSA was involved or assisted with this assessment, describe the role performed:	Conducted a PCI DSS v3.2.1 onsite assessment and documented compliance results in a Report on Compliance (ROC) and associated Attestation of Compliance (AOC).

DocuSigned by:
Ryan Bigelow
A211DB7D38314F2...

Signature of Duly Authorized Officer of QSA Company ↑	*Date:* 03/22/2022
Duly Authorized Officer Name: **Ryan Bigelow**	*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 ISA was involved in this 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 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	☒	☐	N/A
2	Do not use vendor-supplied defaults for system passwords and other security parameters	☒	☐	N/A
3	Protect stored cardholder data	☒	☐	N/A
4	Encrypt transmission of cardholder data across open, public networks	☒	☐	N/A
5	Protect all systems against malware and regularly update anti-virus software or programs	☒	☐	N/A
6	Develop and maintain secure systems and applications	☒	☐	N/A
7	Restrict access to cardholder data by business need to know	☒	☐	N/A
8	Identify and authenticate access to system components	☒	☐	N/A
9	Restrict physical access to cardholder data	☒	☐	N/A
10	Track and monitor all access to network resources and cardholder data	☒	☐	N/A
11	Regularly test security systems and processes	☒	☐	N/A
12	Maintain a policy that addresses information security for all personnel	☒	☐	N/A
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	☒	☐	N/A