Payment Card Industry
Data Security Standard

Attestation of Compliance for Report on Compliance - Merchants

Version 4.0.1

Publication Date: August 2024

PCI DSS v4.0.1 Attestation of Compliance for Report on Compliance - Merchants

Entity Name: Eventbrite, Inc.

Date of Report as noted in the Report on Compliance: 2025-03-14

Date Assessment Ended: 2025-03-06

Section 1: Assessment Information

Instructions for Submission

This Attestation of Compliance (AOC) must be completed as a declaration of the results of the merchant's assessment against the *Payment Card Industry Data Security Standard (PCI DSS) Requirements and Testing Procedures* ("Assessment"). Complete all sections. The merchant 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:	Eventbrite, Inc.
DBA (doing business as):	Not Applicable
Company mailing address:	95 Third Street, 2nd Floor San Francisco, CA 94103
Company main website:	https://www.eventbrite.com
Company contact name:	Vivek Sagi
Company contact title:	Chief Technology Officer (CTO)
Contact phone number:	312-882-4025
Contact e-mail address:	vivek@eventbrite.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):	Not Applicable
Qualified Security Assessor	
Company name:	Coalfire Systems, Inc.
Company mailing address:	8480 E Orchard Rd, Suite 5800 Greenwood Village, CO 80111
Company website:	https://www.coalfire.com
Lead Assessor name:	Christy Belknap
Assessor phone number:	877-224-8077
Assessor e-mail address:	CoalfireSubmission@coalfire.com

Assessor certificate number:	206-020

Part 2. Executive Summary

Part 2a. Merchant Business Payment Channels (select all that apply): (ROC Sections 2.1 and 3.1)

Indicate all payment channels used by the business that are included in this Assessment.

☐ Mail order / telephone order (MOTO)

☒ E-Commerce

☒ Card-present

Are any payment channels not included in this Assessment?	☐ Yes ☒ No
If yes, indicate which channel(s) is not included in the Assessment and provide a brief explanation about why the channel was excluded.	Not Applicable

Note: *If the merchant has a payment channel that is not covered by this Assessment, consult with the entity(ies) to which this AOC will be submitted about validation for the other channels.*

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

For each payment channel included in this Assessment as selected in Part 2a above, describe how the business stores, processes, and/or transmits account data.

Channel	How Business Stores, Processes, and/or Transmits Account Data
Authorization	Card-not-present transaction: • Eventbrite Website/ Eventbrite Mobile Web/ Eventbrite iOS and Android Native Attendee Application/ iOS Organizer / Eventbrite iOS and Android Organizer Mobile Application/ Ticket Transfers/ Embedded Checkout/ Pay Invoices/ Pay Refund Recharge: Eventbrite's web front end receives payment information consisting of PAN, card expiration date, and card validation values (CVV2, CVC2, CID) and communicates to the Payments server using (SOA) via HTTPS using TLS 1.2 with AES 256-bit encryption. The Payments server encrypts card data with Eventbrite 2048-bit RSA key and is retained in the server in- process memory until it is needed for transmission outbound to the selected payment processor. The PAN, card expiration date, and card validation values (CVV2, CVC2,CID) are then transferred to the payment processor server, which encapsulates all operations of processing a transaction. It includes choosing the correct payment gateway: ○ Authorize.net: TLSv1.2 with ECDHE-RSA-AES256-GCM-SHA384-bit encryption. ○ Braintree: TLSv1.2 with ECDHE-RSA-AES128-GCM-SHA256-bit encryption. ○ Cybersource: TLSv1.2 with ECDHE-RSA-AES256-GCM-SHA384-bit encryption. ○ Adyen: TLSv1.2 with ECDHE-RSA-AES128-GCM-SHA256-bit encryption. The payment gateway also performs payment processing, submitting requests, error processing, logging, journaling, and tokenization of the

response. Post authorization, cardholder data is released from the in-process memory and overwritten as new transactions are processed.

Eventbrite only stores the truncated PAN (last four digits of the PAN or first six and last four digits of the PAN) and the reference token in the EBProd and ProdPayments MySQL 5.7 databases. Eventbrite does not store cardholder data to file, disk, or database.

- Partner Flow Using Card Data: The load balancers will forward the data token to the API server which then passes the Braintree or Cybersource nonce to the payment service server for payment processing. Payment service servers process the notification by communicating with the order service which marks the order status complete and logs the last-4 in the database. Payment is added to payment systems for financial reconciliation, fees processing, and other internal back office financial processing needs. Braintree/Cybersource eventually will settle the funds with Eventbrite merchant banks.
- Partner Flow Using nonce: The payment service transmits CHD to the gateway for processing the payment via HTTPS using TLS 1.2 with AES 128-bit encryption. Payment service servers process the notification by communicating with the order service which marks the order status complete and logs the last-4 in the database. Payment is added to payment systems for financial reconciliation, fees processing, and other internal back office financial processing needs. Braintree eventually settles funds with Eventbrite merchant banks.

Card-present transactions:

- iOS Organizer Application (Manually entered payment card data): Inbound payment card data is received by Eventbrite's API servers. CHD consisting of PAN, card expiration date, and card validation values (CVV2, CVC2, CID) is transmitted to the Payments server via HTTPS using TLS 1.2 and AES 128-bit encryption, payment card data is encrypted with Eventbrite 2048-bit RSA key and retained in the server in- process memory until it is needed for transmission outbound to the selected payment processor. The PAN, card expiration date, and card validation values (CVV2, CVC2, CID) are then transferred to the payment processor server, which encapsulates all operations of processing a transaction. It includes choosing the correct payment gateway:
  - Authorize.net: TLSv1.2 with ECDHE-RSA-AES256-GCMSHA384-bit encryption.
  - Braintree: TLSv1.2 with ECDHE-RSA-AES128-GCM-SHA256-bit encryption.
  - Cybersource: TLSv1.2 with ECDHE-RSA-AES256-GCMSHA384-bit encryption.

  The payment gateway also performs payment processing, submitting requests, error processing, logging, journaling, and tokenization of the response. Post authorization, cardholder data is released from the in-process memory and overwritten as new transactions are processed. Eventbrite only stores the truncated PAN (last four digits of the PAN or first six and last four digits of the PAN) and the reference token in the EBProd and ProdPayments MySQL databases. Eventbrite does not store cardholder data to file, disk, or database.
- Stripe Terminal: The incoming payment information is transmitted to Stripe servers via HTTPS using TLS 1.2 and AES 256-bit encryption. The PAN is never reaching the Eventbrite servers or balancers. The payment completion data is saved by having the last 4 digits stored in

	the EB database. Payment is added to the system of record for financial reconciliation, fee processing and other internal back office financial processing needs. Bancontact and Adyen Transactions: Eventbrite's load balancers transmit incoming payment information to Eventbrite web servers via HTTPS using TLS 1.2 and AES 256-bit encryption. This information is then forwarded to the payment service servers after Adyen authorizes the transaction. The payment completion data is saved by having the last 4 digits stored in the EB database. Payment is added to the system of record for financial reconciliation, fee processing and other internal back office financial processing needs. Payment gateways eventually settle funds with Eventbrite's merchant bank account Wells Fargo.
Capture	Eventbrite captures payment data through these following channels: Card-not-present transaction: • Eventbrite Website: An attendee begins a transaction to purchase tickets to an event created by an organizer on the Eventbrite website using their web browser. During this process, the web server accepts the attendee's name, address, primary account number (PAN), card expiration date, and card validation value (CVV2, CVC2, CID) via TLS 1.2 with at least minimum of TLS_DHE_RSA_WITH_AES_128_CBC_SHA 128-bit encryption or higher supporting the most secure protocol and highest cipher that the attendee's web browser can negotiate. • Eventbrite Mobile Web: Eventbrite has a mobile attendee app for both the iOS (iPhone/iPad/iPod Touch) and Android platforms that let attendees purchase tickets to events. The attendee enters their name, address, PAN, card expiration date, and card verification values (CVV2, CVC2, CID). The Eventbrite mobile application is a "skinned" HTML5 web browser view. It uses the native smartphone web browser interface and communicates with Eventbrite's web servers over HTTPS using TLS 1.2 with at least minimum of TLS_DHE_RSA_WITH_AES_128_CBC_SHA128-bit encryption or higher supporting the most secure protocol and highest cipher that the attendee's native smartphone web browser can negotiate. • Eventbrite iOS and Android Native Attendee Application: Eventbrite provides mobile applications for use by their attendees to find events and buy tickets to these events. The applications are built by Eventbrite and are available for download on the iTunes App Store and Google Play App Store. The attendee enters their name, address, PAN, card expiration date, and card verification values (CVV2, CVC2, CID) similar to the Eventbrite Website. The iOS/Android application will first perform RSA 2048-bit asymmetric encryption of the data in-app using a public key published by the Eventbrite API. The encrypted data is then transmitted to Eventbrite load balancer servers via HTTPS using TLS 1.2 with at least minimum of TLS_DHE_RSA_WITH_AES_128_CBC_SHA 128-bit encryption or higher supporting the most secure protocol and highest cipher that the attendee's web browser can negotiate. • Ticket Transfers: In some cases, an attendee may have purchased tickets to one event and may want to transfer that ticket to another date. The transfer of this ticket, if allowed, may incur fees or differences in price, which need to be paid by the attendee. The website/ mobile web user interface will first get the old and new event/ ticket information and inform the attendee on how much money is owed. If they continue, another form will prompt them for payment card information to either get refunded or to pay the difference. The attendee enters their name,

address, PAN, card expiration date, and card verification values (CVV2, CVC2, CID) similar to the Eventbrite Website. Ticket transfers use the web browser interface and communicates with Eventbrite's web servers over HTTPS using TLS 1.2 with at least minimum of TLS_DHE_RSA_WITH_AES_128_CBC_SHA 128-bit encryption or higher supporting the most secure protocol and highest cipher that the attendee's native smartphone web browser can negotiate.

- Embedded Checkout: The Embedded Checkout is a Widget inside an iFrame that connects to Eventbrite website over HTTPS using TLS 1.2 with AES 128-bit encryption. Data including cardholder name, PAN, card expiration date is provided as part of the ticket purchase flow.
- Pay Invoices/Pay Refund Recharge Flow: There are a variety of event configurations where Eventbrite is facilitating the transaction. In these cases, while Eventbrite does not charge credit card processing fees, Eventbrite still has a per-ticket fee that needs to be paid back. This fee is collected through a web user interface. The user receives an email indicating they owe fees with a link to their account details. After logging in, the user will see the "Pay Via Credit Card" option. The customer enters their PAN, card expiration date, and card verification values (CVV2, CVC2, CID) like the Eventbrite Website. Pay Invoices uses the web browser interface and communicates with Eventbrite's web servers over HTTPS TLS 1.2 with at least minimum of TLS_DHE_RSA_WITH_AES_128_CBC_SHA 128-bit encryption or higher supporting the most secure protocol and highest cipher that the attendee's native smartphone web browser can negotiate.
- A similar payment flow methodology is followed by Pay Refund Recharge, where an attendee requests a refund from an organizer after the accounts have been settled with Eventbrite. In order to cover the cost of refund, the organizer is requested to provide their credit card to process a payment or the amount they need to recharge their account. They will then see a page asking them to 'Enter their Credit / Debit card info.' This page will gather the customer's PAN, card expiration date, and card verification values (CVV2, CVC2, CID) similar to the Eventbrite Website.
- Facebook API: Eventbrite and Facebook have launched a partnership that allows attendees to find events they wish to attend through their social network on Facebook and then purchase tickets for these events directly on the Facebook platform. The user on the Facebook platform (Event attendee) initiates the purchase process. Attendees find an update in their newsfeed or on an organizer's page. From this point, the customer can immediately click a "Buy Now" button. They will be presented with a user interface that allows them to select the number of tickets they wish to purchase. Facebook will then collect the payment card data (name, PAN, CVV, expiration date) from the user and transmit this information to the Braintree systems for processing.
- Partner Flow Using Card Data: This flow is for partner systems but using card data. The partner system transmits the data token containing customer's name, PAN, card expiration date and card verification values (CVV2, CVC2, CID) over to the Partner API, which forwards the nonce to the front end CloudFront load balancers using HTTPS with TLS 1.2 and AES 128-bit encryption.
- Partner Flow Using nonce: Partner system sends the data token (name, PAN, CVV, expiration date) and initial payment details to Braintree which returns a reply with nonce to Eventbrite load balancer. The load balancer will forward the nonce to the payment service server for processing.

	Card-present transaction: • iOS Organizer Application (Manually entered payment card data): The event organizers can manually key-in the PAN, card expiration date, and card verification value (CVV2, CVC2, CID) into the Eventbrite iOS/Android application if the card reader cannot read the card magnetic stripe data. Manually entered card data is encrypted at the point of capture by the Eventbrite iOS/Android application using RSA asymmetric (public/private key) encryption with an Eventbrite 2048 bit RSA public key and transmitted to the Eventbrite API servers via HTTPS using TLS 1.2 with at least TLS_DHE_RSA_WITH_AES_256_CBC_SHA bit encryption or higher supporting the most secure protocol and highest cipher that the event organizer's native mobile device web browser can negotiate. • Stripe Terminal: the OrganizerApp (OrgApp) is used as a tap-to-pay option. After selecting Stripe in the OrgApp, it requests a temporary Stripe token from the payments_service (using HTTPS with TLS 1.2 and AES 28-bit encryption). The OrgApp creates a payment_intent within Stripe and requests PAN (the card is tapped to the device with the OrgApp). After that the payment is processed within Stripe and then finalized on the Payments server. Bancontact and Adyen Transactions: The attendee places an order using their Bancontact payment card on the desktop application. Then a data token requesting cardholder name, PAN, card expiration date is routed to the payment service server over HTTPS using TLS 1.2 with AES 128-bit encryption; payment information is then routed to Adyen IPN System over HTTPS using TLS 1.2 with AES 128-bit encryption to be authorized.
Settlement	As a merchant, Eventbrite indirectly supports the Settlement process, as there is no payment card data involved. Once an event attendee purchases a ticket for an event, the funds flow through the payment processors into Eventbrite Wells Fargo merchant bank accounts (account will vary based on currency). Eventbrite does not have a real-time process that reconciles "order to cash" from Wells Fargo to the processor daily. There is an order to cash reconciliation that is done in arrears, where payment processor data is compared to Wells Fargo data and discrepancies are investigated and resolved. Eventbrite settlement/finance personnel access payment transactions data via HTTPS TLS 1.2 with AES 256-bit encryption connection to the payment processor administered settlement site for the purposes of adjusting or refunding the charged amount. Eventbrite personnel do not view full PAN in the process. Also, full PAN is never stored in the process.
Chargeback	Eventbrite chargeback/finance personnel login to a secure virtual portal of processors such as (Well Fargo portal, Braintree, Adyen) via HTTPS TLS1.2 with AES 128-bit encryption and download chargeback data files in Excel/CSV format. These files contain only truncated (first six and last four digits of the PAN). The employee will then upload the report to the Eventbrite Administrative Console (Chargeback tool) where the reports will be parsed, and a "matching" process will take place. This process attempts to match the transactions in the Eventbrite system with the reported Chargeback based on the last four digits of the PAN, Transaction Date/Time, and Transaction Amount. If there is a match, then the system marks it as matched. Any mismatched transactions are reported back to the Eventbrite Finance team for manual reconciliation of adjusting or refunding the charged amount. Full PAN is never visible in this process.
Facilitated Payments	PayPal: Eventbrite allows organizers to configure their events to accept PayPal as a method of payment. In this case, Eventbrite redirects the customer's browser or mobile application to the PayPal site upon which the PayPal IPN system is connected for internal processing. The attendee enters transaction details including the PAN, card expiration date, and card verification values (CVV2, CVC2, CID) directly to the PayPal web pages from their web browser via the

	redirect using HTTPS/TLS 1.2 with at least minimum TLS_DHE_RSA_WITH_AES_128_CBC_SHA 128-bit encryption for authorization.

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.*	Eventbrite's CDE is entirely hosted in dedicated AWS cloud hosting environments, which are physically and logically separated from the company's corporate offices and development/testing environments. There are no direct physical or point-to-point Virtual Private Network (VPN) connections between the production CDE cloud environment and the Eventbrite corporate office network or the development/testing environments. The CDE is segmented from non-CDE systems using virtual firewalls and Access Control Lists (ACLs). Inbound access from the Internet is allowed over a secure protocol and the highest cipher that the customer's browser can negotiate to access the Eventbrite web applications and to accept payment transactions. Remote access to the CDE is restricted via session-based VPN, bastion hosts enabled with multi-factor authentications. Outbound connections are restricted to necessary ports and protocols to support forwarding transactions to payment processors for authorization. The following support systems within the CDE were assessed: • Virtual firewalls (security groups) • Servers • Load balancers • Server configuration management • Multi-factor authentication • Access authorization • Audit log collection and analysis • Network time synchronization • Host-based Intrusion Detection System (HIDS) • File Integrity Monitoring (FIM) • Anti-virus • Change control management • External ASV vulnerability scanning • Internal vulnerability scanning • Penetration testing
Indicate whether the environment includes segmentation to reduce the scope of the Assessment. Refer to "Segmentation" section of PCI DSS for guidance on segmentation.	☒ Yes ☐ No

Part 2. Executive Summary *(continued)*

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

List all types of physical locations/ facilities (for example, retail locations, 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)
Data Centers	2	AWS Cloud Hosting (Region & Availability Zones): • US-East-1 (North Virginia) • US-West-2 (Oregon)
Headquarters	1	San Francisco, California, United States
Corporate Office	1	Godoy Cruz, Mendoza, Argentina
Corporate Office	1	Mahon, Cork, Ireland
Corporate Office	1	Madrid, Spain
Corporate Office	1	Hyderabad, Telangana, India
Corporate Office	1	Melbourne, Victoria, Australia
Corporate Office	2	London, United Kingdom
Corporate Office	1	Nashville, Tennessee, United States
Corporate Office	1	San Francisco, California, United States

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
Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable

* 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) (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)

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)	☒ Yes ☐ No
• Manage system components included in the scope of the Assessment (for example, via network security control services, anti-malware services, security incident and event management (SIEM), contact and call centers, web-hosting services, and IaaS, PaaS, SaaS, and FaaS cloud providers)	☒ Yes ☐ No
• Could impact the security of the entity's CDE (for example, vendors providing support via remote access, and/or bespoke software developers).	☐ Yes ☒ No

If Yes:

Name of Service Provider:	Description of Service(s) Provided:
Amazon Web Services, Inc.	Cloud Hosting Provider
PayPal, Inc.	Payment Processing
Cybersource Corporation	Payment Processing
Adyen N.V.	Payment Processing
Mercado Libre, Inc. (Mercado Pago)	Payment Processing
Stripe, Inc.	Payment Processing
Okta, Inc.	Authentication Services
Wiz.io	Security Servies

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.

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:	☒	☒	☐	☐	☐
Requirement 2:	☒	☒	☐	☐	☐
Requirement 3:	☒	☒	☐	☐	☐
Requirement 4:	☒	☒	☐	☐	☐
Requirement 5:	☒	☒	☐	☐	☐
Requirement 6:	☒	☒	☐	☐	☐
Requirement 7:	☒	☒	☐	☐	☐
Requirement 8:	☒	☒	☐	☐	☐
Requirement 9:	☒	☒	☐	☐	☐
Requirement 10:	☒	☒	☐	☐	☐
Requirement 11:	☒	☒	☐	☐	☐
Requirement 12:	☒	☒	☐	☐	☐
Appendix A2:	☐	☒	☐	☐	☐

Section 2 Report on Compliance

(**ROC Sections 1.2 and 1.3**)

Date Assessment began: ***Note:*** *This is the first date that evidence was gathered, or observations were made.*	2025-03-14
Date Assessment ended: ***Note:*** *This is the last date that evidence was gathered, or observations were made.*	2025-03-06
Were any requirements in the ROC unable to be met due to a legal constraint?	☐ Yes ☒ No
Were any testing activities performed remotely?	☒ Yes ☐ 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 2025-03-14)*.

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)**:***

☒	**Compliant:** 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 **COMPLIANT** rating; thereby *Eventbrite, Inc.* has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above.
☐	**Non-Compliant:** 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 **NON-COMPLIANT** rating; thereby *Not Applicable* has not demonstrated compliance with PCI DSS requirements. **Target Date** for Compliance: Not Applicable 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.
☐	**Compliant but with Legal exception:** 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 **COMPLIANT BUT WITH LEGAL EXCEPTION** rating; thereby *Not Applicable* 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. This option requires additional review from the entity to which this AOC will be submitted. *If selected, complete the following:*

Affected Requirement	Details of how legal constraint prevents requirement from being met
Not Applicable	Not Applicable

Part 3. PCI DSS Validation *(continued)*

Part 3a. Merchant Acknowledgement

Signatory(s) confirms:

(Select all that apply)

☒	The ROC was completed according to *PCI DSS*, Version 4.0.1 and was completed according to the instructions therein.
☒	All information within the above-referenced ROC and in this attestation fairly represents the results of the Assessment in all material respects.
☒	PCI DSS controls will be maintained at all times, as applicable to the entity's environment.

Part 3b. Merchant Attestation

Vivek Sagi

Signature of Merchant Executive Officer ↗	Date: 3/14/2025 | 3:48 PM MDT
Merchant Executive Officer Name: Vivek Sagi	Title: Chief Technology Officer (CTO)

Part 3c. Qualified Security Assessor (QSA) Acknowledgement

If a QSA was involved or assisted with this Assessment, indicate the role performed:	☒ QSA performed testing procedures.
	☐ QSA provided other assistance. If selected, describe all role(s) performed:

Signature of Lead QSA ↗	Date: 3/14/2025 | 2:49 PM PDT
Lead QSA Name: Christy Belknap	

Juston Glenn

Signature of Duly Authorized Officer of QSA Company ↗	Date: 3/14/2025 | 4:06 PM MDT
Duly Authorized Officer Name: Juston Glenn	QSA Company: Coalfire Systems, 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:	☐ ISA(s) performed testing procedures.
	☐ 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	☐	☐	
2	Apply secure configurations to all system components	☐	☐	
3	Protect stored account data	☐	☐	
4	Protect cardholder data with strong cryptography during transmission over open, public networks	☐	☐	
5	Protect all systems and networks from malicious software	☐	☐	
6	Develop and maintain secure systems and software	☐	☐	
7	Restrict access to system components and cardholder data by business need to know	☐	☐	
8	Identify users and authenticate access to system components	☐	☐	
9	Restrict physical access to cardholder data	☐	☐	
10	Log and monitor all access to system components and cardholder data	☐	☐	
11	Test security systems and networks regularly	☐	☐	
12	Support information security with organizational policies and programs	☐	☐	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	☐	☐	

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/