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: 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 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:	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. Scope Verification

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

Name of service(s) assessed:	Eventbrite Monetization Suite Platform

Type of service(s) assessed:

Hosting Provider:	**Managed Services:**	**Payment Processing:**
□ 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):	□ Systems security services □ IT support □ Physical security □ Terminal Management System ☒ Other services (specify): Cloud-based application platform	☒ 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):		

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:	None
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:	Not Applicable

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.	Eventbrite, Inc. is a global marketplace for live experiences that allow event organizers to plan, promote, and sell tickets to events (event management) and publish them across social-networking sites (Facebook, Twitter, etc.) directly from the site's interface. Eventbrite's platform also enables attendees to find and purchase tickets for these experiences. Eventbrite is headquartered in San Francisco, California, United States (US) with offices in Madrid, Cork, London, Hyderabad, Mendoza, and Melbourne. However, the scope of this assessment includes only the locations in the US.

	Eventbrite's cardholder data environment (CDE) is hosted in Amazon Web Services (AWS) Elastic Cloud Compute (EC2) datacenters in AWS-US-East (Northern Virginia) and AWS-US-West (Oregon) used for backup/recovery. AWS is a PCI-DSS v4.0 Level 1 validated Service Provider with an AOC dated 2024-06-13. For the purposes of this PCI DSS assessment, Eventbrite is validating PCI DSS compliance as a Level One Merchant and a Level One Service Provider.
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	The Eventbrite platform enables event organizers to sell tickets and manage registrations. Event attendees can purchase tickets for these experiences. Eventbrite facilitates processing, transmission, and storage of payment card payment transactions on behalf of merchant customers and as a service provider. **Merchant:** Eventbrite acts as the merchant of record (MOR) for the payment transactions. The customer (event organizer) does not need to have a merchant account to sell tickets. Eventbrite will settle payment transactions on behalf of the organizer, then fund the organizer's bank account with the proceeds via check or direct deposit. Eventbrite uses payment processors Braintree, Cybersource, Mercado Pago, Adyen, and Auth.net for authorizing the payment card transactions. PayPal, Amex, and Stripe are also used for processing credit card payments; however, Eventbrite does not have access to any card data when these processors are used. Eventbrite reviews the appropriate PCI-DSS forms for all payment processors, for conformity with their PCI-DSS requirements. **Service Provider:** Direct funding is available to event organizers who already have their own Merchant ID and have set up an account with payment processors, Authorize.net. With this option, the event organizer is the merchant of record for the payment transaction and Eventbrite processes the payment card transactions and then deposits the collected funds directly into the customer's merchant account.
Describe system components that could impact the security of account data.	Eventbrite receives, processes, and transmits cardholder data via the payment methods and channels described below: **<u>Card-not-present transactions:</u>** **Desktop / Mobile Web:** An attendee begins a transaction to purchase tickets to an event on the Eventbrite website, either on their desktop browser or on the browser of their smartphone or tablet, chooses the ticket type and quantity, then are redirected to a checkout page. During the checkout process, the attendee is prompted to manually enter their personal information (name, address), primary account number (PAN), card expiration date, and card validation value (CVV2, CVC2, CID). This information is transmitted

inbound via HTTPS using TLS (Transport Layer Security) 1.2 with at least TLS_DHE_RSA_WITH_AES_128_CBC_SHA 128-bit encryption and maximum of TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 256-bit encryption, supporting the most secure protocol and strongest cipher that the attendee's web browser can negotiate to Eventbrite's front end Load Balancers which terminate the TLS connection and forward the transaction information to Eventbrite's API; the web front end forward the payment information to Eventbrite's Payment servers via HTTPS using TLS 1.2 with AES-256-bit encryption. In the Payments server, 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 Eventbrite's Payment Gateway. The PAN, card expiration date, and card validation values (CVV2, CVC2, CID) are then securely transmitted outbound from the Payment Servers to the supported payment processors using the following transmission protocols:

- 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.
- Mercado Pago: TLSv1.2 with ECDHE-RSA-AES128-GCM-SHA256-bit encryption.
- PayU: TLSv1.2 with ECDHE-RSA-AES128-GCM-SHA256-bit encryption.
- Amex: TLSv1.2 with ECDHE-RSA-AES128-GCM-SHA256-bit encryption.

The Payment Gateway performs additional functions including submitting requests, error processing, logging, journaling, and tokenization of cardholder data. Post authorization, cardholder data is released from the Payment Server's in-process memory and overwritten as new transactions are processed. Eventbrite stores first name, last name, expiration date, truncated PAN (last four digits of the PAN or first six and last four digits of the PAN) and reference token cardholder data in the MySQL 5.7 AWS Aurora databases (EBProd and ProdPayments).

iOS and Android Native Attendee Application: Eventbrite provides mobile applications for use by event attendees to find events and purchase 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 attendees enter their name, address, PAN, card expiration date, and card verification values (CVV2, CVC2, CID) similar to the Eventbrite ecommerce 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 front end CloudFront 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 and maximum of TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 256-bit encryption or higher supporting the most secure protocol and highest cipher that the attendee's web browser can negotiate; Eventbrite uses AWS native CloudFront Content Delivery Network (CDN), Web Application Firewall (WAF), and Application Load Balancer (ALB), collectively called AWS Shield, the TLS termination from the customers happens at the CloudFront layer, which is very close to the customers. The terminal TLS connection happens between CloudFront and ALB. This is finally forwarded to Eventbrite's API. The transaction data is then transmitted to Eventbrite API servers. Once the API servers receive the encrypted data, it is decrypted to cleartext using the 2048-bit RSA private key. This payment card data is forwarded from the API servers to the Payments servers for payment processing. The PAN, card expiration date, and card validation values (CVV2, CVC2, CID) are then securely transmitted outbound from the Payment Servers to the supported payment processors. Payment processing from the Payments server is handled in exactly the same way as detailed above for the Eventbrite Website. **Tokenized Wallets:** In Q2 2022 Payments added the capability for attendees to purchase tickets using mobile payment wallets: Apple Pay & Google Pay. Both of these mobile payment systems are integrated through processing rails with Braintree. There is an SDK utilized within the Checkout application that allows Eventbrite to present the payment method, so long as the SDK call deems the method is available (i.e. the Apple device supports Apple Pay). All processing data and card information is managed between Apple/Google & Braintree as the verification is either done using consumer biometrics or PIN validation (Google). **iOS and Android Organizer Mobile Application:** Eventbrite provides mobile applications that allow event organizers to accept card-present payments when selling tickets "at the door". The mobile applications are developed internally by Eventbrite and available at the Apple / Android stores. Apple iOS/Android applications are developed for use by event organizers and venue managers. These applications support manual card entry. The following describes the manual card entry payment processing flow: The event organizers manually key-in the cardholder's PAN, card expiration date, card verification value (CVV2, CVC2, CID) and ZIP code into the Eventbrite iOS/Android application. Manually entered card data is immediately 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 securely transmitted inbound over the Internet to Eventbrite CloudFront load balancers/API servers via TLS 1.2 with minimum TLS_DHE_RSA_WITH_AES_128_CBC_SHA 128-bit encryption and maximum of TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 256-bit encryption, supporting the most secure protocol and highest cipher that the event organizer’s mobile application can negotiate. The API servers via the embedded order service API passes encrypted key blob to Amazon KMS. Once KMS decrypts the data-encrypting key, the card data is encrypted and stored in Redis. After this, the API servers will fetch the card data from Redis, delete the key from Redis, and resubmit the data back to the payment service via the payment service HTTPS SOA client. During this process, the encrypted data is stored in Redis only in-memory and data that is stored for more than 120 minutes is securely deleted using the Redis eviction component (deletion procedure in Redis). The transaction is handled in API server memory only and authorization of payment card transaction is handled in the same methods as noted above in the Eventbrite website section. Post authorization, Eventbrite does not store cardholder data to file, disk, or database; no payment card information is written, stored, or logged to any systems or within the application. **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 attendees enter their name, address, PAN, card expiration date, and card verification values (CVV2, CVC2, CID) similar to the Eventbrite website data flow discussed above. Ticket transfers use the web browser interface and communicates with Eventbrite’s web servers via TLS 1.2 with at least minimum of TLS_DHE_RSA_WITH_AES_128_CBC_SHA 128-bit encryption and maximum of TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 256-bit encryption or higher supporting the most secure protocol and highest cipher that the attendee’s native smartphone web browser can negotiate. Payment card data received by this channel is handled the same way as detailed above for the Eventbrite website. Eventbrite does not store cardholder data to file, disk, or database. **Embedded Checkout Widget Transactions (iFrame):** The Embedded Checkout is a widget inside an iFrame that connects to the Eventbrite website over HTTPS using TLS 1.2 with AES 128-bit encryption. Data including cardholder name, PAN and card expiration date is provided as part of the ticket purchase flow. The

	request is forwarded to the front end CloudFront load balancers which forwards it to the API servers. The API servers then submit the card data to payment service servers for payment processing. The payment service abstracts the process of transaction authorization and connects to the proper gateway to complete the transaction. Braintree, Cybersource and Adyen are payment gateways which settle the funds with the bank accounts and return the tokenized form of the PAN. This is stored in the payments database along with truncated PAN. Eventbrite does not store cardholder data to file, disk, or database. **PayPal Embedded Checkout:** In an embedded checkout flow, the PayPal button redirects the event attendee to a PayPal page where they can log in. Here PayPal communicates with Braintree and requests a nonce which is sent to the browser. The nonce is then forwarded to the front end CloudFront load balancers using HTTPS with TLS 128-bit encryption, which is then forwarded to Eventbrite's order service server. The order service then passes the nonce to the payment service server which then talks to Braintree and PayPal. Order service uses the response from the payment service server and the payment is added to systems of record for financial reconciliation, fees processing and other internal back-office needs. Braintree eventually settles funds with the merchant banks. **Pay Invoices / Pay Refund Recharge Transaction:** As part of the Eventbrite service, Eventbrite collects a variety of fees for use of the service. In most cases, Eventbrite acts either as the merchant of record or service provider, so the fees incurred in the transaction are deducted from the total being paid out to the organizer leaving them with a net gross for their event. However, 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 organizer receives an email indicating they owe fees with a link to their account details. After logging in, the organizer will see the "Pay Via Credit Card" option and then 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 using TLS 1.2 with at least minimum of TLS_DHE_RSA_WITH_AES_128_CBC_SHA 128-bit encryption and maximum of TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 256-bit encryption higher supporting the most secure protocol and highest cipher that the attendee's web browser can negotiate. Payment card data received by this channel is handled the same way as detailed above for the Eventbrite website dataflow. Eventbrite does not store cardholder data to file, disk, or database.

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 for 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) like the Eventbrite website. Payment card data received by this channel is handled the same way as detailed above for the Eventbrite website dataflow. Eventbrite does not store cardholder data to file, disk, or database.

Partner Flow Using Card Data: This particular 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. 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’s merchant banks.

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 attendees can find events in their newsfeed or an organizer’s page. The event attendee initiates the purchase process on the Facebook platform. From this point, the event attendee can immediately click the "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 event attendee and transmit this information to Braintree for processing. Braintree will process the transaction and return status information back to Facebook. When the transaction is complete, Facebook will redirect the event attendee to the Eventbrite systems with information about the transaction via TLS 1.2 with at least minimum TLS_DHE_RSA_WITH_AES_128_CBC_SHA 128-bit encryption to the Eventbrite load balancers / API servers indicating the success/failure of the transaction including payment amount, transaction ID and last 4 digits of the PAN. This information is forwarded to the payment service server, which communicates with the

	order service server marking the order complete and logging the last 4 digits of the transactions to the EB and Payments databases. Payment is added to the system for record for financial reconciliation, fees processing and other internal back-office needs. Facebook eventually settles the funds with Eventbrite's merchant banks. **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. 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. **<u>Card-present transactions:</u>** **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. 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. The POI device used in this channel is provided by Stripe, direct to the customer. **Bancontact and Adyen Transactions:** The attendee places an order using their Bancontact payment card on the desktop application. A data token requesting the cardholder's name, PAN and card expiration date is routed to the payment service server using HTTPS with TLS 1.2 and AES 128-bit encryption which routes to Adyen Instant Payment Notification (IPN) System to be authorized. Adyen then authenticates the card via 3DSecure and the user is redirected to a page owned by the card issuer bank. Adyen replies with payment session data. The user confirms his credentials using a Quick Response (QR) code/Scan/Credentials/PIN Number. The load balancers then pass on this payment information to Eventbrite web servers. 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. The payment gateways eventually settle funds with Eventbrite's merchant bank account, Wells Fargo, except for Adyen and all international processing, which settles with JPMorgan. **Facilitated Payments:** Eventbrite also receives payment card transactions that are facilitated through PayPal and Authorize.net. In the case of facilitated payment card transactions, Eventbrite does not receive the payment details; the payment data is transmitted directly from the end user to the facilitated payment provider. After payment processing, only the status of the transaction is stored in Eventbrite databases. The payment flow for PayPal and Facebook is described below. **PayPal Desktop / Mobile Web:** 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 into 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. After authorization, PayPal returns a transaction status code, the last 4 digits of the PAN, and the expiration date, which is stored in Eventbrite EBProd and ProdPayments MySQL 5.6 databases. This process is fully outsourced to PayPal, a PCI DSS v3.2.1 validated payment processor with AOC dated 02/13/2024. Payment is added to the system for record for financial reconciliation, fees processing and other internal back- office needs. PayPal eventually settles funds with the organizer's merchant bank. Authorize.net Transactions: Eventbrite allows organizers to configure their events to accept Authorize.net as a method of facilitated payment. In these cases, after selecting a ticket type and quantity, the Eventbrite system redirects the event attendee's browser to the Authorize.net site to complete the transaction including entry of any CHD necessary to complete that transaction. CHD is transmitted using TLS 1.2 with AES 128-bit encryption. Upon completion, the attendee's browser is redirected back to the Eventbrite system where they finalize the order on the Eventbrite side and settle transactions with the organizer's merchant bank. Simultaneously, Authorize.net will send a unique card identifier to Eventbrite's payment service server which provides the success/failure of the transaction and the truncated PAN (first 6 digits and last 4 digits) from the Authorize.net side. This state is then recorded in both the EB and Payments Databases.

	Chargebacks: Eventbrite Finance team logs in over HTTPS TLS 1.2 to the various payment providers and settlement systems such as Well Fargo portal, Braintree, Adyen to acquire chargeback batch files. Batch files contain data tokens, truncated PAN (first six, last four) and other transaction information. These files are retrieved and uploaded over HTTPS TLS 1.2 to the Eventbrite Administrative console (Chargeback Tool). Chargeback batch files do not contain any sensitive cardholder data

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.*	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 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)
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 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
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)

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))	☒ Yes ☐ 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)	☒ 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 Services 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.

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: Eventbrite Monetization Suite Platform

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 A1:	□	☒	□	□	□
Appendix A2:	□	☒	□	□	□

Justification for Approach

For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.	1.4.4: Eventbrite does not store cardholder data. 2.2.5: No insecure services, protocols, or daemons present. 2.3.1, 2.3.2: No wireless connected to the CDE or transmitting account data. 3.3.2: Future dated requirement. 3.3.3: Eventbrite is not an issuer. 3.4.1, 3.4.2, 3.5.1, 3.5.1.1, 3.5.1.2, 3.5.1.3, 3.6.1, 3.6.1.1, 3.6.1.2, 3.6.1.3, 3.6.1.4, 3.7.1, 3.7.2, 3.7.3, 3.7.4, 3.7.5, 3.7.6, 3.7.7, 3.7.8, 3.7.9: Eventbrite does not store cardholder data. 4.2.1.2: No wireless connected to the CDE or transmitting account data. 4.2.2: Eventbrite does not transmit cardholder data via end-user messaging technologies. 5.2.3, 5.2.3.1: All systems are protected by an anti-malware solution. 5.3.2.1: Continuous behavioral analysis is performed to meet Requirement 5.3.2. 6.3.2, 6.4.3: Future dated requirement. 7.2.5.1: Future dated requirement. 7.2.6: Eventbrite does not store cardholder data. 8.2.3: Eventbrite does not have remote access (or any access) to customers' networks. 8.3.10, 8.3.10.1: Eventbrite does not provide customer access to cardholder data. 8.2.7: Third partes don't have remote access to Eventbrite's CDE. 8.5.1, 8.6.1, 8.6.2, 8.6.3: Future dated requirement. 9.4.1, 9.4.1.1, 9.4.1.2, 9.4.3, 9.4.4, 9.4.5, 9.4.5.1, 9.4.6, 9.4.7: No media with CHD. 9.5.1, 9.5.1.1, 9.5.1.2, 9.5.1.2.1, 9.5.1.3: No POI Devices. 10.4.2.1: Future dated requirement. 11.3.1.1, 11.6.1: Future dated requirement. 11.4.7: Not a multi-tenant service provider. 12.3.1, 12.3.2, 12.3.3, 12.5.2.1, 12.5.3, 12.10.4.1, 12.10.7: Future dated requirement. A1.1.1, A1.1.2, A1.1.3, A1.1.4: Not a multi-tenant service provider. A2.1.1, A2.1.2, A2.1.3: No POI devices in Eventbrite's CDE and is not responsible for customer owned POI devices.
For any Not Tested responses, identify which sub-requirements were not tested and the reason.	Not Applicable

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. Service Provider 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. Service Provider Attestation

Vivek Sagi

Signature of Service Provider Executive Officer ↑	Date: 3/14/2025 | 11:37 AM MDT
Service Provider 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 | 10:50 AM PDT
Lead QSA Name: Christy Belknap	

Juston Glenn

Signature of Duly Authorized Officer of QSA Company ↑	Date: 3/14/2025 | 12:25 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 A1	Additional PCI DSS Requirements for Multi-Tenant Service Providers	□	□	
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/