Payment Card Industry (PCI)
Data Security Standard

Attestation of Compliance for Onsite Assessments – Service Providers

Version 3.2.1

Revision 2

September 2022

Document Changes

Date	Version	Description
September 2022	3.2.1 Revision 2	Updated to reflect the inclusion of UnionPay as a Participating Payment Brand.

Section 1: Assessment Information

Instructions for Submission

This Attestation of Compliance must be completed as a declaration of the results of the service provider's assessment with the *Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS).* Complete all sections: The service provider is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the requesting payment brand for reporting and submission procedures.

Part 1. Service Provider and Qualified Security Assessor Information					
Part 1a. Service Provider Organization Information					
Company Name:	Eventbrite, Inc.		DBA (doing business as):	Not Applicable	
Contact Name:	Lanny Baker		Title:	Chief Financial Officer	
Telephone:	415-694-7900		E-mail:	lanny@eventbrite.com	
Business Address:	95 Third Street, 2nd Floor		City:	San Francisco	
State/Province:	CA	Country:	USA	Zip:	94103
URL:	https://www.eventbrite.com				

Part 1b. Qualified Security Assessor Company Information (if applicable)					
Company Name:	Coalfire Systems, Inc.				
Lead QSA Contact Name:	Christy Belknap		Title:	Senior Consultant	
Telephone:	877-224-8077		E-mail:	CoalfireSubmission@coalfire.com	
Business Address:	8480 E Orchard Rd., Suite 5800		City:	Greenwood	
State/Province:	CO	Country:	USA	Zip:	80111
URL:	https://www.coalfire.com				

Part 2. Executive Summary

Part 2a. Scope Verification

Services that were INCLUDED in the scope of the PCI DSS Assessment (check all that apply):

Name of service(s) assessed:	Eventbrite Monetization Suite Platform	
Type of service(s) assessed:		
Hosting Provider: ☐ Applications / software ☐ Hardware ☐ Infrastructure / Network ☐ Physical space (co-location) ☐ Storage ☐ Web ☐ Security services ☐ 3-D Secure Hosting Provider ☐ Shared Hosting Provider ☐ Other Hosting (specify):	**Managed Services (specify):** ☐ Systems security services ☐ IT support ☐ Physical security ☐ Terminal Management System ☒ Other services (specify): Cloud-based application platform	**Payment Processing:** ☒ POS / 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 you feel these categories don't apply to your service, complete "Others." If you're unsure whether a category could apply to your service, consult with the applicable payment brand.*

Part 2a. Scope Verification *(continued)*		
Services that are provided by the service provider but were NOT INCLUDED in the scope of the PCI DSS Assessment (check 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 ☐ Security services ☐ 3-D Secure Hosting Provider ☐ Shared Hosting Provider ☐ Other Hosting (specify):	**Managed Services (specify):** ☐ Systems security services ☐ IT support ☐ Physical security ☐ Terminal Management System ☐ Other services (specify):	**Payment Processing:** ☐ POS / 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 Appliable	

Part 2b. Description of Payment Card Business	
Describe how and in what capacity your business stores, processes, and/or transmits cardholder 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. Eventbrite receives, processes, and transmits cardholder data via the payment methods and channels described below: Card-not-present transactions: 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 firstname, lastname, 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 Deliver 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: ApplePay & GooglePay. Both of these mobile payment systems were

	integrated through our existing processing rails with Braintree. There is an SDK utilized within the Checkout application that allows us to present the payment method, so long as the SDK call deems the method is available (i.e. the Apple device supports ApplePay). 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 both manual card entry and magnetic stripe (Track 1/Track 2) data. 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 Zipcode 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 dataflow discussed above. Ticket transfers uses 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 masked 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 of the 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 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 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. Card-present transactions: iOS and Android Organizer Mobile Application: Eventbrite provides mobile applications that allows event organizers to sell 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 both manual card entry and magnetic stripe (Track 1/Track 2) data. The following describes the card swipe using MagStripe card readers payment processing flow: iOS Organizer Application (U.S. POS): The iOS Organizer Application is a mobile application written by Eventbrite for the iOS platform. A swiped credit card transaction is accepted using a MagStripe card reader connected to an Apple iOS mobile device. The MagStripe readers are manufactured by IDTech Products (iMagPro Mobile MagStripe model, a payment supported magnetic stripe device) and are sold to Eventbrite's organizers for use with the iOS Organizer application. The iMagPro Mobile MagStripe reader uses DUKPT (Derived Unique Key Per Transaction) key management with Triple DES (3DES) encryption to encrypt Track1/Track2 data from each card with a unique 3DES key. The 3DES encrypted magnetic stripe (Track1/ Track 2) data is passed to the Eventbrite iOS application. The encrypted data is then transferred to the Eventbrite API servers via HTTPS using TLS 1.2 with at least AES-128-bit encryption or higher supporting the most secure protocol and highest cipher that the event organizer's native mobile device web browser can negotiate. Once the Eventbrite API servers receive the encrypted data, the block of data must be further decrypted to get the full Track 1/Track 2 card data. In this case, the API server then sends the DUKPT encrypted data block to the Eventbrite credit card decryption service (SSM) servers. The server maintains the split knowledge, dual controlled keys which replay the encryption sequence to derive the symmetric key used to encrypt the data on the swipe reader. The algorithm for key management used is the ANSI X9.24 DUKPT standard. The Eventbrite SSM server computes the encryption key, decrypts the block of data, and returns the full Track 1/Track 2 data back to the API server for transaction processing. Once the API server receives the full Track 1/ Track 2 data from the SSM server, the transaction is handled in API server memory only and authorization of payment card transaction is handled by payment processors in the same methods as noted above in the Eventbrite website

	dataflow. 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. iOS Organizer Application with Adyen Mobile Transaction (International POS): The iOS Organizer App is a mobile application written by Eventbrite for the iOS platform transactions, which allows organizers to sell tickets to their events at the door of their venue using the attendee's credit card information. This product is currently only enabled for non-US venues. This product is tightly coupled with the Adyen POS reader (a payment supported magnetic stripe device), which does both magnetic stripe and chip-based capture of cardholder data. The iOS app will capture the cardholder data (PAN, CVV, expiration date) using the vendor-supplied API using redirect, which is integrated into the iOS application. This API will forward the captured information to Adyen Instant Payment Notification (IPN) via HTTPS with TLS 1.2 using 128-bit encryption for processing and returns status information. At this time, the organizer application will complete its payment processing by sending an Eventbrite API request to the front end CloudFront load balancers through to the API servers, which then store transaction details in the EBProd and ProdPayments MySQL 5.7 databases. Asynchronous to this process, the Adyen servers will return an API response directly to the Eventbrite API servers and that will update the payment details, such as truncated PAN (last four digits of the PAN or first six and last four digits of the PAN) and the reference token in the EB and ProdPayments MySQL databases. 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. Android Organizer App: The Android Organizer App is a mobile application written by Eventbrite for the Android platform, which allows organizers to sell tickets to their events at the door of their venue using the attendee's payment card information. The swiped transaction is accepted using a MagStripe card reader connected to an Android mobile device. The MagStripe readers are manufactured by IDTech Products (iMagPro Mobile MagStripe model, a

	payment supported magnetic stripe device) and are sold to Eventbrite's organizers for use with the Android Organizer application. The iMagPro Mobile MagStripe reader uses DUKPT (Derived Unique Key Per Transaction) key management with Triple DES (3DES) encryption to encrypt Track1/Track2 data from each card with a unique 3DES key. The 3DES encrypted magnetic stripe (Track1/ Track 2) data is passed to the Eventbrite iOS application. The Eventbrite iOS application treats the encrypted block of data as an opaque block of data and then additionally encrypts it within the application with RSA 2048-bit asymmetric encryption using an Eventbrite's RSA 2048-bit public key. The encrypted data is then transferred internally to the Eventbrite API servers using HTTPS using TLS 1.2 with at least minimum TLS_DHE_RSA_WITH_AES_128_CBC_SHA 128-bit encryption or higher supporting the most secure protocol and highest cipher that the event organizer's native mobile device web browser can negotiate. Once the Eventbrite API servers receive the encrypted data, it is decrypted with the 2048-bit RSA private key and the block of data must be further decrypted to get the full Track 1/Track 2 card data. In this case, the API server then sends the DUKPT encrypted data block to the Eventbrite SSM servers. The server maintains the set of derivation keys necessary to compute what the encryption key for a given card swipe on a given swipe device was at the time the card passed over the magnetic card reader head. The algorithm for key management used is the ANSI X9.24 DUKPT standard. The Eventbrite SSM server computes the encryption key, decrypts the block of data, and returns the full Track 1/Track 2 data back to the API server for transaction processing. Once the API server receives the full Track 1/ Track 2 data from the SSM server, the transaction is handled in the API server. Now, the API servers via the embedded order service will encrypt and store the card data in-memory by fetching the data-encrypting key from 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 the 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. Organizer App PayPal Here Card Present: The Organizer App is a mobile application, which allows organizers to sell tickets to their events at the door of their venue using the attendee's credit card information. This product is tightly coupled with the PayPal Here card reader (a payment supported magnetic stripe device), which does both magnetic stripe and chip-based capture of cardholder data. The PayPal Here readers communicate to the mobile application using the SDK provided by PayPal. The PayPal Here SDK notifies the Organizer app of the successful transaction swipe by the reader, containing card type and last 4 digits of the card. The Organizer App then notifies Eventbrite API via a HTTPS request to initiate the processing of the PayPal Here transaction. Front end CloudFront load balancers forward the request to payment service servers for processing. Payment service responds with an 'external reference' identifier used to identify the order at a later date. Organizer App injects this external reference identifier into the order and prompts the PayPal SDK to process the order. SDK then sends magstripe and reference identifiers to PayPal for payment processing. The SDK notifies the app of the successful transaction, forwarding the successful invoice id to order service to process the order. Payment service uses the invoice number to request the transaction status from PayPal to be returned to the Organizer App. 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. PayPal syncs with Braintree for settlement of funds and information of transactions. Payment gateways then settle the funds with the Eventbrite bank accounts. The accountability and ownership of the security of the PayPal here card readers are solely a customer responsibility. The customers purchase the PayPal Here card readers directly from PayPal. At no point

	of this flow does Eventbrite store cardholder data to file, disk, or database. Bancontact and Adyen Transactions: The attendee places an order using their Bancontact payment card on the desktop application. A data token requesting the cardholder 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 masked 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, masked 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.

Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	None, all functionality, and services that could impact the security of cardholder data are listed above.

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):
AWS Hosted Data Center	2	US-East-1, US-West-2
Corporate Headquarters	1	San Francisco, CA
Corporate Offices	5	Madrid, Spain; Cork, Ireland; London, England; Hyderabad, India; and Mendoza Argentina

Part 2d. Payment Applications

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)
Not Applicable	Not Applicable	Not Applicable	☐ 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.*	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
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 have a relationship with a Qualified Integrator & Reseller (QIR) for the purpose of the services being validated?	☐ 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 have a relationship with one or more 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.) for the purpose of the services being validated?	☒ Yes ☐ No

If Yes:

Name of service provider:	**Description of services provided:**
Amazon Web Services, Inc.	Cloud Hosting Provider
PayPal, Inc.'s Braintree Payment Processing System	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

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

Part 2g. Summary of Requirements Tested

For each PCI DSS Requirement, select one of the following:

- **Full** – The requirement and all sub-requirements of that requirement were assessed, and no sub-requirements were marked as "Not Tested" or "Not Applicable" in the ROC.
- **Partial** – One or more sub-requirements of that requirement were marked as "Not Tested" or "Not Applicable" in the ROC.
- **None** – All sub-requirements of that requirement were marked as "Not Tested" and/or "Not Applicable" in the ROC.

For all requirements identified as either "Partial" or "None," provide details in the "Justification for Approach" column, including:

- Details of specific sub-requirements that were marked as either "Not Tested" and/or "Not Applicable" in the ROC
- Reason why sub-requirement(s) were not tested or not applicable

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	**Details of Requirements Assessed**			
	Full	**Partial**	**None**	**Justification for Approach** (Required for all "Partial" and "None" responses. Identify which sub-requirements were not tested and the reason.)
Requirement 1:	☐	☒	☐	Requirement 1.3.6: Not Applicable – Cardholder data is not stored on system components.
Requirement 2:	☐	☒	☐	Requirement 2.1.1: Not Applicable – No wireless environments are connected to the cardholder data environment. Requirement 2.2.3: Not Applicable – There are no insecure services, daemons, or protocols enabled in the CDE. Requirement 2.6: Not Applicable – Eventbrite is not a shared hosting provider.
Requirement 3:	☐	☒	☐	Requirement 3.4: Not Applicable – Eventbrite does not store cardholder data to disk, database or on any CDE system components. Requirement 3.4.1: Not Applicable – Disk encryption is not used to protect cardholder data. Requirement 3.5, 3.5.1, 3.5.2, 3.5.3, 3.5.4: Not Applicable – Eventbrite does not store cardholder data to disk, database or on any CDE system components. Requirement 3.6, 3.6.1, 3.6.2, 3.6.3, 3.6.4, 3.6.5, 3.6.6, 3.6.7, 3.6.8: Not Applicable – Eventbrite does not store cardholder data to disk, database or on any CDE system components.

Requirement 4:	☐	☒	☐	Requirement 4.1.1: Not Applicable – Eventbrite does not directly transmit or receive cardholder data over wireless networks.
Requirement 5:	☐	☒	☐	Requirement 5.1.2: Not Applicable – All systems within Eventbrite's CDE are equipped with the use of malware protection.
Requirement 6:	☒	☐	☐	
Requirement 7:	☒	☐	☐	
Requirement 8:	☐	☒	☐	Requirement 8.1.5: Not Applicable – Eventbrite does not allow vendors to access the CDE remotely. Requirement 8.5.1: Not Applicable – Eventbrite does not provide services that require remote access to customer premises or systems. Requirement 8.7: Not Applicable – No cardholder data is stored to databases, disk or within the Eventbrite CDE.
Requirement 9:	☐	☒	☐	Requirements 9.5, 9.5.1, 9.6, 9.6.1, 9.6.2, 9.6.3, 9.7, 9.7.1, 9.8, 9.8.1, 9.8.2: Not Applicable – Eventbrite does not generate any media (digital or non-digital) containing cardholder data. Requirement 9.9, 9.9.1, 9.9.2, 9.9.3: Not Applicable – No card-present point of interaction (POI) devices are owned by Eventbrite directly.
Requirement 10:	☐	☒	☐	Requirement 10.2.1: Not Applicable – Eventbrite does not store cardholder data and does not provide individual user access to cardholder data.
Requirement 11:	☐	☒	☐	Requirement 11.2.3: Not Applicable – No significant changes during the assessment period.
Requirement 12:	☐	☒	☐	Requirement 12.3.9: Not Applicable – Eventbrite does not allow vendors to access the CDE.
Appendix A1:	☐	☐	☒	A1.1, A1.2, A1.3, A1.4: Not Applicable – Eventbrite is not a shared hosting provider.
Appendix A2:	☐	☐	☒	A2.1, A2.2, A2.3: Not Applicable – Eventbrite does not process any card-present transactions from any point-of-sale systems (POS) or point of interaction (POI) terminals.

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:	*03/15/2024*	
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 *03/15/2024.*

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 *Eventbrite, Inc.* 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: Not Applicable 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 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, CVN2, CVV2, or CID 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 *MegaplanIT Holdings LLC.*

Part 3b. Service Provider Attestation

Lanny Baker

Signature of Service Provider Executive Officer ↑	*Date:* 3/18/2024 | 12:08 PM PDT
Service Provider Executive Officer Name: **Lanny Baker**	*Title:* **Chief Financial Officer**

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

If a QSA was involved or assisted with this assessment, describe the role performed:	Conducted PCI DSS 3.2.1 remote onsite assessment and documented compliance results in a Report on Compliance and associated Attestation of Compliance (AOC).

Signature of Duly Authorized Officer of QSA Company ↑	*Date:* 3/18/2024 | 12:22 PM PDT
Duly Authorized Officer Name: **Christy Belknap**	*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 ISAs were involved with 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 the applicable 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	☒	☐	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	☒	☐	
3	Protect stored cardholder data	☒	☐	
4	Encrypt transmission of cardholder data across open, public networks	☒	☐	
5	Protect all systems against malware and regularly update anti-virus software or programs	☒	☐	
6	Develop and maintain secure systems and applications	☒	☐	
7	Restrict access to cardholder data by business need to know	☒	☐	
8	Identify and authenticate access to system components	☒	☐	
9	Restrict physical access to cardholder data	☒	☐	
10	Track and monitor all access to network resources and cardholder data	☒	☐	
11	Regularly test security systems and processes	☒	☐	
12	Maintain a policy that addresses information security for all personnel	☒	☐	
Appendix A1	Additional PCI DSS Requirements for Shared Hosting Providers	☒	☐	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	☒	☐