Payment Card Industry (PCI)
Data Security Standard

Attestation of Compliance for Onsite Assessments – Service Providers

Version 3.2.1

June 2018

Section 1: Assessment Information

Instructions for Submission

This Attestation of Compliance must be completed as a declaration of the results of the 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:	155 5th Street, 7th 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:	Riona Mascarenhas		Title:	QSA	
Telephone:	303-554-6333		E-mail:	coalfiresubmission@coalfire.com	
Business Address:	11000 Westmoor Circle, Suite 450		City:	Westminster	
State/Province:	CO	Country:	USA	Zip:	80021
URL:	https://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 Applicable	

Part 2b. Description of Payment Card Business	
Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	Eventbrite, Inc. (Eventbrite) platform enables event organizers to sell tickets and manage registrations. Eventbrite facilitates processing, transmission, and storage of payment card payment transactions on behalf of customers (event organizers) as a service provider. Direct funding is available to event organizers who already have their own merchant ID (MID) and have set up an account with the payment processor, Authorize.net. With this option, the event organizer is the merchant of record (MOR) for the payment transaction and Eventbrite processes the payment card transactions and then deposits the collected funds directly to the customer's Authorize.net merchant account. Eventbrite receives, processes, and transmits cardholder data via the following payment methods and channels as described below: **Card-not-present transaction:** Eventbrite Website: An event attendee begins a transaction to purchase tickets to an event created by an organizer on the Eventbrite website using their web browser. During this process, the web server accepts the attendee's name, address, primary account number (PAN), card expiration date, and card validation value (CVV2, CVC2, CID) via HTTPS using TLS (Transport Layer Security) 1.2 with at least

TLS_DHE_RSA_WITH_AES_128_CBC_SHA 128-bit encryption minimum, supporting the most secure protocol and strongest cipher that the attendee's web browser can negotiate. The Eventbrite web front end HAProxy load balancers then communicate to the Eventbrite's payments server. 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 outbound transmission to the selected payment processor. Post authorization, only truncated PAN (last four digits of the PAN or firstsix and last four digits of the PAN) and the reference token received from the payment processors is stored to the databases. Eventbrite does not store any cardholder data to file, disk or database.

Eventbrite iOS and Android Native Attendee Application: Eventbrite provides mobile applications for iOS or Android used by their attendees to find events and buy tickets to these events. The applications are built by Eventbrite and are available for download on the iTunes App Store and Google Play App Store. The attendees enter their name, address, PAN, card expiration date, and card verification values (CVV2, CVC2, CID) and the CHD is transmitted to Eventbrite servers. The payment processing from the payment's server is handled the same way as the Eventbrite website described above.

iOS and Android Organizer Mobile Application: Eventbrite provides mobile applications for iOS or Android 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. 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: 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 HAProxy load balancers /API servers via TLS 1.2 with minimum TLS_DHE_RSA_WITH_AES_128_CBC_SHA 128-bit encryption. The API servers via the embedded order service API passes encrypted data to payment service for processing. 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.

Pay Invoices/Pay Refund: Eventbrite can act either as the merchant of record or service provider and thus can collect a variety of fees for use of the service. There are cases when Eventbrite does not charge credit card processing fees but still have a per-ticket fee that is collected through a web user interface. The attendee receives an email indicating they owe fees with a link to

their account details. The attendee then enters the payment card details which are sent encrypted over HTTPS using TLS 1.2 with at least minimum of TLS_DHE_RSA_WITH_AES_128_CBC_SHA 128-bit minimum encryption to Eventbrite payment servers. Payment card data received is handled the similar way as detailed above for Eventbrite website. 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.

Ticket Transfers: Purchased tickets to one event may be transferred to another date with incurred fees. The website/mobile web user interface will prompt the purchaser for payment card information to either get refunded or to pay the difference. Payment card data received by this channel is handled the same way as the Eventbrite website and Eventbrite does not store cardholder data to file, disk or database.

Embedded Checkout: The Embedded Checkout is a widget inside an iFrame that connects to the Eventbrite website over HTTPS using TLS 1.2 with AES-256-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 HAProxy load balancers which forwards it to the payment service servers for payment processing. The appropriate payment gateways settle the funds with the bank accounts and return back the tokenized form of the PAN which is stored in the database. Eventbrite does not store cardholder data to file, disk or database.

PayPal Embedded Checkout: The embedded checkout flow directs the attendee to a PayPal page where they are able to communicate with Braintree for order processing. The response from payment service server after processing the order 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.

Partner Flow Using Card Data: This particular flow is for partner systems but using card data. The partner system transmits the data token containing attendee's name, PAN, card expiration date and card verification values (CVV2, CVC2, CID) over to the Partner API, which forwards the nonce to the HAProxy load balancers using HTTPS with TLS 1.2 and AES 128-bit encryption, which then passes the data token to the payment servers for processing the Braintree or Cybersource nonce. Once the order status is processed and marked complete, Braintree/Cybersource eventually will settle the funds with Eventbrite's merchant banks, Wells Fargo or National Australia Bank.

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 attendee can find events in their newsfeed or on an organizer's page. The user (event attendee) then initiates the purchase process on the Facebook platform. The attendee will be presented 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 attendee and transmit this information to the Braintree system for processing. Braintree processes the transaction and returns status information back to Facebook. Facebook then redirects the attendee to Eventbrite systems indicating the success/failure of the transaction. Facebook eventually settles the funds with Eventbrite's merchant bank, Wells Fargo and National Australia Bank.

Card-present transactions:

iOS and Android Pay Organizer Application: Eventbrite provides mobile applications on iOS/Android platforms that allows event organizers to sell tickets "at the door". The mobile applications are developed internally by Eventbrite for use by event organizers, and venue managers and are available at the Apple/Android stores. These applications support both manual card entry and magnetic stripe (Track/1Track2) data. The following describes the card swipe using MagStripe card readers payment processing flow:

- iOS Organizer Application (US 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 reader encrypts Track1/Track2 data with DUKPT (Derived Unique Key Per Transaction) key management and Triple DES (3DES) encryption. The 3DES encrypted magnetic stripe (Track1/ Track 2) data is passed to the Eventbrite iOS application using RSA asymmetric (public/private key) encryption with an Eventbrite 2048-bit RSA public key and securely transmitted inbound over the Internet to HAProxy load balancers/API servers via TLS 1.2 with minimum TLS_DHE_RSA_WITH_AES_128_CBC_SHA 128-bit encryption. The API servers via the embedded order service API passes encrypted data to payment service for processing. 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.
- iOS Organizer Application with Adyen (International POS): The iOS Organizer App is a mobile application which allows organizers to sell tickets to their events at the door at non-US venues using the attendee's credit card information. This product is used with the Adyen POS reader (a PCI certified magnetic stripe device), which does both magnetic stripe and chip-based capture of cardholder data. The

vendor supplied API forwards the captured payment cardholder data using redirect to Adyen Instant Payment Notification (IPN) for processing and returns back status information. The application completes it's payment processing by sending an Eventbrite API request to the HAProxy load balancers which then store transaction details in payment databases. 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 and reference tokens to the payments databases.

- 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 encrypted data is then transferred internally via the Internet 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. The API servers pass encrypted data to the payment service for processing via the embedded order service API. 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.

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 attendee is redirected to a page owned by the card issuer bank. User credentials are verified by Quick Response (QR) code/Scan/Credentials/PIN Number. After Adyen authorizes the transaction, the payment gateways eventually settle the funds with Eventbrite's merchant bank account, Wells Fargo.

Facilitated Payments:

Eventbrite also receives payment card transactions that are facilitated through PayPal, Affirm, and Authorize.net. 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. Affirm: In the Affirm flow, the attendee places an order in the US with currency as 'USD' and selects 'Affirm' as the payment method. The attendee is then redirected to an intermediate page of the JavaScript script provided by Affirm. This script receives information about the order and billing information and redirects the attendee to the Affirm website. On the Affirm site, the attendee completes fields with their information and selects the installment option. Upon completing this process with Affirm, the attendee's browser is redirected to the HAProxy load balancers which then forwards to the payment service server, which communicates with order service server marking the order complete. Affirm eventually settles funds with merchant bank, Wells Fargo. PayPal: Eventbrite allows organizers to configure their events to accept PayPal as a method of payment. In this case, Eventbrite redirects the '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 directly into the PayPal webpages from their web browser via the redirect used 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's databases. This process is fully outsourced to PayPal, which is a PCI DSS v3.2.1 validated payment processor with an AOC dated 12/3/2020. 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 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 from the Authorize.net is then recorded in the databases.
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):
Cloud Hosted Production Datacenter	2	(us-east-1) AWS US East (N. Virginia) (us-west-2) AWS US West Coast (Oregon)

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 and over a session based VPN enabled with two-factor authentication to a bastion host to support Eventbrite administrative remote access. Outbound connections are restricted to necessary ports and protocols to support forwarding transactions to payment processors for authorization. The following critical system components within the CDE were assessed: • AWS Virtual Private Cloud (VPC)

	• Virtual firewalls (security groups) • AWS virtual servers (EC2 Instances for terminal, processing, logging and administrative) • Load balancers Support Systems • 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) • Automated application code deployment • 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? If Yes: Name of QIR Company: Not Applicable QIR Individual Name: Not Applicable Description of services provided by QIR: Not Applicable	☐ Yes ☒ No
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	Cloud Hosting Provider
Braintree	Transaction Processing
CyberSource	Transaction Processing
Adyen	Transaction Processing

Authorize.net	Transaction Processing
PayPal	Payment System
Affirm	Transaction Processing
First Data	Transaction Processing
Mercado Pago	Transaction Processing
OmniPay	Transaction Processing
PayU	Transaction Processing
Signal Sciences	Web application firewall functionalities
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 1.2.3: Not Applicable – Eventbrite does not possess wireless networks in the CDE. Requirement 1.3.6: Not Applicable – Cardholder data (defined as including full PAN and/or sensitive authentication 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 Eventbrite's CDE. Requirement 2.6: Not Applicable – Eventbrite is not a shared hosting provider.
Requirement 3:	☐	☒	☐	Requirement 3.1: 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 3.6, 3.6.2: Not Applicable – Eventbrite does not share or distribute keys with customers. Requirement 3.6.6: Not Applicable – Eventbrite does not maintain manual clear-text cryptographic key management operations in the CDE.

Requirement 4:	☐	☒	☐	Requirement 4.1.1: Not Applicable – Eventbrite does not directly transmit or receive cardholder data over open, public networks
Requirement 5:	☐	☒	☐	Requirement 5.1.2: Not Applicable – All systems within Eventbrite's CDE are equipped with the use of antivirus software.
Requirement 6:	☐	☒	☐	Requirement 6.4.6: Not Applicable – Eventbrite did not have any significant changes in the past 12 months. Requirement 6.5.3: Not Applicable- Eventbrite does not store any card data that requires encryption other than the last four digits of the PAN or the first six and last four digits of the PAN.
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 otherwise within the Eventbrite CDE.
Requirement 9:	☐	☒	☐	Requirement (s) 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 – Backup media is not used within the Eventbrite CDE; and no media containing cardholder data, paper or electronic, is generated or stored by Eventbrite. 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 – Eventbrite did not have any significant changes in the past 12-months.
Requirement 12:	☒	☐	☐	
Appendix A1:	☐	☒	☐	A1.1, A1.2, A1.3, A1.4: Not Applicable – Eventbrite is not a shared hosting provider.
Appendix A2:	☐	☒	☐	A2.1: Not Applicable – Eventbrite does not process any card-present transactions from any point-of-sale systems (POS) or point of interaction (POI) terminals. A2.2, A2.3: Not Applicable – SSL or TLS1.0 is not used in Eventbrite's in-scope environment.

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:	03/11/2021	
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 *03/11/2021*

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, CID, or CVV2 data[2], or PIN data[3] storage after transaction authorization was found on ANY system reviewed during this assessment.
☒	ASV scans are being completed by the PCI SSC Approved Scanning Vendor *Coalfire Systems, Inc. (Certificate Number 5094-01-02)*

Part 3b. Service Provider Attestation

DocuSigned by:
Lanny Baker
E783753D6FA8439...

Signature of Service Provider Executive Officer	*Date:* 3/17/2021
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 onsite assessment and documented compliance results in a Report on Compliance and associated Attestation of Compliance (AOC).

DocuSigned by:
Riona Mascarenhas
F1651A6407BF4FF...

Signature of Duly Authorized Officer of QSA Company	*Date:* 3/17/2021
Duly Authorized Officer Name: Riona Mascarenhas	*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	☒	☐	