



# Payment Card Industry (PCI) Data Security Standard

---

## Attestation of Compliance for Onsite Assessments – Merchants

Version 3.2.1

June 2018



## Section 1: Assessment Information

### Instructions for Submission

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

#### Part 1. Merchant and Qualified Security Assessor Information

##### Part 1a. Merchant Organization Information

Company Name:	Eventbrite, Inc.	DBA (doing business as):	Not Applicable		
Contact Name:	Lanny Bakker	Title:	Chief Financial Officer		
Telephone:	415-694-7900	E-mail:	lanny@eventbrite.com		
Business Address:	155, 5 <sup>th</sup> Street, 7 <sup>th</sup> 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:	Humberto Zepeda	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. Type of Merchant Business (check all that apply)

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

What types of payment channels does your business serve?

- Mail order/telephone order (MOTO)  
 E-Commerce  
 Card-present (face-to-face)

Which payment channels are covered by this assessment?

- Mail order/telephone order (MOTO)  
 E-Commerce  
 Card-present (face-to-face)

**Note:** If your organization has a payment channel or process that is not covered by this assessment, consult your acquirer or payment brand about validation for the other channels.



## Part 2b. Description of Payment Card Business

How and in what capacity does your business store, process and/or transmit cardholder data?

Eventbrite, Inc.'s (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 as a service provider. Direct funding is available to event organizers who already have their own Merchant ID and have set up an account with payment processor, Authorize.net. With this option, the event organizer is the merchant of record for the payment transaction and Eventbrite accepts the payment card transactions and then passes the collected cardholder data to the payment processors, Braintree, CyberSource, Stripe and Adyen. Eventbrite receives, processes and transmits cardholder data via the following payment methods and channels as described below:

### **Card-not-present transaction:**

**Eventbrite Website:** An attendee begins a transaction to purchase tickets to an event created by an organizer on the Eventbrite website using their web browser. During this process, the web server accepts the attendee's name, address, primary account number (PAN), card expiration date, and card validation value (CVV2, CVC2, CID) via a secure protocol and encryption. The Eventbrite web front end then communicates to the Eventbrite's Payments server. In the Payments server, payment card data is encrypted and retained in the server in-process memory until it is needed for transmission outbound to the selected payment processor. Post authorization, cardholder data is released from the in-process memory and overwritten as new transactions are processed. Eventbrite does not store cardholder data to file, disk or database.

**Eventbrite iOS and Android Native Attendee Application:** Eventbrite provides mobile applications for use by their attendees to find events and buy tickets to these events. The applications are built by Eventbrite and are available for download on the iTunes App Store and Google Play App Store. The encrypted transaction data is transmitted to Eventbrite load balancer servers with secure protocol and encryption. Then the data is transmitted to Eventbrite servers. The payment processing from the payment's server is handled exactly the same way as the Eventbrite website described above.

**Eventbrite Mobile Web:** Eventbrite has a mobile attendee app for both the iOS (iPhone/iPad/iPod Touch) and Android platforms that lets attendees purchase tickets to events. Payment card data received by this channel is handled exactly the same way as the Eventbrite website and does not store cardholder data to file, disk or database.

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

**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 exactly the same way as the Eventbrite Website and also does not store cardholder data to file, disk or database.

Embedded Checkout: The Embedded Checkout is a Widget inside an iFrame that connects to Eventbrite website over HTTPS 1.2 with AES-256-bit encryption. Data including cardholder name, PAN, card expiration date is provided as part of the ticket purchase flow. The request is forwarded to the Load Balancer 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. It chooses and connects to the proper gateway to complete the transaction. The payment gateways which settle the funds with the bank accounts then return back tokenized form of the PAN which is stored in the Payments Database. Eventbrite does not store cardholder data to file, disk or database.

PayPal Embedded Checkout: The embedded checkout flow directs the user to a PayPal page where they are able to communicate with Braintree for order processing. The response from Payment service server is added to systems of record for financial reconciliation, fees processing and other internal back office needs. Braintree eventually settles funds with our Merchant Banks.

Bancontact and Adyen transactions: The attendee can place an order using their Bancontact debit card on the desktop application. A data token requesting cardholder name, PAN, card expiration date is routed to the payment service server which routes to Adyen IPN System to be authorized. After authentication, the load balancers then pass on the user's payment information to Eventbrite payment service servers after Adyen authorizes the transaction.

Bancontact: The attendee places an order using their Bancontact debit card on the desktop application. A data token requesting cardholder name, PAN, card expiration date is routed to the payment service server and is then routed to Adyen IPN System to be authorized.

Facebook API: Eventbrite and Facebook have launched a partnership that allows attendees to find events they wish to attend through their social network on Facebook, and then purchase tickets for these events directly on the Facebook platform. The user on the Facebook platform (Event attendee) initiates the purchase process. Attendee finds an update in their newsfeed or on an organizer's page. From this point, the customer can immediately click a "Buy Now" button. They will be presented a user interface that allows them to select the number of tickets they wish to purchase. Facebook will then collect the payment card data (name, PAN, CVV, expiration date) from the user and transmit this information to the Braintree systems for processing. Braintree will process the transaction and return status information back to Facebook. When the transaction is complete, Facebook will redirect the user to the Eventbrite system 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 order service server marking the order complete and logging last 4 digits of these 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 funds with merchant bank, Wells Fargo and National Australia Bank.

Pay Invoices/Pay Refund Recharge Flow: The Pay Refund Recharge allows the attendee to request a refund from an organizer after the accounts have been settled with Eventbrite. The event organizer is requested to provide their credit card to process a payment for the amount they need to recharge their account. Partner flow using card data: This particular flow is for partner systems but using card data. Partner system sends 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 Eventbrite Load Balancer. The Load balancer will forward the data token to the payment service server for payment processing. Payment is added to payment systems for financial reconciliation, fees processing and other internal back office financial processing needs.

**Card-present transactions:**

iOS and Android Pay Organizer Application: Eventbrite provides a mobile application that allows event organizers to sell tickets "At-the-door". This application facilitates the processing of payment card transactions on the Apple iOS/Android application platform, developed internally by Eventbrite, and deployed for use by event organizers, and venue managers via the Apple AppStore/Android Store. Manually entered card data is encrypted and securely transmitted to the Eventbrite API servers. The inbound payment card data is received by the Eventbrite servers; and it is securely transmitted outbound to the selected payment processors using HTTPS with TLS 1.2 for authorization.

iOS Organizer Application (US POS): Swiped transaction is accepted using a MagStripe card reader connected to an Apple iOS mobile device. Eventbrite API servers receive the secured data and is transmitted outbound to the selected payment processor for authorization.

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 information to Adyen IPN for processing and return back status information. The application will complete its payment processing by sending an Eventbrite API request to the Eventbrite 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.

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. 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. The Eventbrite API servers receive the encrypted data and retain it memory only while authorization of payment card transaction is handled in the same method as noted above in the Eventbrite Website section.



### **Facilitated Payments:**

Eventbrite also receives payment card transactions that are facilitated through PayPal, Facebook, iOS (Apple Pay) application, Android Pay application. Eventbrite does not receive the payment details; the payment data is transmitted directly from the end user to the facilitated payment provider. Only the status of the transaction after payment processing is stored in Eventbrite databases.

Affirm: In the Affirm flow, the user places an order in US with currency as 'USD' and selects 'Affirm' as payment method. The user 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 user to the Affirm website.

PayPal: Eventbrite allows organizers to configure their events to accept PayPal as a method of payment. In this case, Eventbrite redirects the customer's browser or mobile application to the PayPal site upon which PayPal IPN system is connected for internal processing. The attendee enters transaction details directly to the PayPal web pages from their web browser via the redirect using for authorization. After authorization, PayPal returns a transaction status code, last 4 digits of PAN and expiry date, which is, stored in the Eventbrite's databases. This process is fully outsourced to PayPal, which is a PCI DSS v3.2.1 validated payment processor with AOC dated 12/31/2019.

### **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 Application**

Does the organization use one or more Payment Applications?  Yes  No

Provide the following information regarding the Payment Applications your organization uses:

Payment Application Name	Version Number	Application Vendor	Is application PA-DSS Listed?	PA-DSS Listing Expiry date (if applicable)
Not Applicable	Not Applicable	Not Applicable	Not Applicable	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.,*

Eventbrite's CDE is entirely hosted in a dedicated AWS cloud hosting environment, which is both physically and logically separated from the company's corporate offices and development/testing environments. There are no direct physical or point-to-point VPN connections between the production CDE cloud environment and the Eventbrite corporate office network or the development/testing environments. The CDE is segmented with the cloud



<p><i>and any other necessary payment components, as applicable.</i></p>	<p>environment from non-CDE systems using specific network segments and Access Control Lists (ACLs).</p> <p>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.</p> <p>Outbound connections are restricted to necessary ports and protocols to support forwarding transactions to payment processors for authorization.</p> <p>Critical systems components within the CDE include:</p> <p>AWS Services</p> <ul style="list-style-type: none"> <li>• Virtual Private Cloud (VPC) enables Eventbrite to provision a logically isolated section of the Amazon Web Services (AWS) Cloud</li> </ul> <p>Servers – AWS VMs</p> <ul style="list-style-type: none"> <li>• API servers</li> <li>• Front End Load Balancers</li> <li>• Web Server</li> </ul> <p>Support Systems/Applications</p> <ul style="list-style-type: none"> <li>• Server configuration management and deployment system</li> <li>• Network Time synchronization</li> <li>• Host-based Intrusion Detection System (HIDS)</li> <li>• File Integrity Monitoring (FIM)</li> <li>• Centralized logging and log correlation manager</li> <li>• Automated application code build and deployment solution</li> <li>• Cloud-hosted Software as a Service issue and project tracking system which also supports change control management</li> <li>• External ASV Vulnerability Scanning</li> <li>• Internal Vulnerability Scanning</li> <li>• Bastion Host/VPN on AWS hosts: Authenticates access.</li> </ul> <p>Mac OS X and Ubuntu Linux laptops: Admin devices for remote connection to Bastion Host/VPN.</p>
--	---

<p>Does your business use network segmentation to affect the scope of your PCI DSS environment? <i>(Refer to “Network Segmentation” section of PCI DSS for guidance on network segmentation)</i></p>	<p><input checked="" type="checkbox"/> Yes <input type="checkbox"/> No</p>
--	--



## Part 2f. Third-Party Service Providers

Does your company use a Qualified Integrator & Reseller (QIR)?

Yes  No

If Yes:

Name of QIR Company: Not Applicable

QIR Individual Name: Not Applicable

Description of services provided by QIR: Not Applicable

Does your company share cardholder data with any third-party service providers (for example, Qualified Integrator & Resellers (QIR), gateways, payment processors, payment service providers (PSP), web-hosting companies, airline booking agents, loyalty program agents, etc.)?

Yes  No

**If Yes:**

**Name of service provider:**

**Description of services provided:**

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

Stripe

Transaction Processing

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





## Section 2: Report on Compliance

---

This Attestation of Compliance reflects the results of an onsite assessment, which is documented in an accompanying Report on Compliance (ROC).

The assessment documented in this attestation and in the ROC was completed on:	03/18/2020	
Have compensating controls been used to meet any requirement in the ROC?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Were any requirements in the ROC identified as being not applicable (N/A)?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
Were any requirements not tested?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Were any requirements in the ROC unable to be met due to a legal constraint?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No



## Section 3: Validation and Attestation Details

### Part 3. PCI DSS Validation

This AOC is based on results noted in the ROC dated **03/18/2020**.

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**):

<input checked="" type="checkbox"/>	<p><b>Compliant:</b> All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall <b>COMPLIANT</b> rating; thereby <i>Eventbrite, Inc.</i> has demonstrated full compliance with the PCI DSS.</p>				
<input type="checkbox"/>	<p><b>Non-Compliant:</b> Not all sections of the PCI DSS ROC are complete, or not all questions are answered affirmatively, resulting in an overall <b>NON-COMPLIANT</b> rating, thereby <i>Not Applicable</i> has not demonstrated full compliance with the PCI DSS.</p> <p><b>Target Date</b> for Compliance: Not Applicable</p> <p>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. <i>Check with your acquirer or the payment brand(s) before completing Part 4.</i></p>				
<input type="checkbox"/>	<p><b>Compliant but with Legal exception:</b> 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.</p> <p><i>If checked, complete the following:</i></p> <table border="1" style="width: 100%;"> <thead> <tr> <th style="text-align: center;">Affected Requirement</th> <th style="text-align: center;">Details of how legal constraint prevents requirement being met</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;">Not Applicable</td> <td style="text-align: center;">Not Applicable</td> </tr> </tbody> </table>	Affected Requirement	Details of how legal constraint prevents requirement being met	Not Applicable	Not Applicable
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**)

<input checked="" type="checkbox"/>	The ROC was completed according to the <i>PCI DSS Requirements and Security Assessment Procedures</i> , Version 3.2.1, and was completed according to the instructions therein.
<input checked="" type="checkbox"/>	All information within the above-referenced ROC and in this attestation fairly represents the results of my assessment in all material respects.
<input type="checkbox"/>	I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
<input checked="" type="checkbox"/>	I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
<input checked="" type="checkbox"/>	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)

- |                                     |  |
|-------------------------------------|--|
| <input checked="" type="checkbox"/> | No evidence of full track data <sup>1</sup> , CAV2, CVC2, CID, or CVV2 data <sup>2</sup> , or PIN data <sup>3</sup> storage after transaction authorization was found on ANY system reviewed during this assessment. |
| <input checked="" type="checkbox"/> | ASV scans are being completed by the PCI SSC Approved Scanning Vendor <i>Coalfire Systems, Inc.</i> (Certificate Number 50940-01-01)   |

### Part 3b. Merchant Attestation

DocuSigned by:

225630FF86AA4B9...

Signature of Merchant Executive Officer ↑

Date: 2020-03-18

Merchant Executive Officer Name: Lanny Bakker

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:

F143028320754DE...

Signature of Duly Authorized Officer of QSA Company ↑

Date: 3/19/2020

Duly Authorized Officer Name: Humberto Zepeda

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.

<sup>1</sup> 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.

<sup>2</sup> 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.

<sup>3</sup> Personal identification number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.



#### Part 4. Action Plan for Non-Compliant Requirements

Select the appropriate response for “Compliant to PCI DSS Requirements” for each requirement. If you answer “No” to any of the requirements, you may be required to provide the date your Company expects to be compliant with the requirement and a brief description of the actions being taken to meet the requirement.

*Check with your acquirer or the payment brand(s) before completing Part 4.*

PCI DSS Requirement	Description of Requirement	Compliant to PCI DSS Requirements (Select One)		Remediation Date and Actions (If “NO” selected for any Requirement)
		YES	NO	
1	Install and maintain a firewall configuration to protect cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3	Protect stored cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
4	Encrypt transmission of cardholder data across open, public networks	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
5	Protect all systems against malware and regularly update anti-virus software or programs	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6	Develop and maintain secure systems and applications	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
7	Restrict access to cardholder data by business need to know	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8	Identify and authenticate access to system components	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9	Restrict physical access to cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10	Track and monitor all access to network resources and cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
11	Regularly test security systems and processes	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12	Maintain a policy that addresses information security for all personnel	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

