eventbrite

REPORT ON EVENTBRITE, INC.'S SOFTWARE AS A SERVICE (SAAS) SOLUTION RELEVANT TO SECURITY, AVAILABILITY AND CONFIDENTIALITY THROUGHOUT THE PERIOD JUNE 1, 2019 TO JANUARY 31, 2020

SOC 3® - SOC for Service Organizations: Trust Services Criteria for General Use Report

COALFIRE CONTROLS

TABLE OF CONTENTS

SECTION 1

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Eventbrite, Inc. ("Eventbrite")

SCOPE

We have examined Eventbrite's accompanying assertion titled "Assertion of Eventbrite, Inc. Management" (assertion) that the controls within Eventbrite's Software as a Service (SaaS) Solution (system) were effective throughout the period June 1, 2019 to January 31, 2020, to provide reasonable assurance that Eventbrite's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability and confidentiality (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

SERVICE ORGANIZATION'S RESPONSIBILITIES

Eventbrite is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Eventbrite's service commitments and system requirements were achieved. Eventbrite has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Eventbrite is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

SERVICE AUDITOR'S RESPONSIBILITIES

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that controls were not effective to achieve Eventbrite's service commitments and system requirements based on the applicable trust services criteria.
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Eventbrite's service commitments and system requirements based on the applicable trust services criteria.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

INHERENT LIMITATIONS

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

OPINION

In our opinion, management's assertion that the controls within Eventbrite's Software as a Service (SaaS) Solution were effective throughout the period June 1, 2019 to January 31, 2020, to provide reasonable assurance that Eventbrite's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

RESTRICTED USE

Certain complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Eventbrite, to achieve Eventbrite's service commitments and system requirements based on the applicable trust services criteria. Users of this report should have sufficient knowledge and understanding of complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements. Eventbrite uses Amazon Web Services (AWS) as a cloud hosting infrastructure-as-a-service (IaaS) provider. Users of this report should obtain the relevant AWS SOC 2 or SOC 3 reports.

Coalfire Controls LLC

Westminster, Colorado
May 5, 2020

SECTION 2

ASSERTION OF EVENTBRITE, INC. MANAGEMENT

Assertion of Eventbrite, Inc. ("Eventbrite") Management

We are responsible for designing, implementing, operating and maintaining effective controls within Eventbrite's Software as a Service (SaaS) Solution (system) throughout the period June 1, 2019 to January 31, 2020, to provide reasonable assurance that Eventbrite's service commitments and system requirements relevant to security, availability and confidentiality were achieved. Our description of the boundaries of the system is presented in attachment A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period June 1, 2019 to January 31, 2020, to provide reasonable assurance that Eventbrite's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability and confidentiality (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). Eventbrite's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in attachment B.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period June 1, 2019 to January 31, 2020, to provide reasonable assurance that Eventbrite's service commitments and system requirements were achieved based on the applicable trust services criteria.

Eventbrite, Inc.

ATTACHMENT A

EVENTBRITE, INC.'S DESCRIPTION OF THE BOUNDARIES OF ITS SOFTWARE AS A SERVICE (SAAS) SOLUTION

TYPE OF SERVICES PROVIDED

Eventbrite ("Eventbrite" or "the Company") is a U.S.-based event management and ticketing website. Eventbrite was founded in 2006 to allow users to browse, create, and promote local events. The service charges a fee on the price of a ticket, which can be absorbed by the organizer or passed along to the purchaser, in exchange for online ticketing services, unless the event is free. Eventbrite is a marketplace for live experiences that allows event organizers (those hosting events) to create events and event attendees (those buying tickets and attending events) to find them. The platform allows event organizers to plan, promote, and sell tickets to events (event management) and publish these events through various marketing channels including Eventbrite Search/Directory, Organizer Websites, Search Indexes, and Social Media Outlets such as Facebook and Twitter.

The description of the boundaries of the system in this section of the report details the Eventbrite Software-as-a-Service (SaaS) Solution. Any other Eventbrite services are not included within the scope of this report. The accompanying description includes only policies, procedures, and control activities at Eventbrite and does not include policies, procedures, and control activities at any subservice organizations.

THE BOUNDARIES OF THE SYSTEM USED TO PROVIDE THE SERVICES

The boundaries of the system are the specific aspects of the Company's infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of the system.

The components that directly support the services provided to customers are as follows:

INFRASTRUCTURE

- Public Cloud Hosted Virtual Private Clouds; Isolated production account in Amazon Web Services (AWS)
- Virtualized Network Equipment
- Server Operating System (O/S)
- MySQL Databases and AWS native storage solutions
- Multi Region System Design

SOFTWARE

- Eventbrite SaaS application and Data Foundry application
- Application Monitoring Tools: Datadog and PagerDuty
- Web Application Firewall: Signal Sciences
- Intrusion Detection System/Intrusion Prevention System (IDS/IPS): Threat Stack
- Multi-Factor Authentication: Duo Security
- Backup/Replication Software: Percona tool for backup
- Security Information and Event Manager (SIEM)/Logging System: rsyslog, Splunk, AWS
- Infrastructure Monitoring: Datadog
- Single Sign On and Federation Services through Okta
- Patch Management: InsightVM

- File Integrity Monitoring: Threat Stack
- Anti-Virus (Server): ClamAV, Rkhunter, Chkrootkit
- Anti-Virus (Workstation): Carbon Black

PEOPLE

Eventbrite develops, manages, and secures the Eventbrite system via separate departments. The responsibilities of these departments are defined in the following table:

- Information Security Team: Eventbrite Security is responsible for all aspects of information security across the enterprise from Web and Mobile application security, to security awareness training, policy, and parts of compliance like Payment Card Industry Data Security Standard (PCI-DSS) and SOC 2. This team is charged with building the foundations that help protect the Company's information and customer data.
- Product and Engineering: The Product and Engineering team covers all aspects of the System Development Life Cycle (SDLC) including product specifications, requirements, design, implementation, testing, release engineering, and on-going maintenance.
- IT Team: The IT Team is responsible for all internal technology for users, user access to those technologies, and overall Corporate IT.
- Human Resources: The Human Resource Department is responsible for the following personnel security safeguards: hiring practices, training, change of role practices, and termination practices.
- Legal: Legal reviews contracts that customers submit and prepares any custom drafting required for sales contracts, including new drafts and later drafts of contracts or if an organizer requests legal documentation like a Certificate of Insurance. Legal assists if an organizer is in breach of contract or can help answer product-related and privacy-related questions.
- Site Reliability Engineering (SRE) Team: SRE designs and maintains the infrastructure that runs Eventbrite, makes sure new features and products can work at scale, and keeps the site running in the face of hardware or software failure.

PROCEDURES

- Policy management and communication - Policies are designed and maintained by the security team. The information security policies are hosted in an area available to all employees.
- Operations security - The Company has established procedures on the proper management of customer production environments, including change management, capacity management, malware detection and prevention, data backup, logging, security monitoring, vulnerability management, and system patching.
- Network operations- Communications security is governed by procedures that define controls related to network security, segregation, network services, transfer of information, and messaging.
- Change management - Changes to the architecture and the configuration of servers is managed by the Release Engineering and Site Reliability Engineering team and overseen by the Information Security team.
- Incident response - The Company has established incident management procedures including reporting events and weaknesses, defining responsibilities, response procedures, and collection of evidence. These procedures are documented and tested at least annually.
- Data Backup - Regular backups are routinely carried out to ensure that the Company can recover from unforeseen events, system failure, accidental or deliberate loss of information or facilities.

- System development - SDLC is in place. SDLC is a process followed for a software project that consists of a detailed plan describing how to develop, maintain, replace and enhance software. The life cycle defines a methodology for improving the quality of software and the overall development process.

DATA

Encrypted connections are made to Eventbrite using client virtual private network (VPN) connection and servers operate following transport layer security (TLS) standards and protocols.

Data collected by Eventbrite includes the personal data of users, organizers, and consumers. When a user registers for the services or otherwise submits Personal Data to Eventbrite, it may be associated to other Non-Personal Data (including Non-Personal Data collected from third parties) with other Personal Data. Data is segmented on multi-tenant MySQL databases and secured datastores.

ATTACHMENT B

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Commitments are declarations made by management to customers regarding the performance of the Eventbrite SaaS Solution. Commitments are communicated in a Terms of Service, Privacy Policy and Data Protection Agreement. The Company's commitments include the following:

SECURITY

- To implement and maintain an information security program that contains administrative, technical, and physical safeguards that are commercially reasonable in light of Eventbrite's size and complexity, the nature and scope of its activities, and the sensitivity of any information at issue.

AVAILABILITY

- To use commercially reasonable efforts to ensure that the site is available to customers within the context of the customer's contract with Eventbrite and/or terms of service, exclusive of commercially reasonable planned downtime for maintenance and downtime caused by matters outside of Eventbrite's reasonable control.

CONFIDENTIALITY

- To apply confidentiality standards to customer data consistent with data protection requirements.
- Eventbrite will make reasonable steps to protect customer data from loss, misuse, unauthorized use, access, inadvertent disclosure, alterations and destruction.

System requirements are specifications regarding how the Eventbrite SaaS Solution should function to meet the Company's commitment to user entities. Requirements are specified in the Company's policies and procedures, which are available to all employees. The Company's system requirements include the following:

- Employee provisioning and deprovisioning standards
- Logical access controls such as the use of user IDs and passwords to access systems
- Protection of data in transit
- Protection of data at rest
- Risk assessment and risk mitigation standards
- System monitoring
- Change management procedures
- Incident response plan and test
- Confidentiality agreements
- Background checks