BUGCROWD, INC.

INDEPENDENT SERVICE AUDITOR'S SOC 3 REPORT

FOR THE

CROWDCONTROL VULNERABILITY MANAGEMENT PLATFORM SYSTEM

FOR THE PERIOD OF DECEMBER 1, 2021, TO NOVEMBER 30, 2022

Attestation and Compliance Services

INDEPENDENT SERVICE AUDITOR'S REPORT

To Bugcrowd, Inc.:

Scope

We have examined Bugcrowd, Inc.'s ("Bugcrowd") accompanying assertion titled "Assertion of Bugcrowd, Inc. Service Organization Management" ("assertion") that the controls within Bugcrowd's Crowdcontrol Vulnerability Management Platform system ("system") were effective throughout the period December 1, 2021, to November 30, 2022, to provide reasonable assurance that Bugcrowd'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, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*.

Bugcrowd uses a subservice organization for cloud hosting services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Bugcrowd, to achieve Bugcrowd's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

Bugcrowd 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 Bugcrowd's service commitments and system requirements were achieved. Bugcrowd has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Bugcrowd is responsible for selecting, and identifying in its assertion, the applicable trust services 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 systems 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 Bugcrowd's service commitments and system requirements based on the applicable trust services criteria; and
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Bugcrowd'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 Bugcrowd'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 Bugcrowd's Crowdcontrol Vulnerability Management Platform system were effective throughout the period December 1, 2021, through November 30, 2022, to provide reasonable assurance that Bugcrowd's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Schellman & Company, LLC

Tampa, Florida
December 30,2022

ASSERTION OF BUGCROWD SERVICE ORGANIZATION MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within Bugcrowd, Inc.'s ("Bugcrowd") Crowdcontrol Vulnerability Management Platform system ("system") throughout the period December 1, 2021, to November 30, 2022, to provide reasonable assurance that [Service Organization's Abbreviated Name]'s service commitments and system requirements relevant to security, availability, and confidentiality were achieved. Our description of the boundaries of the system is presented below 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 December 1, 2021, to November 30, 2022, to provide reasonable assurance that Bugcrowd'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, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*. Bugcrowd's objectives for the system in applying the applying the applicable trust services criteria are embodied in its service commitments and systems requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented below.

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 December 1, 2021, to November 30, 2022, to provide reasonable assurance that Bugcrowd's service commitments and systems requirements were achieved based on the applicable trust services criteria.

DESCRIPTION OF THE BOUNDARIES OF THE CROWDCONTROL VULNERABILITY MANAGEMENT PLATFORM SYSTEM

Company Background

Based in San Francisco, Bugcrowd provides a range of public, private, and on-demand options that allow companies to commission a customized security testing program to fit their specific needs. Bugcrowd is backed by Blackbird Ventures, Costanoa Ventures, Industry Ventures, Paladin Capital Group, Rally Ventures, Salesforce Ventures, and Triangle Peak Partners.

Having architected security into the design, support, and management of programs for over four years, Bugcrowd has delivered hundreds of programs, helping crowdsourced security grow into a security practice for organizations of any size and any stage of security maturity. This is why many organizations including Mastercard, Tesla, Fitbit, Jet.com, NETGEAR, Western Union, and Open Web Application Security Project (OWASP), rely on Bugcrowd to manage their bug bounty programs.

Description of Services Provided

Bugcrowd delivers products that allow companies to perform security assessments for the enterprise and crowdsourced security testing. Bugcrowd pairs the power of more than 75,000 security researchers with a platform that identifies vulnerabilities before adversaries can take advantage of them.

Bugcrowd assists organizations in designing a security assessment program to fit their specific needs and testing requirements. Security researchers are then assigned to uncover vulnerabilities, which are submitted, prioritized, and reported back to customers, and a pay-for-performance model is used to incentivize results. Due to a diverse and capable crowd of experts from around the world, this process has proven to be an efficient alternative to traditional penetration testing and security assessments.

Bugcrowd allows customers to choose a custom-tailored approach to vulnerability testing to ensure program's success. The following options are available:

- Private or public: Keep the bug bounty program invite-only or open it up to the collective intelligence of thousands of hackers.
- Continuous or on-demand: Choose from on-going vulnerability testing and assessment, or take a project-based, on-demand approach.
- Compliance requirements: Add methodology-based assessment to the program to meet compliance requirements, including a penetration test report and re-testing.
- Uncover hidden or forgotten assets using crowdsourced assets surface management services.

System Boundaries

A system is designed, implemented, and operated to achieve specific business objectives in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which includes the services outlined above and the five components described below: infrastructure, software, people, procedures, and data.

Principal Service Commitments and System Requirements

Commitments

Bugcrowd has implemented reasonable measures to safeguard customers' data and confidential information. Bugcrowd has put into place a set of policies and procedures to help ensure that security commitments are met.

Information security policies and procedures are documented to define key roles and responsibilities, risk management governing principles, and design principles to protect systems and data.

In addition to security procedures, standard operating procedures are documented by each department involved in the operation of Bugcrowd's system. Management has identified actions, in the form of control activities, which are established and monitored on a periodic basis.

Bugcrowd's availability commitments and technical support program are documented in the standard terms and conditions. Bugcrowd makes the hosted services available to customers in accordance with industry standards and uses commercially reasonable efforts to make the services available 24 hours a day, 7 days a week, excluding scheduled maintenance and downtime caused by circumstances beyond Bugcrowd's control. Bugcrowd provides reasonable advance notice of schedule maintenance and downtime via the platform.

Bugcrowd has agreed to the following:

- Maintain security procedures that are consistent with applicable industry standards.
- Establish incident management and escalation procedures with customers.
- Conduct security training for employees who support in-scope services.
- Use commercially reasonable efforts to make the services available 24/7.
- Safeguard customers' data in accordance with confidential data handling policies and procedures.
- Delete customer data upon customers' written request.

System Requirements

Bugcrowd has put into place a set of policies and procedures to help ensure that the confidentiality commitments are met. Confidentiality agreements with third parties are documented and enforced prior to sharing any confidential data. In addition to the confidential agreements, Bugcrowd also has procedures in place to review documentation from third-party providers to ensure that they are in compliance with security and confidentiality policies. Bugcrowd's commitments and requirements are documented in customer contracts and are updated and communicated upon any changes in the confidentiality practices.

In accordance with our assertion, and the description criteria, the aforementioned service commitments and requirements are those principal service commitments and requirements common to the broad base of users of the system and may therefore not fully address the specific service commitments and requirements made to all system users, in each individual case.

Infrastructure and Software

The infrastructure and software supporting the Crowdcontrol Vulnerability Management Platform is maintained at a third-party data center facility and the infrastructure is located in the US East region. Data is replicated in real-time across multiple availability zones within the aforementioned region. The Crowdcontrol Vulnerability Management Platform utilizes server instances running Linux and databases running PostgreSQL.

The production network is administered remotely and access to the production servers requires an established connection authenticated via the use of public key infrastructure (PKI) and encrypted via transport layer security (TLS). Terminal sessions are also authenticated via the use of PKI and encrypted with secure shell (SSH).

Access to the public facing application is encrypted via TLS. TLS is provisioned as part of the default installation to help ensure a secure transmission over the Internet for the platform. In addition, a virtual firewall is utilized to restrict access to the application.

People

The personnel supporting the system include executive and senior leadership, which play important roles in establishing the Company's tone and core values. The organization assigns roles and responsibilities to provide

for appropriate staffing, security, operations, and segregations of duties. Management has also established authority and appropriate lines of reporting for key personnel.

Bugcrowd follows a standard onboarding process to help ensure personnel are familiar with Bugcrowd's processes, systems, security practices, policies, and procedures. At least annually, personnel must complete security awareness training.

Procedures

Bugcrowd has operational procedures in place to help ensure that customer security, availability, processing integrity, and confidentiality commitments can be met. Bugcrowd's operational procedures include but is not limited to the following areas of security: logical, change management, replications, backups, disaster recovery, incident response, system monitoring, vulnerability assessments, penetration testing, and processing integrity.

Data

The following table describes the information used and supported by the system:

Data Used and Supported by the System		
Data Description	**Data Reporting**	**Classification**
Customer data, including customers' vulnerability data information, platform account credentials, and personal identifiable information (PII) that are hosted in Bugcrowd's systems	Data is available to respective Bugcrowd customers and restricted to authorized internal personnel	Confidential
Researcher data, including researcher PII, reward payment information, and platform account credentials	Restricted to authorized internal personnel	
Bugcrowd's intellectual property		

Subservice Organizations

The cloud hosting services provided by Amazon Web Services (AWS) were not included within the scope of this examination. The following table presents the applicable Trust Services criteria that are intended to be met by controls at AWS, alone or in combination with controls at Bugcrowd, and the types of controls expected to be implemented at AWS to meet those criteria.

Control Activity Expected to be Implemented by Bugcrowd	Applicable Trust Services Criteria
AWS is responsible for implementing controls to manage logical access to the underlying network, virtualization management software, and storage devices for its cloud hosting services where the Bugcrowd systems reside.	CC6.1 – CC6.3, CC6.6
AWS is responsible for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers.	CC6.4 – CC6.5
AWS is responsible for implementing controls for the transmission, movement, and removal of the underlying storage devices for its cloud hosting services where the Bugcrowd systems reside.	CC6.7

Control Activity Expected to be Implemented by Bugcrowd	Applicable Trust Services Criteria
AWS is responsible for monitoring the logical access control systems for the underlying network, virtualization management software, and storage devices for its cloud hosting services where the Bugcrowd systems reside.	CC7.2
AWS is responsible for monitoring the capacity demand and ensuring capacity resources are available and functioning to meet Bugcrowd's availability commitments and requirements.	A1.1
AWS is responsible for ensuring the data center facilities are equipped with environmental security safeguards and utilizing an environmental monitoring application to monitor for environmental events.	A1.2

Complementary Controls at User Entities

Complementary user entity controls are not required, or significant, to achieve the service commitments and system requirements based on the applicable trust services criteria.

Trust Services Criteria Not Applicable to the In-Scope System

All criteria within the security, availability, and confidentiality, and privacy categories are applicable to the Crowdcontrol Vulnerability Management Platform system.