SLACK TECHNOLOGIES, INC.

INDEPENDENT SERVICE AUDITOR'S SOC 3 REPORT
FOR THE TEAM COLLABORATION PLATFORM

FOR THE PERIOD OF OCTOBER 1, 2019, TO SEPTEMBER 30, 2020

Attestation and Compliance Services

INDEPENDENT SERVICE AUDITOR'S REPORT

To Slack Technologies, Inc.:

Scope

We have examined Slack Technologies, Inc's ("Slack Technologies") accompanying assertion titled "Assertion of Slack Technologies, Inc. Service Organization Management" ("assertion") that the controls within Slack Technologies' Team Collaboration Platform system ("system") were effective throughout the period October 1, 2019, to September 30, 2020, to provide reasonable assurance that Slack Technologies' 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)*.

Slack Technologies 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 Slack Technologies, to achieve Slack Technologies' 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.

The description of the boundaries of the system indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Slack Technologies, to achieve Slack Technologies' service commitments and system requirements based on the applicable trust services criteria. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

Slack Technologies 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 Slack Technologies' service commitments and system requirements were achieved. Slack Technologies has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Slack Technologies 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 Slack Technologies' 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 Slack Technologies' 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 Slack Technologies' 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 Slack Technologies' Team Collaboration Platform system were effective throughout the period October 1, 2019, to September 30, 2020, to provide reasonable assurance that Slack Technologies' 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
October 26, 2020

ASSERTION OF SLACK TECHNOLOGIES SERVICE ORGANIZATION MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within Slack Technologies, Inc.'s ("Slack Technologies") Team Collaboration Platform system ("system") throughout the period October 1, 2019, to September 30, 2020, to provide reasonable assurance that Slack Technologies' 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 October 1, 2019, to September 30, 2020, to provide reasonable assurance that Slack Technologies' 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)*. Slack Technologies' 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 October 1, 2019, to September 30, 2020, to provide reasonable assurance that Slack Technologies' service commitments and systems requirements were achieved based on the applicable trust services criteria.

DESCRIPTION OF THE BOUNDARIES OF THE TEAM COLLABORATION PLATFORM SYSTEM

Company Background

Since 2014, Slack Technologies Inc. ("Slack Technologies" or the "Company") has provided a collaboration hub called "Slack" (the "System") to businesses and organizations ("user entities"), designed to allow the right people are always in the loop and key information is always at their fingertips.

With Slack, users join a secure instance called a "Workspace" ("Slack Workspace") where members can message each other in real time individually or in groups across multiple device types. Discussions can be organized into different topics (called "channels") or different groups of Workspace members, as desired. Slack Workspaces can connect to one another, and all members within an organization share a directory. As a collaboration hub, Slack allows other services to connect into the different discussions, providing updates and notifications directly into Slack. Slack provides a valuable repository of information by capturing all of this communication and content in one archive that is searchable.

Slack integrates with a large number of third-party services and supports community-built integrations. Slack provides mobile apps for iOS, Android, and Windows Phone (beta), in addition to their web browser client and electron desktop clients for macOS, Windows, and Linux (beta). Slack has been used for organizational communication, as well as a community platform.

Additional detail is posted on the Company's website and made available to internal and external users.

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

Slack makes the following security, availability, and confidentiality commitments to their customers:

- Slack will make the services available 99.99% of the time, except for maintenance or as otherwise provided in service level agreement (SLA) described in the service contract;
- Production cloud infrastructure hosted within multiple geographically diverse availability zones/regions;
- Encrypt data in transmission using transport layer security (TLS) or other technologies over public networks;
- Maintain commercially reasonable administrative, technical, organizational, and physical measures to protect the security of customer data against anticipated threats or hazards;
- Confidential data stored within the production services utilize advanced encryption standard (AES) encryption;
- Confidential data stored within the production services is retained per customer defined retention policies; and
- Disaster recovery plans are in place and tested at least once per year.

Slack has put into place a set of policies and procedures, inclusive of technology-based controls and automation, to help ensure that security, availability, and confidentiality commitments are met. Slack's commitments to security, availability, and confidentiality are described in the standard service agreement contracts for contracted customers. Customers are required to sign the Terms of Service agreement prior to receiving Slack's services. These agreements describe the technical and organizational controls that Slack is responsible for maintaining for their customers.

Infrastructure

The System production environment is hosted by infrastructure subprocessors. The Company maintains the list of current subprocessors here: https://slack.com/slack-subprocessors, which included Amazon Web Services ("AWS"), among others during the period covered by this report. Development occurs on systems in environments that are separate from the production environment.

Customer data is processed by and stored in hosted infrastructure compute services (such as AWS Elastic Compute Cloud (EC2) instances and hosted infrastructure storage services (such as AWS Simple Storage Service (S3)). AWS S3 is also utilized to store backup copies of customer data.

Software

The System is implemented using Linux, Apache, Hypertext Processor (PHP), and MySQL technologies with well-understood performance, scalability, and security properties. The System's real-time service is implemented in Java using the WebSocket protocol.

People

The Company's control environment is implemented, maintained, and supported by Service Engineering, Security, Customer Experience, People Operations ("People Ops"), Information Technology ("IT"), Quality Assurance ("QA"), Legal, Product Development, and Executive Management. All of the Company's personnel are recruited and managed according to policies and procedures which are described in the Summary of Control Activities section below.

Procedures

Physical Security

Subprocessors hosting Slack's production infrastructure ('hosting providers') manage the physical security of the facilities that host the development and production environments. Each hosting provider's System and Organization Control (SOC) 2 report details the security measures in place; the Company's management reviews these reports annually. Further, physical security is enforced at the Company's corporate office. Personnel are required to show proof of identity to enter the office building and entrances to the office are locked and required authorized badge for entry after close of business.

Device and Network Security

Devices issued to Company personnel must meet minimum security criteria that include being locked when unattended, employing full-disk encryption, and being kept up-to-date with security patches from the operating system vendor. Company laptops and workstations running Windows, Mac OS, or Linux are required to run antivirus software with up-to-date virus definitions.

Development and production servers are configured to a baseline via configuration management tools, such as Chef, and to automatically apply security patches made available by the operating system vendor daily. Office networks grant no elevated access to the development or production environments. The development and production environments use firewalls and multi-factor authentication to isolate themselves from the Internet.

Additional security measures are undertaken in accordance with the risk management program described above. Vulnerability management, automated scanning, penetration tests, a 'bug bounty' program, restrictive firewalls, and strong encryption of data transmitted over the public Internet are among the security measures employed by the Company.

Access to Internal Systems

Access to internal systems, including web-based tools and the development and production environments, is granted based upon job responsibilities, and revoked upon termination. Access to the System production environment and source code is reviewed quarterly by management.

Company personnel must pass background checks before starting work and attend security training during the onboarding period and annually thereafter.

Two-factor authentication is required to access the production environment, source code, hosting provider interfaces, the Company's internal administrative website, and the System itself.

Access to User Data

Access to sensitive customer data is restricted to Service Engineering personnel with credentials to access such data. All access by non-Service Engineering personnel requires management authorization or explicit customer approval. Company personnel are not authorized to store customer data on laptops, phones, USB drives, or any other device or portable media outside of the Company's data center. Instead, non-sensitive user data is accessed via web-based tools. Access to these tools is managed centrally and may be revoked at any time.

Change Management

Code changes are tested in the development environment, committed to a source code management system that logs all changes in perpetuity, and reviewed through automated testing or by peers. Major releases are tested by QA before deployment.

Incident Response

An incident response plan defines roles, responsibilities, escalation paths, and communication requirements in case of incidents that affect the security, availability, or confidentiality of the System. Incidents impacting availability are communicated externally via https://status.slack.com. Incidents impacting security and confidentiality of customer data are communicated to the impacted customers as per the Terms of Services ("ToS"), pertinent contractual obligations, and Security policies published on the Company's website.

Disaster Recovery and Data Backup

The Company values reliability and simplicity in its infrastructure. The System is hosted in multiple availability zones. Availability zones are designed to fail independently, thus allowing the System to remain available when any single availability zone fails.

Additionally, at least every 90 days, the Company practices recovery from backup, as would occur in the case of a complete failure and a requirement to move the System to a different region altogether.

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	Data provided by customer's in their designated workspaces	Confidential and private to the customer

The System stores and processes all information provided by user entities without inspection; all such information is maintained as confidential and private to that user entity. This confidential and private information is available only to members of the user entity's Slack Workspace. Each user entity has designated administrators who authorize member access to information stored in their Slack Workspace.

As described in Summary of Control Activities, access to customer data by Company personnel is restricted to authorized personnel. All other access to customer data by Company personnel requires management authorization or explicit approval from the user entity.

Subservice Organizations (Subprocessors)

The cloud hosting services provided by AWS and the service management services provided by ZenDesk, were not included within the scope of this examination. See the Complementary Subservice Organization Controls section below for more details.

Complementary Subservice Organization Controls

The Company utilizes the following three (3) service organizations ("subservice organizations") to implement portions of the System: 1) AWS; 2) Zendesk, Inc. ("Zendesk"); 3) AWS Simple E-mail Service (SES).

AWS

The Company utilizes services from AWS, such as EC2 for infrastructure hosting and S3 for data storage. AWS is responsible for operating, managing, and controlling the components from the host operating system and virtualization layer and storage, down to the physical security and environmental controls over the facilities in which the services operate. AWS is examined annually in accordance with the *AICPA Guide, Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy (SOC 2®).* This description includes only the controls of the System and does not include any of the controls expected to be implemented at AWS.

It is expected that AWS has implemented the following types of controls to support achievement of the associated criteria:

AWS	
Applicable Trust Services Criteria	**CSOCs**
CC3.2, CC3.3	Procedures are established and implemented to identify, analyze, and remediate potential security, availability, and confidentiality threats and/or risks.
CC4.1, CC4.2	Procedures are established and implemented to evaluate the designs and operating effectiveness of controls as they relate to security, availability, and/or confidentiality commitments, as well as to identify and track to resolution the corrective actions for control deficiencies.
CC6.3	Logical and physical access to the datacenter facility is provisioned to authorized personnel and revoked upon termination or when access is no longer needed.
CC6.4, CC6.5	Physical access to the datacenter facility is restricted to authorized personnel.
CC7.3, CC7.4, CC7.5	Incident Response Procedures are established and implemented to identify, analyze, and remediate potential security, availability, and confidentiality events and/or incidents.
A1.2	Environmental protections, data backup processes, recovery infrastructure, and monitoring and alarming mechanisms have been implemented to adequately address availability requirements.
A1.3	Business continuity/disaster recovery procedures are tested periodically.

ZenDesk

The Company utilizes Zendesk for receiving, managing, and resolving requests for assistance from its users. Zendesk is responsible for collecting and storing customer-submitted requests and providing help desk functionality for the Company's Customer Experience Department. Zendesk is examined annually in accordance with the AICPA Guide, Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy (SOC 2®). This description includes only the controls of the System and does not include any of the controls expected to be implemented at Zendesk.

It is expected that Zendesk has implemented the following types of controls to support achievement of the associated criteria:

Zendesk	
Applicable Trust Services Criteria	**CSOCs**
CC3.2, CC3.3	Procedures are established and implemented to identify, analyze, and remediate potential security, availability, and confidentiality threats and/or risks
CC4.1, CC4.2	Procedures are established and implemented to evaluate the designs and operating effectiveness of controls as they relate to security, availability, and/or confidentiality commitments, as well as to identify and track to resolution the corrective actions for control deficiencies.
CC6.1	Logical security has been implemented to authenticate authorized users, restrict access, prevent, and detect unauthorized access.
CC6.1	The systems are configured to identify and authenticate internal and external users with appropriate valid credentials.
CC6.2	Procedures are implemented to provision and de-provision user access to systems and applications based on appropriate authorization.
CC6.3	Logical access to the software and physical access to the software hosting datacenter facility is provisioned to authorized personnel and revoked upon termination or when access is no longer needed.
CC6.6	Logical security measures have been implemented to protect and detect external threats.
CC6.7	Logical security measures have been implemented to secure the transmission, movement, and removal of information, as well as restricting users with the ability to do so.
CC6.8	Antivirus and/or malware software have been implemented to prevent or detect the introduction of unauthorized or malicious software.
CC7.2	Vulnerability scans and penetration testing are performed periodically to identify vulnerabilities threatening the systems.
CC7.3, 7.4, 7.5	Incident Response Procedures are established and implemented to identify, analyze, and remediate potential security, availability, and confidentiality events and/or incidents.
CC8.1	Software development lifecycle (SDLC) has been established and implemented to ensure system changes are authorized, tested, and approved prior to production deployment.
CC8.1	Policies and procedures for SDLC or infrastructure changes have been established and reviewed and are updated periodically.

Zendesk	
Applicable Trust Services Criteria	**CSOCs**
CC8.1	Procedures are implemented to identify deficiencies in the system and to ensure secured change management procedures are tracked and monitored.

AWS SES

The Company utilize AWS SES to send and receive e-mail-based communication with users. AWS SES is examined annually in accordance with the AICPA Guide, Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy (SOC 2®). This description includes only the controls of the System and does not include any of the controls expected to be implemented at AWS SES.

It is expected that AWS SES have implemented the following types of controls to support achievement of the associated criteria:

AWS SES	
Applicable Trust Services Criteria	**CSOCs**
CC3.2, CC3.3	Procedures are established and implemented to identify, analyze, and remediate potential security, availability, and confidentiality threats and/or risks.
CC4.1, CC4.2	Procedures are established and implemented to evaluate the designs and operating effectiveness of controls as they relate to security, availability, and/or confidentiality commitments, as well as to identify and track to resolution the corrective actions for control deficiencies.
CC6.1	Logical security has been implemented to authenticate authorized users, restrict access, prevent, and detect unauthorized access.
CC6.1	The systems are configured to identify and authenticate internal and external users with appropriate valid credentials.
CC6.2	Procedures are implemented to provision and de-provision user access to systems and applications based on appropriate authorization.
CC6.3	Logical access to the software and physical access to the software hosting datacenter facility is provisioned to authorized personnel and revoked upon termination or when access is no longer needed.
CC6.6	Logical security measures have been implemented to protect and detect external threats.
CC6.7	Logical security measures have been implemented to secure the transmission, movement, and removal of information, as well as restricting users with the ability to do so.
CC6.8	Antivirus and/or malware software have been implemented to prevent or detect the introduction of unauthorized or malicious software.
CC7.2	Vulnerability scans and penetration testing are performed periodically to identify vulnerabilities threatening the systems.
CC7.3, 7.4, 7.5	Incident Response Procedures are established and implemented to identify, analyze, and remediate potential security, availability, and confidentiality events and/or incidents.
CC8.1	SDLC has been established and implemented to ensure system changes are authorized, tested, and approved prior to production deployment.

AWS SES	
Applicable Trust Services Criteria	**CSOCs**
CC8.1	Policies and procedures for SDLC or infrastructure changes have been established and reviewed and are updated periodically.
CC8.1	Procedures are established and implemented to ensure changes to systems are authorized, designed, developed, configured, documented, tested, and approved prior to production deployment.
A1.1	Monitoring tools are implemented to monitor and manage the systems' capacity and availability.
CC8.1	Procedures are implemented to ensure confidential information is protected during systems change management processes.
CC6.1	Security measures are implemented to prevent unauthorized disclosure, usage, and/or access to confidential information.
CC9.2	Confidential information is only obtained in accordance with the defined commitments or agreements.

Complementary Controls at User Entities

Slack Technologies' services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the applicable trust criteria related to Slack Technologies' services to be solely achieved by Slack Technologies' control procedures. Accordingly, user entities, in conjunction with the Team Collaboration Platform system and related services, should establish their own internal controls or procedures to complement those of Slack Technologies.

The following complementary user entities controls should be implemented by user entities to provide additional assurance that the applicable trust criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls

#	Complementary User Entity Control	Related Applicable Trust Criteria
1.	User entities are responsible for informing Slack of any regulatory issues that may affect the services provided by the System.	Common Criteria 6.1; Availability Criteria 1.2
2.	User entities are responsible for understanding and complying with their contractual obligations to Slack.	Common Criteria 2.2, 2.3, 6.1; Availability Criteria 1.2
3.	User entities are responsible for keeping the technical, billing, and administrative contact information on file with Slack up-to-date.	Common Criteria 2.2, 2.3
4.	User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize the System.	Availability Criteria 1.2, 1.3
5.	User entities are responsible for configuring the System security settings appropriately for the user entity.	Common Criteria 6.1, 6.3, 6.6
6.	User entities are responsible for ensuring the confidentiality of any user accounts and passwords assigned to them for use with the System.	Common Criteria 6.1, 6.3, 6.6
7.	User entities are responsible for inviting new users to sign up for an account in the System, as well as removing terminated user accounts from the System.	Common Criteria 6.1, 6.3, 6.6

#	Complementary User Entity Control	Related Applicable Trust Criteria
8.	User entities are responsible for ensuring that entity profile information stored by the System is accurate and complete.	Common Criteria 6.1, 6.3, 6.6
9.	User entities are responsible for immediately notifying Slack of any actual or suspected information security breaches, including compromised user accounts.	Common Criteria 7.3, 7.4, 7.5
10.	User entities are responsible for ensuring the appropriateness of designated Slack Workspace owner(s) and administrator(s).	Common Criteria 6.1, 6.3, 6.6
11.	User entities are responsible for providing accurate and complete contact information to Slack for end users to be provisioned.	Common Criteria 6.1, 6.3, 6.6
12.	User entities are responsible for accepting the terms and agreement for utilizing Slack's services.	Common Criteria 2.2, 2.3
13.	User entities are responsible for monitoring and enforcing organizational compliance to Slack's terms and agreements.	Common Criteria 2.2, 2.3
14.	User entities are responsible for configuring the message retention settings appropriately for the organization.	Common Criteria 6.1; Confidentiality Criteria 1.1, 1.2
15.	User entities are responsible for developing and implementing their own information classification policies to govern sharing Personally Identifiable Information (PII) and other sensitive data in the System.	Common Criteria 6.1, 8.1

Trust Services Criteria Not Applicable to the In-Scope System

All criteria within the security, availability, and confidentiality categories are applicable to the Team Collaboration Platform system.