Slack Technologies, Inc.

System and Organization Controls ("SOC") for Service Organizations: Trust Service Principles Report Relevant to Security, Availability, and Confidentiality Related to the Team Communication Platform Referred to as Slack

For the period February 1, 2017 to September 30, 2017

Standards for Attestation Engagements,
SOC 3® Report

BPM
Accountants & Consultants

Table of Contents

60 South Market Street, Suite 800, San Jose, CA 95113
Phone (408) 961-6300 **Fax** (408) 961-6324 **Email** bpm@bpmcpa.com **Web** bpmcpa.com

Report of Independent Accountants

To the Management
Slack Technologies, Inc.

We have examined management's assertion that Slack Technologies, Inc. ("Slack Technologies" or the "Company") maintained effective controls over the security, availability, and confidentiality of its team communication platform referred to as Slack (the "System") to provide reasonable assurance that, for the period February 1, 2017 to September 30, 2017, the System was:

- Protected against unauthorized access, use, or modification;
- Available for operation and use, as committed and agreed; and
- Protected as committed and agreed with regard to the information within the System designated as confidential,

based on the criteria for security, availability, and confidentiality in the American Institute of Certified Public Accountants' TSP Section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (2016) (applicable trust services criteria). This assertion is the responsibility of Slack Technologies' management. Our responsibility is to express an opinion based on our examination. Management's Description of the System (the "Description") covered by its assertion is attached. We did not examine the Description and, accordingly, we do not express an opinion on it.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included (1) obtaining an understanding of Slack Technologies' relevant security, availability, and confidentiality controls; (2) testing and evaluating the operating effectiveness of the controls; and (3) performing such other procedures as we considered necessary in the circumstances. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risks of material misstatement of management's assertion, whether due to fraud or error. We believe that our examination provides a reasonable basis for our opinion.

Our examination was not conducted for the purpose of evaluating Slack Technologies' cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

Because of their nature and inherent limitations, controls at a service organization may not always operate effectively to meet the applicable trust services criteria. Also, the projection to the future of any evaluation of the fairness of the presentation of the Description or conclusions about the suitability of the design or operating effectiveness of the controls to meet the applicable trust services criteria is subject to the risks that the System may change or that controls at a service organization may become inadequate or fail.

In our opinion, Slack Technologies' management's assertion referred to above is fairly stated, in all material respects, based on the aforementioned criteria for security, availability, and confidentiality.

BPM LLP

San Jose, California
December 6, 2017

Assertion of the Management of Slack Technologies, Inc.

Slack Technologies, Inc. ("Slack Technologies" or the "Company") provides businesses and organizations with a team communication platform called "Slack." The Company utilizes the following four (4) service organizations ("subservice organizations") to perform aspects of the System: 1) Amazon Web Services ("AWS"); 2) Google Cloud Platform ("GCP"); 3) Zendesk, Inc. ("Zendesk"); and 4) Mailgun Technologies, Inc. ("Mailgun").

Slack Technologies maintained effective controls over the security, availability, and confidentiality of its team communication platform referred to as Slack (the "System") to provide reasonable assurance that, for the period of February 1, 2017 to September 30, 2017, the System was:

- Protected against unauthorized access, use or modification;
- Available for operation and use, as committed and agreed; and
- Protected as committed and agreed with regard to the information within the System designated as confidential,

based on the criteria for security, availability, and confidentiality in the American Institute of Certified Public Accountants' TSP Section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (2016) (applicable trust services criteria), if the aforementioned subservice organizations maintained effective controls and if user entities applied the complementary user entity control throughout the period February 1, 2017 to September 30, 2017.

Our attached Description of the System summarizes those aspects of the team communication platform referred to as Slack covered by our assertion, the complementary controls expected to be implemented at the subservice organizations, and the complementary user entity controls expected to be applied by our customers.

The Management of Slack Technologies, Inc.

Slack Technologies' Description of the System

Company Background and Services

Since 2014, Slack Technologies, Inc. ("Slack Technologies" or the "Company") has provided a team communication platform called "Slack" to businesses and organizations ("user entities") around the world. With Slack, users join a secure instance called a "Team." or a Workspace" ("Workspace"). Workspace 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. Workspaces can connect to one another and all members within an organization share a directory. As a platform, 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.

Description of Slack Service

A description of the System is posted on the Company's website and made available to internal and external users. This description includes System boundaries and describes relevant System components (infrastructure, software, people, processes, and data) and how they ensure the Company's ability to meet its security, availability, and confidentiality commitments.

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 currently includes Amazon Web Services ("AWS") and Google Cloud Platform ("GCP"), among others. 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 Amazon EC2 or Google Compute Engine) and hosted infrastructure storage services (such as Amazon S3 or Google Cloud Storage Standard). Amazon S3 is also utilized to store backup copies of customer data.

Data Centers and Redundancy

The System is architected with resiliency and redundancy in mind, helping minimize single points of failure and the impact of common equipment failures and environmental risks. User data is replicated to at least two (2) locations.

Authentication and Access

Strong authentication and access controls are implemented to restrict administrative access to Slack production systems, internal support tools, and customer data. All administrative access to Slack production systems requires a second factor of authentication. Machine-level access restriction relies on a key-based authentication and uses transport encryption to enhance data confidentiality in transit. All data traffic is encrypted to and between Slack production facilities. Unique user identifications ("IDs"), strong passwords, and One-Time-Passwords ("OTPs") are used to help ensure access to customer data is appropriate and authorized.

Data

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.

All access to customer data by Company personnel is restricted to Service Engineering personnel with authorization to access such data. All other access to customer data by Company personnel requires management authorization or explicit approval from the user entity. Company personnel are not authorized to store customer data on laptops, phones, USB drives, or any other devices or portable media outside of the Company's data center.

Procedures

Formal policies and procedures codify the principles and requirements ensuring the security, availability and confidentiality of the System. All personnel are required to adhere to the Company's policies and procedures, which are located on the Company's intranet and can be accessed by any Company personnel. The Company policies address Acceptable Use, Access Control, Asset Management, Authorized Devices, Business Continuity and Disaster Recovery, Change Control, Data Encryption, Systems Development Lifecycle, Incident Response, Information Classification, Information Labeling and Handling, Malicious Code Prevention, People Operations, Records Retention, Security Assessments, System Audit and Monitoring, Third-Party Relationships, and Vulnerability Management. Audits are performed to evaluate the effective operation of the information security program.

People

The Company's management philosophy and operating style is consistent with a sound control environment and encompasses a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks and management's attitudes toward information processing, accounting functions, and personnel (employees and contractors). The Company's management style fosters open communication among all personnel. The executive management and senior leadership are committed to reinforcing the core values for all personnel. Management has documented information security policies, which are communicated to all Company personnel. Roles and responsibilities relevant to Slack's control environment are documented.

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

The Company follows a structured on-boarding process to ensure all personnel participate in the effective operation of Slack Technologies' information security management system. Prior to starting work, the PeopleOps Department completes a background verification check for each employee. Slack Technologies manages an orientation process to familiarize new personnel with Company tools, processes, systems, security practices, policies and procedures. All personnel are provided with and must acknowledge Slack Technologies' Information Security Policy to educate them as to their responsibilities concerning information security.

Complementary Subservice Organization Controls

The Company utilizes four (4) service organizations ("subservice organizations") to implement portions of the System; specifically, the following:

- Services from **Amazon Web Services** ("AWS"), such as Elastic Compute Cloud ("EC2") for infrastructure hosting and Simple Storage Service ("S3") for data storage.
- Services from **Google Cloud Platform** ("GCP"), such as Google Compute Engine ("GCE") for infrastructure hosting and Google Cloud Storage Standards for data storage.
- **Zendesk** for receiving, managing and resolving requests for assistance from members.
- **Mailgun** to send and receive email-based communication with members.

It is expected that the subservice organizations have implemented the following types of controls:

- Procedures are established and implemented to identify, analyze, and remediate potential security, availability, and confidentiality threats and/or risks.
- 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.
- 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.
- Logical security has been implemented to authenticate authorized users, restrict access, prevent and detect unauthorized access.
- Physical access to the datacenter facility is restricted to authorized personnel.
- Procedures are implemented to provision and de-provision user access to systems and applications based on appropriate authorization.
- The systems are configured to identify and authenticate internal and external users with appropriate valid credentials.
- Logical security measures have been implemented to protect and detect external threats.
- 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.
- Antivirus and/or malware software have been implemented to prevent or detect the introduction of unauthorized or malicious software.
- Vulnerability scans and penetration testing are performed periodically to identify vulnerabilities threatening the systems.
- Incident Response Procedures are established and implemented to identify, analyze, and remediate potential security, availability, and confidentiality events and/or incidents.
- Software development lifecycle ("SDLC") has been established and implemented to ensure system changes are authorized, tested, and approved prior to production deployment.
- Environmental protections, data backup processes, recovery infrastructure, and monitoring and alarming mechanisms have been implemented to adequately address availability requirements.

Complementary User Entity Controls

The System is 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 criteria related to the System to be solely achieved by the Company's control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of the Company.

As the complementary user entity controls listed below represent only a part of the control considerations that might be pertinent for user entities, they should not be considered as a comprehensive list.

List of Complementary User Entity Controls

User entities are responsible for:

- Informing Slack Technologies of any regulatory issues that may affect the services provided by the System.
- Understanding and complying with their contractual obligations to Slack Technologies.
- Keeping the technical, billing, and administrative contact information on file with Slack Technologies up-to-date.
- Developing their own disaster recovery and business continuity plans that address the inability to access or utilize the System.
- Configuring the System security settings appropriately for the user organization.
- Ensuring the confidentiality of any user accounts and passwords assigned to them for use with the System.
- Inviting new users to sign up for an account in the System, as well as removing terminated user accounts from the System.
- Ensuring that entity profile information stored by the System is accurate and complete.
- Immediately notifying Slack Technologies of any actual or suspected information security breaches, including compromised user accounts.
- Ensuring the appropriateness of designated Workspace owner(s) and administrator(s).
- Providing accurate and complete contact information to Slack Technologies for end users to be provisioned.
- Accepting the terms and agreement for utilizing Slack Technologies' services.
- Monitoring and enforcing organizational compliance to Slack Technologies' terms and agreements.
- Configuring the message retention settings appropriately for the organization.
- Developing and implementing their own information classification policies to govern sharing Personally Identifiable Information ("PII") and other sensitive data in the System.