LogMeIn® Customer Engagement & Support

SOC 3® – Reporting on Controls at a Service Organization

A SOC 3® Independent Service Auditor's Report on LogMeIn's Description of its Customer Engagement and Support (CES) System and on the Suitability of the Design and Operating Effectiveness of its Controls Based on the Trust Services Criteria Relevant to **Security, Availability, and Confidentiality**

Throughout the Period September 1, 2019 to August 31, 2020

Report of Independent Service Auditors

To: Management of LogMeIn, Inc.

SCOPE

We have examined LogMeIn, Inc.'s (LogMeIn's) accompanying assertion titled, "Management's Assertion Regarding the Effectiveness of its Controls over the Customer Engagement and Support (CES) System based on the Trust Services Criteria for Security, Availability, and Confidentiality" (assertion) that the controls within LogMeIn's Customer Engagement and Support (CES) System (system) were effective throughout the period September 1, 2019 to August 31, 2020, to provide reasonable assurance that LogMeIn'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

LogMeIn 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 LogMeIn's service commitments and system requirements were achieved. LogMeIn has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, LogMeIn 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 LogMeIn'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 LogMeIn's service commitments and system requirements based the applicable trust services criteria

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

INHERENT LIMITATIONS

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual report users may consider important to meet their informational needs.

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 LogMeIn's Customer Engagement and Support (CES) System were effective throughout the period September 1, 2019 to August 31, 2020, to provide reasonable assurance that LogMeIn's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Irvine, CA
October 30, 2020

October 30, 2020

Michael Donahue
General Counsel
LogMeIn, Inc.
320 Summer Street
Boston, MA 02210

John D. Redding, CPA.CITP
c/o Tevora Business Solutions
17875 Von Karman Ave., Suite 100
Irvine, CA 92614

Management's Assertion Regarding the Effectiveness of its Controls over the Customer Engagement and Support (CES) System based on the Trust Services Criteria for Security, Availability, and Confidentiality

We, as management of LogMeIn, Inc. (LogMeIn) are responsible for designing, implementing, operating, and maintaining effective controls within LogMeIn's Customer Engagement and Support (CES) System (system) throughout the period September 1, 2019 to August 31, 2020, to provide reasonable assurance that LogMeIn'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 the attached description 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 September 1, 2019 to August 31, 2020, to provide reasonable assurance that LogMeIn'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*). LogMeIn'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 also presented in the attached description.

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 September 1, 2019 to August 31, 2020, to provide reasonable assurance that LogMeIn's service commitments and system requirements were achieved based on the applicable trust services criteria.

DocuSigned by:
6B6C997D75D44E2...

Michael Donahue
General Counsel

Description of the Customer Engagement and Support (CES) System

BACKGROUND

LogMeIn is a global Software-as-a-Service (SaaS) company headquartered in Boston, Massachusetts with additional locations in North America, South America, Europe, Asia, and Australia.

LogMeIn products are SaaS solutions that allow its users to work remotely, collaborate with other users, and support and manage remote computers and other Internet-enabled devices. LogMeIn's core SaaS products can generally be categorized into three groups of products, based upon customer needs and respective use cases: Unified Communications and Collaboration, Customer Engagement and Support, and Identity and Access Management. LogMeIn customers range from multinational enterprises to small and medium businesses (SMBs), as well as individual consumers. Subscriptions may include or be offered in free, fee-based, and/or premium software services.

SERVICES PROVIDED

The Customer Engagement and Support (CES) System is designed to empower external customer service and support organizations, online retail and web-based businesses, as well as IT outsourcers and internal IT departments to deliver customer engagement and support. The in-scope products that make up the CES System are Bold360, GoToAssist, and Rescue (collectively referred to as CES Services).

bold360 by LogMeIn	**Bold360** is LogMeIn's suite of omni-channel engagement platform solutions designed to empower companies to deliver personalized customer engagement and support to their customers and employees through the use of artificial intelligence-powered chatbots and human agents. LogMeIn's Bold360 service offerings range in features and functionality based on industry and applicable use case. Bold360 Service (fka Bold360 ai) is an automated digital engagement solution that allows companies to utilize artificial intelligence-powered customer-facing chatbots, virtual agents and a customized knowledge-base to provide a smarter customer engagement experience and improve agent productivity and content curation for external facing website(s) or

	channels. Bold360 Advise is an artificial intelligence-based knowledge management solution used by customers for internal business purposes to support their employees in client-facing roles (such as retail associates or call center agents). Bold360 HelpDesk extends these capabilities to address the needs of internal employee support roles (such as human resources or IT help) and includes artificial intelligence-based self-service capabilities, such as employee-facing chatbots, virtual agents and FAQs to improve employee productivity, and content curation.
	**GoToAssist Remote Support (GTARS), GoToAssist Corporate, GoToAssist Seeit**, and **GoToAssist Service Desk** are cloud-based remote support solutions designed to help IT professionals and IT helpdesks remotely troubleshoot and fix computers, equipment. GTARS (formerly known as RescueAssist), the next generation of LogMeIn's GoToAssist remote support solution, provides an integrated toolset built specifically for IT managers, consultants, and managed service providers. GoToAssist Mobile Support is an add-on to GoToAssist Remote Support that allows agents to remotely view, and in certain cases control, select mobile devices through a web browser or application. GoToAssist Corporate extends these capabilities to address the needs of professional IT helpdesks and customer support organizations to securely connect to customers and provide live remote assistance using two-way screen-sharing, integrated chat, and mouse and keyboard control to resolve technical issues. GoToAssist Seeit enables individuals and support organizations to securely connect to a live stream of an individual's mobile device camera allowing the individual to physically show the agent any support issue that requires resolution. GoToAssist Service Desk is a cloud-based application that enables IT organizations to manage their IT services from end to end. Service Desk covers the full spectrum of managing a service, from dealing with customer issues to implementing changes to a service and mapping your assets and infrastructure. With Service Desk, support teams can also create a self-service portal where customers and employees can submit support requests and track the progress of their issue, as well as view knowledge-base documents to resolve issues on their own. Service Desk is based on the internationally recognized Information Technology Infrastructure Library (ITIL) framework and is designed to enable the easy application of ITIL best practices to managing incidents, problems, changes, releases, and

	configuration items. Unlike Remote Support, Service Desk does not access, control, or scan other machines for purposes of monitoring or support.
Rescue by LogMeIn	**LogMeIn Rescue** is LogMeIn's remote support and customer care service, which is used by helpdesk professionals and large customer care organizations to provide remote support via the internet without the need of pre-installed software. Using LogMeIn Rescue, support and customer service professionals can communicate with end users through an internet chat window while diagnosing and repairing PC, server, and mobile device problems. If given permission by the end user, the support professional can access, view, or even take control of the end user's device to take the necessary support actions and to train the end user on the use of software and operating system applications. LogMeIn Rescue+Mobile is an add-on of LogMeIn Rescue's web-based remote support service that allows customer care technicians and IT professionals to remotely access and support iOS and Android smartphones and tablets. A complementary and optional offering with any LogMeIn Rescue license, Rescue Lens extends this remote support paradigm to virtually any product. Not just computers and smartphones, by enabling end users to utilize the cameras on the personal smartphone or tablet to stream live video back to support professionals.

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

LogMeIn designs its processes and procedures to meet the objectives for LogMeIn's CES Services. Those objectives are based on the service commitments that LogMeIn makes to user entities and the financial, operational, and compliance requirements that LogMeIn has established for the services.

Security, availability, and confidentiality commitments to customers (user entities) are documented in customer agreements and communicated on LogMeIn's website (https://www.logmeininc.com/legal/terms-and-conditions and https://logmeininc.com/trust/), as well as in the description of services provided online.

LogMeIn establishes operational requirements that support the achievement of security, availability, and confidentiality commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in LogMeIn's system policies and

procedures, system design documentation, and customer contracts. LogMeIn's corporate policies define an organization-wide approach to how systems and data are protected, how information and systems are maintained and made available for operation, and how LogMeIn meets its objectives.

This documentation includes policies around how LogMeIn's CES Services are designed and developed, how the system operates, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the services.

System Boundaries

This description of LogMeIn's CES System includes the design of the company's controls relevant to security, availability, and confidentiality. This description does not include other company or third-party service offerings which may complement, support, or access LogMeIn's CES System operation(s).

COMPONENTS OF THE SYSTEM USED TO PROVIDE SERVICES

Infrastructure

LogMeIn's CES Services infrastructure redundancy design includes server and database clustering, Internet Protocol (IP) and Domain Name System (DNS) load balancing, containerized services, and use of Internet Service Providers (ISPs).

The CES Services are built on an infrastructure with measures and controls designed to provide high availability and as applicable, are hosted by the following data center and cloud service providers:

- Amazon Web Services, Inc. (AWS);
- Equinix, Inc. (Equinix);
- Microsoft Azure (Azure); and
- Switch, Ltd. (Switch).

LogMeIn's data center and cloud service providers either maintain ISO 27001 compliance, have current SOC 1 or SOC 2 reports, or otherwise undergo on-site assessments by LogMeIn which are reviewed by the LogMeIn Governance, Risk, & Compliance (GRC) Team to ensure consistency with LogMeIn's vendor risk management requirements/policies.

LogMeIn's service architecture is designed to perform replication in near-real-time to geo-diverse locations.

LogMeIn's Technology Operations Department (TechOps) manages production servers, monitors systems, performs backups, upgrades operating systems, and manages production firewalls and system updates. The LogMeIn Security and Information Technology (IT) teams manage the configuration of corporate firewalls, network system security, and endpoint devices (desktops, laptops, and mobile devices).

Authentication and Access

Physical and logical access controls are implemented to restrict access to the CES Services' production systems, internal support tools, and customer data (referred to as Content in the LogMeIn Terms of Service). These control procedures are designed to prevent or mitigate the threat of unauthorized application access and data loss in corporate and production environments. LogMeIn follows a formal process to grant or revoke employee access to LogMeIn resources (corporate systems, applications, and production environments). This process is designed to grant access rights to systems and data only to authorized users. Both user and internal access to customer data is restricted by using unique user account IDs, where technically feasible. Access to sensitive systems and applications requires multi-factor authentication in the form of a unique user account ID, strong passwords, security keys, and/or specialized security tokens. Periodic reviews of access lists are implemented to help ensure access to customer data is appropriate and authorized. Access to production machines, network devices, and support tools is managed via an access management procedure and access is reviewed as needed on at least a quarterly basis.

Software

The CES Services are developed by the LogMeIn software development staff and run on shared multi-tier architectures with network segmentation and server role assignments.

People and Organization

LogMeIn has implemented a process-based system and environment designed to deliver the CES Services to customers. In order to deliver consistent and quality services, LogMeIn has invested in developing a highly skilled team of resources and has adopted standardized, repeatable processes. LogMeIn has established internal teams to efficiently manage core infrastructure and product related security, availability, and confidentiality controls.

Formal organizational structures exist and are made available to LogMeIn employees on LogMeIn's intranet and human resource information system (HRIS). LogMeIn's HRIS provides drill-down functionality for identifying employees in the functional operations team. Executive and senior leadership play important roles in establishing LogMeIn's tone and core values with regards to the support and implementation of the security program. Management has also established authority and appropriate lines of reporting for key personnel.

LogMeIn has developed and documented formal policies, standards, procedures, and job descriptions for operational areas including security administration, change management, hiring, training, performance appraisals, terminations, and incident detection and response. These policies and procedures have been designed to segregate duties and enforce entitlements based on job responsibilities and implementing least-privilege principles. Policies, standards, and procedures are reviewed and updated as necessary.

LogMeIn ensures that employees and contractors undergo position-appropriate background investigations to the extent permitted by applicable law and are bound to appropriate confidentiality obligations (e.g., by executing a non-disclosure agreement). All newly-hired employees are required to review and formally acknowledge the following Corporate Policies during on-boarding: Code of Business Conduct and Ethics, Global Workplace Conduct Policy, Information Security Policy, Acceptable Use Standard, Insider Trading and Whistleblower Hotline, and Disclosure Policy. Additionally, employees are required to complete annual training programs for confidentiality and information security in order to support data confidentiality obligations.

Policies and Procedures

LogMeIn maintains policies and procedures to assist in guiding business operations. The procedures include control activities designed to help ensure that operations are carried out properly, consistently, and efficiently. LogMeIn uses a risk management approach to select and develop these control activities. After relevant risks are identified and evaluated, controls are established, implemented, monitored, reviewed, and improved, in each case, when determined necessary to meet the overall objectives of the organization.

Applicable policies are reviewed by management on no less than an annual basis to ensure that, where determined necessary, relevant procedures and standards are updated in accordance with contractual and legal commitments, as well as company requirements and standards. Additionally, applicable policies, when determined necessary, are reviewed upon material changes or revisions to the relevant environment. Management posts policy updates to LogMeIn's intranet site, as needed, and notifies employees when specified policies need to be acknowledged.

Change Management

Change management guidance is included in the Security Standard and has been developed in accordance with relevant commitments and requirements. It details the procedures for infrastructure and developmental changes, including design, implementation, configuration, testing, modification, and maintenance of systems.

Furthermore, processes and procedures are in place to verify that changes have been authorized, approved, and tested before being applied to a production environment. Policies are in place to

provide guidance for the management, modification, and implementation of system changes to infrastructure and supporting applications.

Changes are approved and tested in a staging environment that exists separately from the production environment. Regression, manual, and/or automated testing is performed in a QA/staging environment prior to being released into production. If testing is successful, changes are reviewed and approved for final release.

Data

LogMeIn provides controls for the access, transfer, and storage of specified data. All product feature launches that include new collection, processing, or sharing of customer data are required to go through the appropriate internal review process. LogMeIn has also established incident response processes to report and handle events related to confidentiality. To preserve the confidentiality of information, LogMeIn establishes agreements, including non-disclosure agreements, which are designed to preserve confidentiality of information and technology that may be exchanged with external parties.

The CES System is designed to enable authenticated LogMeIn consumers to access and manage their customer data through tools that allow them to manage access to the CES Services, configure how the CES Services operate, and initiate actions to remove or delete customer data. LogMeIn has also implemented technical and physical controls designed to prevent unauthorized access to, or disclosure of, customer data.

LogMeIn has established training programs for privacy and information security to support data confidentiality and all employees are required to complete these training programs annually. LogMeIn monitors the performance of third parties supporting the CES System through periodic reviews, which evaluate performance against contractual obligations, including confidentiality commitments.

When storage media used in providing the CES Services has reached the end of its useful life, LogMeIn procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. LogMeIn uses industry-standard techniques (e.g., taking into account those documented in NIST SP 800-88) when decommissioning relevant assets. All decommissioned hardware is appropriately sanitized and physically destroyed in accordance with industry-standard practices.

System Monitoring and Incidents

LogMeIn incorporates continuous programs that monitor and report server health, performance, availability, uptime, capacity, and other relevant metrics. Issues are created via automated ticket generation and sent to the Network Operations Center (NOC) for review.

There were no identified system incidents that were (a) the result of controls that were not suitably designed or operating effectively or (b) otherwise resulted in a significant failure in the achievement of one or more of those service commitments and system requirements during the reporting period September 1, 2019 to August 31, 2020.

Complementary User-Entity Controls

LogMeIn's system was designed with the assumption that certain controls will be implemented by user entities. In certain situations, the application of specified internal controls at user organizations is necessary to achieve certain Security, Availability, and Confidentiality Trust Services Criteria included in this report.

Subservice Organizations

LogMeIn uses service organizations to perform data center and cloud service related to the Trust Services Criteria (subservice organizations). The description does not include any of the controls expected to be implemented at the subservice organizations, which include Amazon Web Services (AWS), Equinix, Inc. (Equinix), Microsoft Azure (Azure), and Switch, Ltd. (Switch).

System Incidents

There were no identified material system incidents that were (a) the result of controls that were not suitably designed or operating effectively or (b) otherwise resulted in a significant failure in the achievement of one or more of those service commitments and system requirements during the reporting period September 1, 2019 to August 31, 2020.

Changes to the System During the Period

During the period of September 1, 2019 to August 31, 2020, the following changes occurred to LogMeIn and the applicable Customer Engagement and Support (CES) System used to provide services, which should not impact the ability to meet the test controls and criteria of this report.

- On December 17, 2019, LogMeIn entered into a definitive agreement (i.e., a "go-private transaction") to be acquired by global private equity firms Francisco Partners and Evergreen Coast Capital Corp. Completion of the sale was announced on August 31, 2020, resulting in LogMeIn (inclusive of the respective System referenced herein) becoming a privately-owned company.
- Business Continuity policies and procedures were expanded in 2020 to include controls appropriate for remote working conditions mandated at times during the COVID-19 pandemic.