SOC 3® – Reporting on System and Organization Controls

A SOC 3® Type 2 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 Relevant to the Trust Services Criteria Relevant to Security, Availability, and Confidentiality

Throughout the Period September 1, 2018 to August 31, 2019

LogMeIn® Customer Engagement & Support

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, 2018 to August 31, 2019, 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, 2018 to August 31, 2019, 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 18, 2019

October 18, 2019

Gerald Beuchelt
Chief Information Security Officer
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, 2018 to August 31, 2019, 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, 2018 to August 31, 2019, 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, 2018 to August 31, 2019, to provide reasonable assurance that LogMeIn's service commitments and system requirements were achieved based on the applicable trust services criteria.

Gerald Beuchelt
Chief Information Security Officer

Description of the Customer Engagement and Support (CES) System

BACKGROUND

LogMeIn is a public 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 business units 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 BoldChat, Bold360, Bold360 ai, GoToAssist, GoToAssist Corporate and LogMeIn Rescue (collectively, referred to as CES Services).

bold360	Bold360 (including BoldChat) is a live-chat and omni-channel engagement service that helps customer service staff, ranging from sales to pre-and-post sales support, to directly engage and provide assistance to visitors of their organization's website. Key features include real-time visitor monitoring, co-browsing, detailed reporting on chat activity and its overall effectiveness, the ability to define rules that automatically trigger the initiation of a chat window, the ability to route and distribute chats to improve efficiency and the ability to monitor and manage customer conversations on Twitter, email and via SMS messages. BoldChat service offerings range from a basic free offering to a fully-featured

	enterprise offering, with multiple pricing tiers based on the number of users and desired features. Bold360 ai is an automated customer service, helpdesk and CRM platform that uses artificial intelligence, bots, machine learning and user interface to build and maintain a knowledge base, or KB, and make it available to support agents, employees and end-users across multiple platforms. Bold360 ai captures a company's knowledge in the form of replies to contextual or personalized inquiries, decision trees and KB articles, and maintains the context and matches customer inquiries with KB answers. The intelligent KB also collects inquiries and learns answers as well as monitors answers to incoming tickets and publishes them to the KB so that information is available broadly to authorized agents – such content can be viewed, approved, added, edited or deleted manually. Bold360 ai also provides a customer service queue management tool that utilizes learning algorithms, intent repository, and structured rule settings as well as analytics that provide insight and optimization opportunities.
GoToAssist	GoToAssist is a cloud-based IT support solution designed for remote troubleshooting and fixing computers, mobile devices, applications, and other physical devices. The toolset is built specifically for IT managers, consultants and managed service providers allowing them to securely resolve customer issues. The integrated service desk enables teams to manage incidents, problems or changes. This product consists of three modules: GoToAssist Remote Support, GoToAssist Service Desk and GoToAssist Seeit.
GoToAssist	GoToAssist Corporate extends the capabilities of GoToAssist 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, mouse and keyboard control to resolve technical issues.
Rescue	LogMeIn Rescue is a 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, mobile device and kiosk problems. If given permission by the user, the support professional can access, view or even take control of the end-user's device to take 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, Android and Blackberry smartphones and tablets.

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 its 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), as well as in the description of services provided online.

LogMeIn establishes operational requirements that support: (i) the achievement of security, availability, and confidentiality commitments; (ii) relevant applicable laws and regulations; and (iii) other system requirements. Such requirements are communicated in LogMeIn's system policies and/or procedures, system design documentation and contracts with customers. Corporate policies and/or procedures define an organization-wide approach to: (i) how systems and data are protected; (ii) how information and systems are maintained and made available for operation; and(iii) how LogMeIn meets its objectives.

This documentation includes policies and/or procedures 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 utilization of multiple 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 (AWS), Equinix, Inc. (Equinix), Microsoft Azure (Azure), and Switch, Ltd. (Switch).

Each of LogMeIn's data centers and cloud service providers are certified ISO 27001 compliant, have current SOC reports, certifying compliance with AICPA's Trust Services Criteria, and/or otherwise undergo on-site assessments by LogMeIn which are reviewed by the Director of Governance, Risk and Compliance (GRC) in order 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 Corporate Information Technology (IT) Security Team, with the full support of the IT Department, manages 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 through the use of unique user account IDs, where technically feasible. Access to sensitive systems and applications require 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 are 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 in order 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 guide 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 relevant procedures and standards are updated in accordance with contractual and legal commitments, as well as company requirements and standards. Additionally, applicable policies 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.

Further, 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 the quality assurance/staging environment prior to releasing to production. Once 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 utilized 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.

During the reporting period September 1, 2018 to August 31, 2019, 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.

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.