SOC 3® – Reporting on Controls at a Service Organization

Independent Service Auditor’s Report on LogMeIn’s Identity and Access Management (IAM) System Relevant to the Trust Services Principles and Criteria for Security, Availability, and Confidentiality

Throughout the Period September 1, 2017 to August 31, 2018
Management’s Assertion Regarding the Effectiveness of its Controls Over the Identity and Access Management System Based on the Trust Services Principles and Criteria for Security, Availability, and Confidentiality

We, as management of LogMeln, Inc. (LogMeln IAM or the Company), are responsible for designing, implementing, operating, and maintaining effective controls over the Identity and Access Management System (system) throughout the period September 1, 2017 to August 31, 2018, to provide reasonable assurance that LogMeln IAM’s commitments and system requirements relevant to security, availability, and confidentiality were achieved. Our accompanying description 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, 2017 to August 31, 2018, to provide reasonable assurance that LogMeln IAM’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 100A, Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2016) (AICPA, Trust Services Criteria). LogMeln IAM’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 presented in the accompanying description.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of 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, 2017 to August 31, 2018 to provide reasonable assurance that LogMeIn IAM’s service commitments and system requirements were achieved based on the applicable trust services criteria.

Very truly yours,

Ian Pitt

Chief Information Officer
LogMeIn, Inc.
320 Summer Street
Boston, MA 02210
Report of Independent Service Auditors

To: LogMeIn, Inc.

SCOPE

We have examined LogMeIn, Inc.’s (referred to hereafter as LogMeIn IAM or the service organization) accompanying assertion titled “Management’s Assertion Regarding the Effectiveness of its Controls Over the Identity and Access Management System Based on the Trust Services Principles and Criteria for Security, Availability, and Confidentiality” (assertion) that the controls within LogMeIn IAM’s Identity and Access Management System (system) were effective throughout the period September 1, 2017 to August 31, 2018, to provide reasonable assurance that LogMeIn IAM’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 100A, Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2016) (AICPA, Trust Services Criteria).

SERVICE ORGANIZATION’S RESPONSIBILITIES

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

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

INHERENT LIMITATIONS

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance 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 IAM’s Identity and Access Management System were effective throughout the period September 1, 2017 to August 31, 2018, to provide reasonable assurance that LogMeIn IAM’s service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

John D. Redding, CPA.CITP
c/o Tevora Business Solutions
One Spectrum Pointe Drive, Suite 200
Lake Forest, CA 92630
T: (657) 204-2737 • compliance@reddingadvisory.com
Description of The LogMeIn Identity and Access Management 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: 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 include or are offered in free, fee-based, and/or premium software services.

SERVICES PROVIDED

The Identity and Access Management (IAM) System is designed to deliver individuals, line of business teams, security professionals, as well as internal and external IT professionals with secure remote access tools needed to manage and secure passwords, remote computers and other Internet-enabled devices and internet applications, as well as to automate common IT tasks. The in-scope products that make up the IAM System are GoToMyPC, LastPass, LogMeIn Central, LogMeIn Pro (collectively, referred to as IAM Services).

| GoToMyPC | GoToMyPC provides secure, remote access to a PC or Mac from virtually any Internet-connected computer, as well as from supported iOS or Android mobile devices, such as an iPad, iPhone, Kindle Fire and Samsung Galaxy. GoToMyPC sets up with a secure encrypted connection and enables individuals to remotely use resources hosted on their desktop just as though they were sitting in front of it. |

Page | 1
© 2018 LogMeIn, Inc. All rights reserved.
| **LastPass** | LastPass is a password management and single sign on, or SSO, solution that gives individuals, business teams and enterprises the ability to securely store, create and access the user identity and login credentials for online applications and websites. Available online, in a desktop app and via iOS and Android mobile apps, LastPass is offered in free, premium and enterprise versions and runs on popular browsers, devices and operating systems. |
| **LogMeIn Central** | LogMeIn Central is a web-based management console that helps IT professionals access, manage and monitor remote computers, deploy software updates and patches, automate IT tasks and run antivirus software. LogMeIn Central is offered as a premium service with multiple pricing tiers based on the number of computers supported and desired features. |
| **LogMeIn Pro** | LogMeIn Pro is a premium remote access service that provides secure access to a remote computer’s cloud and/or locally stored files or other Internet-connected devices such as point-of-sale systems or kiosks, from any other Internet-connected computer or iOS or Android-based smartphones or tablets. Once a LogMeIn Pro host is installed on a device, a user can access that device’s desktop, files, applications and network resources remotely from their other Internet-enabled devices. |

**INFRASTRUCTURE**

LogMeIn’s IAM Services infrastructure redundancy design includes server and database clustering, internet protocol (IP) and domain name system (DNS) load balancing, containerized services, and utilization, as applicable, of multiple telecommunications and internet service providers (ISPs). LogMeIn’s IAM Services are built on an infrastructure with measures and controls designed to provide high availability.

**DATA CENTERS AND REDUNDANCY**

LogMeIn’s redundant service architecture is designed to perform replication in near-real-time to geo-diverse data centers. LogMeIn maintains consistent policies and standards across its data
centers for physical security in order to help protect production and corporate servers, network devices, and network connections within LogMeIn data centers.

The data centers are connected through multiple encrypted network links and secure interfaces. LogMeIn uses a dashboard that provides details such as resources, processing capacity, and storage availability to monitor the availability of IAM Services across data centers, and to validate that data has been replicated to more than one geographically dispersed location.

AUTHENTICATION AND ACCESS

Physical and logical access controls are implemented to restrict access to the IAM 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 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.

CHANGE MANAGEMENT

Change management policies have been developed in accordance with relevant commitments and requirements, detailing the procedures for infrastructure and developmental changes, including design, implementation, configuration, testing, modification, and maintenance of systems.

Further, processes and procedures are in place in order 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 IAM 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 IAM Services, configure how the IAM Service operates, 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 its employees are required to complete these training programs annually. LogMeIn monitors the performance of third parties supporting the IAM System through periodic reviews, which evaluate performance against contractual obligations, including confidentiality commitments.

When storage media utilized in providing the IAM 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.

NETWORK ARCHITECTURE AND MANAGEMENT

The IAM System architecture utilizes a redundant network infrastructure, designed to perform replication in near-real-time to geo-diverse locations. LogMeIn incorporates vulnerability management and intrusion detection programs into its production and Corporate IT environments, as well as perimeter devices designed to protect the LogMeIn network from
external attacks. LogMeIn regularly reviews relevant risks that may threaten the achievement of its service commitments and updates to existing control activities and information security policies are performed as determined necessary.

The IAM System is architected in a manner intended to maintain availability of its IAM Services through defined programs, processes, and procedures. These programs address the processes and procedures by which LogMeIn identifies, responds to, and recovers from potential availability events or security incidents within its environment. This program builds upon the traditional approach of addressing contingency management, incorporating elements of business continuity and disaster recovery plans, while also expanding to consider critical elements of proactive risk mitigation strategies.

PEOPLE AND ORGANIZATION

LogMeIn has implemented a process-based system and environment designed to deliver the IAM 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 the Company’s intranet and human resource information system (HRIS). The Company’s HRIS provides drill-down functionality for identifying employees in the functional operations team. Executive and senior leadership play important roles in establishing the Company’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 Company’s Code of Business Conduct and Ethics and are additionally required to complete annual training programs for privacy and information security in order to support data confidentiality obligations.