



**LogMeIn**<sup>®</sup> LastPass

## SOC 3<sup>®</sup> – Reporting on System and Organization Controls

**Independent Service Auditor's Report**

A SOC 3<sup>®</sup> Independent Service Auditor's Report on LogMeIn's LastPass System  
Relevant to **Security, Availability, and Confidentiality**

For the Period September 1, 2020 to August 31, 2021



December 7, 2021

Michael Oberlaender  
Chief Information Security Officer  
LogMeIn, Inc.  
333 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 LastPass 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 LastPass System (system) throughout the period September 1, 2020 to August 31, 2021, 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 attachment A 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, 2020 to August 31, 2021, 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 attachment B.

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, 2020 to August 31, 2021, to provide reasonable assurance that LogMeIn's service commitments and system requirements were achieved based on the applicable trust services criteria.

DocuSigned by:

*Michael Oberlaender*

0721B94F34824F1...

Michael Oberlaender

Chief Information Security Officer



# 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 LastPass System based on the Trust Services Criteria for Security, Availability, and Confidentiality" (assertion) that the controls within LogMeIn's LastPass System (system) were effective throughout the period September 1, 2020 to August 31, 2021, 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 LastPass System were effective throughout the period September 1, 2020 to August 31, 2021, 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.



J. Lopez, CPA, CITP

Irvine, CA  
December 7, 2021

## Attachment A – LogMeIn’s Description of the Boundaries of Its LastPass System

### BACKGROUND


LogMeIn is a provider of cloud services for the work-from-anywhere economy. LogMeIn’s portfolio of category-defining products, such as GoTo, LastPass, Rescue, LogMeIn Central and more, allow its users to work remotely, collaborate with other users, and support and manage remote computers and other internet-enabled devices. LogMeIn is a global SaaS company with tens of millions of active users, more than 3,500 global employees, and approximately 2 million customers worldwide who use the Company’s software as an essential part of their daily lives.

LogMeIn is headquartered in Boston, MA with additional locations in North America, South America, Europe, Asia, Australia and thousands of home offices around the globe.

On August 31, 2020, LogMeIn, Inc. was acquired by affiliates of Francisco Partners and Evergreen Coast Capital Corp. in a take-private transaction.

### SERVICES PROVIDED

LogMeIn’s LastPass System is designed to provide individuals, businesses, security professionals, and internal and external IT professionals with secure access tools needed to manage and secure passwords, sensitive information, and cloud and legacy apps, as well as to automate common IT tasks such as user onboarding and offboarding. The in-scope products that make up this lineup are LastPass Business and the add-ons for Advanced Single Sign-On and Advanced Multi-Factor Authentication.

	<p><b>LastPass</b> is a password management solution that enables users to generate, store, and share credentials while providing insight and control to Administrators. LastPass Business offers additional access and authentication features, including single sign-on for simplified access to a limited number of cloud applications and multi-factor authentication (MFA) to secure the LastPass vault and single sign-on applications.</p> <p>Add-ons include Advanced Single Sign-On that enables users to access cloud applications through a single sign-on and</p>
---	---

	<p>Advanced Multi-Factor Authentication, which leverages biometric and contextual factors to assist in verifying a user's identity and restricting unauthorized access. LastPass MFA offers an authentication experience that can be deployed across cloud and legacy applications, VPNs, workstations, and identity providers.</p> <p>LastPass is available online, in a desktop application, and via iOS and Android mobile apps. LastPass is offered in free, premium, and enterprise versions and runs on most browsers, devices and operating systems.</p>
--	---

## System Boundaries

This description of LogMeIn's LastPass 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 that may complement, support, or access LogMeIn's LastPass System operation(s). Compliance with laws and regulations for privacy, export, or similar requirements are not included in the scope of this description.

## COMPONENTS OF THE SYSTEM USED TO PROVIDE SERVICES

### Infrastructure

LogMeIn's LastPass 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 LastPass System is 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)
- Switch, Ltd. (Switch)

LogMeIn's data center and cloud service providers either maintain ISO 27001 compliance or have current SOC 1 or SOC 2 reports, which indicate compliance with the AICPA's Trust Services



Criteria. They may otherwise undergo on-site assessments by LogMeIn, which are reviewed by the LogMeIn Governance, Risk, & Compliance (GRC) Team in order to ensure consistency with LogMeIn's vendor risk management requirements and policies.

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

LogMeIn's Global Infrastructure Services (GIS) and DevOps teams manage production servers, monitor systems, perform backups, upgrade operating systems, and manage 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 LastPass System's production environment, internal support tools, and customer data (referred to as Content in the [LogMeIn Terms of Service](#)). These access control procedures are in place and designed to prevent or mitigate the threats 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).

Employees' access to LogMeIn systems, applications, networks, and devices is subject to relevant restrictions based upon specific job functions. Access to customer production data is restricted to authorized personnel and is granted solely on a "need-to-know" basis.

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, 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 LastPass services are developed by the LogMeIn software development staff and run on shared multi-tier architectures with network segmentation and server role assignments.

### System Monitoring

LogMeIn incorporates programs that are designed to continuously monitor and report on the LastPass System.



The Network Operations Center (NOC) is staffed twenty-four (24) hours per day, seven (7) days per week, and is responsible for monitoring the availability and performance of the LastPass System. It is tasked with researching, analyzing, reporting, and escalating issues believed or determined to be impacting the applications and their associated operations. The NOC follows a set of standard operating procedures and monitors and reports availability and uptime metrics through a series of dashboards and reports.

The Security Operations Center (SOC) operates twenty-four (24) hours per day, seven (7) days per week, and its primary function is to monitor and respond to threats externally and internally within the organization. The SOC uses security sensors and analysis systems to identify potential issues and responds to them through a defined Incident Response Plan.

The Corporate IT Department, in addition to its other roles and responsibilities, monitors for content that may be harmful to the corporate environment through web content filtering software. The filters are monitored, analyzed, and adjusted on an ongoing basis, as determined necessary by the Corporate IT Security Team. Enterprise workstations are deployed with endpoint device management solutions that are designed to monitor, detect, and mitigate vulnerabilities. Audit logging is enabled on enterprise laptops and relevant alerts are sent to the SOC for follow-up and resolution.

### 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 LogMeIn's service commitments and system requirements during the reporting period September 1, 2020 to August 31, 2021.

### 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 to policies and procedures are reviewed and approved by the CISO. Relevant customer-facing system changes, upgrades, and releases may be communicated through appropriate channels, including but not limited to, the status pages located on the applicable product web page.

## People and Organization

LogMeIn has implemented a process-based system and environment designed to deliver the LastPass 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 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, in each case controls are established, implemented, monitored, reviewed, and improved 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 as needed to LogMeIn's intranet site and notifies employees when specified policies need to be acknowledged.

## Data

LogMeIn's services, as outlined in this report, include the handling of electronic information submitted by or otherwise maintained on behalf of its customers within the applicable LogMeIn service environment. Such information is encrypted in transit and, depending upon the product, may employ additional technical measures, such as encryption at rest. Product or suite-specific technical specifications, including applicable encryption standards and methods, may be found either on the applicable product-specific resource web pages or in the Security and Privacy Operational Controls (SPOC) documentation, located on the LogMeIn Trust & Privacy Center web pages under Product Resources.

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.

LogMeIn retains Customer Content in accordance with its internal policies and procedures, applicable legal and regulatory requirements, and any contractual agreements with its customers. To the extent applicable, automated retention periods for Customer Content are disclosed via the applicable SPOC located in the Product Resources section of the LogMeIn Trust & Privacy Center. When disposing of electronic data storage devices, LogMeIn evaluates against industry-standard practices and internal controls to determine the appropriate approach to ensure that data destruction is irreversible.

## Changes to the System During the Period

During the period of September 1, 2020 through August 31, 2021 the following changes occurred to LogMeIn and the applicable LastPass System used to provide services, which should not impact the ability to meet the tested controls and criteria of this report.

- Business Continuity policies and procedures were expanded in 2020 and 2021 to include controls appropriate for remote working conditions mandated at times during the COVID-19 pandemic.

- The business group Identity and Access Management (IAM) was rebranded to Identity. As part of the change, the following products that were previously within the scope of this (IAM) Report are now under the Remote Solutions Group (RSG) SOC 2 Report scope:
  - GoToMyPC
  - LogMeIn Pro
  - LogMeIn Central
- The report only contains the LastPass product; therefore, the System was renamed from the Identity and Access Management (IAM) System to the LastPass System.

### 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 includes Amazon Web Services (AWS), Equinix, Inc. (Equinix), Microsoft Azure (Azure), and Switch, Ltd. (Switch).

## Attachment B – Principal Service Commitments and System Requirements

LogMeIn designs its processes and procedures to meet the objectives for LogMeIn's LastPass System. 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:** LogMeIn documents service-specific information about our technical and organizational security measures (e.g., as located in the Security and Privacy Operational Controls or "SPOC" documentation found at LogMeIn's Trust and Privacy Center at <https://logmein.com/trust/>).
- **Confidentiality:** LogMeIn maintains a global privacy and security program designed to protect Customer Content and any associated personal data that LogMeIn may collect and/or process.
- **Availability:** LogMeIn maintains backup and recovery processes designed to ensure service availability.

Security, availability, and confidentiality commitments to customers (user entities) are documented in customer agreements and communicated on LogMeIn's websites (including, <https://www.logmein.com/legal/terms-and-conditions> and <https://logmein.com/trust/>), as well as in the description of services provided online. For more information, please see an excerpt from LogMeIn's online Terms and Conditions:

**4.2. Your Privacy and Security.** We maintain a global privacy and security program designed to protect your Content and any associated personal data we may collect and/or process on your behalf. You can visit our Trust & Privacy Center (<https://www.logmein.com/trust>) to review applicable data processing locations and Sub-Processor Disclosures, as well as Service-specific information about our technical and organizational security measures (located in the Security and Privacy Operational Controls or "SPOC" documentation). When providing our Services, we act as a data processor, service provider, or the equivalent construct. To review and execute our Data Processing Addendum ("DPA"), please visit [www.logmein.com/legal](http://www.logmein.com/legal).

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. These include policies around how the service is designed and developed, how the system is operated,

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 for the operation and development of the LastPass System.