LastPass

SOC 3® – Reporting on System and Organization Controls

Independent Service Auditor's Report

A SOC 3® Independent Service Auditor's Report on LastPass' LastPass System Relevant to **Security, Availability, and Confidentiality** for the Period September 1, 2021 to August 31, 2022

October 31, 2022

On behalf of GoTo:

Olga Lagunova
Chief Technology Officer
GoTo Group, Inc.
333 Summer Street
Boston, MA 02210

On behalf of LastPass:

Gabor Angyal
Vice President, Head of Engineering – LastPass
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

Together, GoTo Group, Inc. ("GoTo") and its affiliate entity, LastPass US LP ("LastPass"), we, as management of LastPass US LP (LastPass) are responsible for designing, implementing, operating, and maintaining effective controls within LastPass' LastPass System (system) throughout the period September 1, 2021 to August 31, 2022, to provide reasonable assurance that LastPass' 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, 2021 to August 31, 2022, to provide reasonable assurance that LastPass' 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*). LastPass' 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, 2021 to August 31, 2022, to provide reasonable assurance that LastPass' service commitments and system requirements were achieved based on the applicable trust services criteria.

On behalf of GoTo:		On behalf of LastPass:	
By	DocuSigned by: Olga Lagunova AFAE658D354B4C3...	By	DocuSigned by: Gabor Angyal 829226E2595F44F...
Name	Olga Lagunova	Name	Gabor Angyal
Title	Chief Technology Officer - GoTo	Title	VP, Head of Engineering

Report of Independent Service Auditors

To: Management of LastPass US LP

SCOPE

We have examined LastPass US LP's (LastPass') 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 LastPass' LastPass System (system) were effective throughout the period September 1, 2021 to August 31, 2022, to provide reasonable assurance that LastPass' 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*).

The information included in attachment C, "Other Information Provided by LastPass That Is Not Covered by the Service Auditor's Report," is presented by LastPass's management to describe the service organization's response to a security incident and is not a part of LastPass's description of its LastPass System made available to user entities during the period September 1, 2021 to August 31, 2022. Information about LastPass's security incident has not been subjected to the procedures applied in the examination and accordingly, we express no opinion on it.

SERVICE ORGANIZATION'S RESPONSIBILITIES

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

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

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 LastPass' LastPass System were effective throughout the period September 1, 2021 to August 31, 2022, to provide reasonable assurance that LastPass' service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Irvine, CA
October 31, 2022

Attachment A – An Overview of LastPass' System

BACKGROUND

LastPass is an advanced password and identity management solution that keeps users and businesses' digital life secure. With LastPass, you can achieve security goals faster, removing everyday password-related friction, such as generating, storing, managing, and monitoring your and your business' most sensitive credentials. Trusted by the most, with over 1B sites secured, 33M lifetime registered users, and 100,000 Business customers, LastPass makes online security simple.

LastPass 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, GoTo Group, Inc. (GoTo), formerly LogMeIn, Inc., was acquired by affiliates of Francisco Partners and Evergreen Coast Capital Corp. in a take-private transaction. In December 2021, GoTo announced the separation of LastPass into a standalone company. In February 2022, LogMeIn, Inc. rebranded to GoTo.

As of the date of this report, LastPass is still in the process of separating from GoTo, and LastPass continues to rely on GoTo for certain infrastructure, people, technology, and processes which are provided to LastPass as part of an inter-company transition services agreement.

SERVICES PROVIDED

LastPass provides individuals and businesses with a solution that removes everyday password-related friction by helping to generate, store, manage, and maintain users' passwords. LastPass is available online, in a desktop application, and via iOS and Android mobile apps. LastPass is offered in free, premium, and enterprise versions with the option to add advanced add-on features.

LastPass	LastPass is a password manager that empowers users to generate, secure, access, and share credentials, while also offering customized security policies (100+), dark web monitoring, single sign-on (stand-alone or integrated), and a multi-factor authentication option for streamlined access and authentication.

	In addition, LastPass offers advanced add-on options for single sign-on and multi-factor authorization. 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.

System Boundaries

This description of the 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 the 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

LastPass' infrastructure redundancy design includes server and database clustering, Internet Protocol (IP) and Domain Name System (DNS) load balancing, containerized services, and utilization 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, is hosted by the following data center and cloud service providers:

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

Our data center and cloud service providers either maintain ISO 27001 compliance or have current SOC 1 or SOC 2 reports that indicate compliance with the AICPA's Trust Services Criteria. They may otherwise undergo on-site assessments by GoTo, which are reviewed by the GoTo Governance, Risk, and Compliance (GRC) Team to ensure consistency with GoTo's vendor risk management requirements and policies.

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

GoTo'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 GoTo 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 LastPass 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. LastPass follows a formal process to grant or revoke employee access to LastPass resources (corporate systems, applications, and production environments).

Employee access to LastPass 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. Employee application and data source access lists are reviewed on at least a quarterly basis to verify that current access levels for employees are authorized and appropriate for their position and that access is revoked promptly upon termination.

Software

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

System Monitoring

GoTo incorporates programs that are designed to continuously 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. The NOC is staffed 24 hours per day, 7 days per week, and is responsible for monitoring the availability and performance of the LastPass System. The NOC follows a set of standard operating procedures and monitors and reports availability and uptime metrics through a series of dashboards and

reports. Multiple tools are used in monitoring operations and data is reviewed and made available to management and the business on an ongoing basis, as deemed necessary.

The Security Operations Center (SOC) operates 24 hours per day, 7 days per week. 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. On an ongoing basis, SOC team members analyze application and production log data using industry-standard tools. The SOC team generates daily reports of their activities, which are reviewed on at least a weekly basis by Security leadership.

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.

The GIS Department uses automated tools that are configured to analyze and monitor production systems for processing integrity, availability, and performance. Policies and procedures exist to support backup scheduling, network monitoring, and overall data handling. GIS has also developed procedures related to backup scheduling, network monitoring, and overall data handling, which are supported by the Information Backup Policy.

System Incidents

As of the date of the Management Assertion, the following material system incident had been identified.

On August 25, 2022, LastPass disclosed a security incident on its blog after detecting unusual activity within the LastPass Development environment. Please refer to Attachment C of this report for additional information regarding LastPass' investigation.

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

LastPass has implemented a process-based system and environment designed to deliver the LastPass services to customers. In order to deliver consistent and quality services, LastPass has invested in developing a highly skilled team of resources and has adopted standardized, repeatable processes. LastPass 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 LastPass 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 LastPass' 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.

During the reporting period, the GoTo Information Security Team oversaw the information security program for LastPass. LastPass is expected to separate from GoTo after the reporting period, at which time the entity will employ an independent information security team.

GoTo 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 Policy, and Insider Trading and Whistleblower Hotline and Disclosure Policy. Additionally, employees are required to complete annual training programs for confidentiality and information security to support data confidentiality obligations.

Policies and Procedures

GoTo maintains policies and procedures to assist in guiding business operations, including security administration, change management, hiring, training, performance appraisals, terminations, and incident detection and response. The procedures include control activities designed to help ensure that operations are carried out properly, consistently, and efficiently. GoTo 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 GoTo's intranet site and notifies employees when specified policies need to be acknowledged.

Data

LastPass' 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 LastPass service environment. Such information is encrypted in transit and, depending upon the product, may use 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 the Technical and Organizational Measures (TOM) documentation located on the LastPass Trust and Privacy Center web pages under Product Resources.

LastPass 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. LastPass has also established incident response processes to report and handle events related to confidentiality. To preserve confidentiality of information, LastPass establishes agreements, including non-disclosure agreements, which are designed to preserve confidentiality of information and technology that may be exchanged with external parties.

GoTo 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 TOM located in the Product Resources section of the LastPass Trust and Privacy Center. When disposing of electronic data storage devices, GoTo 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, 2021, through August 31, 2022, the following changes occurred to LastPass 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 to include controls appropriate for remote working conditions mandated at times during the COVID-19 pandemic.
- In December 2021, GoTo announced that LastPass will become a standalone company.
- In February 2022, LogMeIn is rebranded to GoTo.
- In August 2022, LastPass enhanced existing practices and processes in response to the security incident disclosed in the System Incidents section.

Complementary User-Entity Controls

LastPass' 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

LastPass 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); Switch, Ltd. (Switch); Akamai Technologies, Inc.; Splunk, Inc.; and PasswordPing, Ltd.

Attachment B – Principal Service Commitments and System Requirements

The Company designs its processes and procedures to meet the objectives for the LastPass System. Those objectives are based on the service commitments that LastPass makes to user entities and the financial, operational, and compliance requirements that LastPass has established for the services.

- **Security:** LastPass documents service-specific information about the technical and organizational security measures (e.g., as located in the "TECHNICAL AND ORGANIZATIONAL MEASURES (TOMs)" documentation found at LastPass Trust and Privacy Center at https://www.lastpass.com/trust-center).
- **Confidentiality:** LastPass maintains a global privacy and security program designed to protect Customer Content and any associated personal data that LastPass may collect or process.
- **Availability:** LastPass maintains redundancy and 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 LastPass' websites (including https://www.lastpass.com/legal-center/terms-of-service/business and https://www.lastpass.com/trust-center), as well as in the description of services provided online. For more information, please see an excerpt from LastPass' online Terms and Conditions:

> **4.2 Your Privacy and Security.** LastPass agrees to maintain appropriate organizational, administrative, and technical safeguards designed to protect your Content against any unauthorized access, loss, misuse, or disclosure, in accordance with industry standards. Additional information about LastPass' technical and organizational security measures ("TOMs"), including, but not limited to, encryption use and standards, retention periods, and other helpful information can be found in our Trust & Privacy Center https://www.lastpass.com/trust-center), along with information regarding our independent third-party security audits and certifications.

LastPass establishes operational requirements that support the achievement of security, availability, confidentiality commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in system policies and procedures, system design documentation, and customer contracts. GoTo'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 LastPass meets its objectives.

This documentation includes policies around how the LastPass System is 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.

Attachment C – Other Information Provided by LastPass That Is Not Covered by the Service Auditor's Report

LastPass Additional Disclosures

As of the date of the Management Assertion, LastPass is investigating a security incident. LastPass encourages readers of this report to visit https://blog.lastpass.com/2022/notice-of-recent-security-incident/ for the latest updates and information on this event.