A-LIGN

LastPass US LP

Type 2 SOC 3

2023

LastPass

SOC 3 FOR SERVICE ORGANIZATIONS REPORT

September 1, 2022 to June 30, 2023

Table of Contents

SECTION 1

ASSERTION OF LASTPASS US LP MANAGEMENT

ASSERTION OF LASTPASS US LP MANAGEMENT

July 31, 2023

We are responsible for designing, implementing, operating, and maintaining effective controls within LastPass US LP's ('LastPass' or 'the Company') LastPass Services System throughout the period September 1, 2022 to June 30, 2023, to provide reasonable assurance that LastPass'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*, in AICPA, *Trust Services Criteria*. Our description of the boundaries of the system is presented below in "LastPass US LP's Description of Its LastPass Services System throughout the period September 1, 2022 to June 30, 2023" 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, 2022 to June 30, 2023, to provide reasonable assurance that LastPass's service commitments and system requirements were achieved based on the trust services criteria. LastPass'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 "LastPass US LP's Description of Its LastPass Services System throughout the period September 1, 2022 to June 30, 2023".

LastPass uses Amazon Web Services ('AWS'), Microsoft Azure ('Azure'), and Switch, Ltd. ('Switch') to provide cloud hosting services (collectively, the 'subservice organizations'). The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at LastPass, to achieve LastPass's service commitments and system requirements based on the applicable trust services criteria. The description presents LastPass's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of LastPass's controls. The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary to achieve LastPass's service commitments and system requirements based on the applicable trust services criteria. The description presents the applicable trust services criteria and the complementary user entity controls assumed in the design of LastPass's controls.

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, 2022 to June 30, 2023 to provide reasonable assurance that LastPass's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of LastPass's controls operated effectively throughout that period.

Christofer Hoff
Chief Secure Technology Officer
LastPass US LP

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

A-LIGN

INDEPENDENT SERVICE AUDITOR'S REPORT

To LastPass US LP:

Scope

We have examined LastPass US LP's ('LastPass' or 'the Company') accompanying assertion titled "Assertion of LastPass US LP Management" (assertion) that the controls within LastPass's LastPass Services System were effective throughout the period September 1, 2022 to June 30, 2023, to provide reasonable assurance that LastPass'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*, in AICPA *Trust Services Criteria*.

LastPass uses AWS, Azure, and Switch to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at LastPass, to achieve LastPass's service commitments and system requirements based on the applicable trust services criteria. The description presents LastPass's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of LastPass's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at LastPass, to achieve LastPass's service commitments and system requirements based on the applicable trust services criteria. The description presents LastPass's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of LastPass's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

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's service commitments and system requirements were achieved. LastPass has also provided the accompanying assertion (LastPass 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 services 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 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 AICPA. 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 the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its 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.

Independence and Ethical Responsibilities

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

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 are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating 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

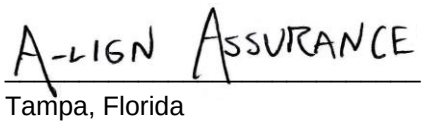
In our opinion, management's assertion that the controls within LastPass's LastPass Services System were suitably designed and operating effectively throughout the period September 1, 2022 to June 30, 2023, to provide reasonable assurance that LastPass's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects, if complementary subservice organization controls and complementary user entity controls assumed in the design of LastPass's controls operated effectively throughout that period.

The SOC logo for Service Organizations on LastPass's website constitutes a symbolic representation of the contents of this report and is not intended, nor should it be construed, to provide any additional assurance.

Restricted Use

This report, is intended solely for the information and use of LastPass, user entities of LastPass's LastPass Services System during some or all of the period September 1, 2022 to June 30, 2023, business partners of LastPass subject to risks arising from interactions with the LastPass Services System, and those who have sufficient knowledge and understanding of the complementary subservice organization controls and complementary user entity controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.

This report is not intended to be, and should not be, used by anyone other than these specified parties.



Tampa, Florida
July 31, 2023

SECTION 3

LASTPASS US LP'S DESCRIPTION OF ITS LASTPASS SERVICES SYSTEM THROUGHOUT THE PERIOD SEPTEMBER 1, 2022 TO JUNE 30, 2023

OVERVIEW OF OPERATIONS

Company Background

LastPass is a password manager which helps millions of registered users organize and protect their online lives. For more than 100,000 businesses of all sizes, LastPass provides password and identity management solutions that are convenient, easy to manage and effortless to use. From enterprise password management and single sign-on to adaptive multi-factor authentication, LastPass for Business gives superior control to IT and frictionless access to users.

LastPass is headquartered in Boston, Massachusetts with additional locations in North America, South America, Europe, and Australia.

On August 31, 2020, GoTo Group, Inc. (formerly known as “LogMeIn, Inc.,” and referred to herein as “GoTo”) was acquired by affiliates of Francisco Partners and Evergreen Coast Capital Corp. in a take-private transaction. In December 2021, GoTo announced its intention to establish LastPass as a separate, standalone company. On December 31, 2021, GoTo completed an internal reorganization whereby its LastPass and GoTo businesses were separated into two distinct subsidiary structures under a common ownership group. As of January 1, 2023, LastPass operates as its own company. However, the process of separating LastPass’ technology and infrastructure from GoTo is ongoing and is expected to be complete in the third quarter of 2023.

Description of Services Provided

LastPass provides individuals and businesses with a password management solution designed to removed everyday password-related friction. This includes generating, storing, managing, and monitoring users' most sensitive credentials. The service 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 multi-factor authentication option for streamlined access and authentication.

LastPass offered in free, premium, and enterprise versions with the option for additional advanced add-on features such as single sign-on and multi-factor authentication, and is available online, in a desktop application, and via iOS and Android mobile apps.

Principal Service Commitments and System Requirements

The company designs its processes and procedures to meet the objectives for the LastPass Services 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 our technical and organizational security measures (e.g., as located in the “Technical and Organizational Measures” (TOMs) documentation found at LastPass Trust 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 and/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
- https://www.lastpass.com/trust-center
- As well as in the description of services provided online

Components of the System

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

- AWS
- Azure
- Switch

Our data center and cloud service providers maintain both International Organization for Standardization (ISO) 27001 compliance and have current SOC 1 or SOC 2 reports which indicate compliance with the AICPA's Trust Services Criteria.

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

LastPass' 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 LastPass Security and Information Technology (IT) teams manage the configuration of corporate firewalls, network system security, and endpoint devices (desktops, laptops and mobile devices).

Software

The LastPass Services System is developed by the software development staff and runs on shared multi-tier architectures with network segmentation and server role assignments. The hardware and software components of the infrastructure supporting the LastPass Services System include:

Primary Software		
#	**Component**	**Description**
1	Server Hardware	Virtualized cloud hardware, Infrastructure as a Service (IaaS), and LastPass-owned physical servers
2	Operating systems	LastPass uses macOS, Windows, and Linux
3	Databases	A variety of databases and database tools are used to store user account information, summary data, logs, etc.
4	Monitoring systems	There are multiple monitoring systems in use, including but not limited to: • Security Incident and Event Management (SIEM) • Amazon and Azure platform monitoring for each respective cloud provider • System and performance monitoring • System server logs, error logs, and security audit trails • Advanced Endpoint Protection (AEP) technology • Threat intelligence monitoring

Primary Software		
#	**Component**	**Description**
5	Network infrastructure	The network infrastructure uses a common set of redundant network components: • Load balancers • Advanced Firewalls • Gateways (NAT, Internet) • Virtual Private Clouds (VPCs), subnets, routing tables • Network Access Control Lists (NACLs) and whitelisting • Network intrusion detection system
6	Key Supporting Tools, Processes, and Applications	The other significant application programs and IT system software that support application programs include: • Secure Development Lifecycle, including automated application security assessment tools and composition analysis • Change Management through ticketing and workflow management • Vulnerability management • Identity and Access Management Tools - Azure AD and SailPoint IdentityNow • Backup tools • Physical security and safety controls • Database security controls, including access control, encryption, and logging • Personnel security measures • 24/7 security incident monitoring and response • Security and privacy awareness training • Offensive security testing and remediation • Governance and risk management

People

Corporate Leadership

Management of LastPass is the responsibility of the Chief Executive Officer (CEO). The Executive Leadership Team responsible for daily operations includes the following:

- Chief Secure Technology Officer (CSTO)
- Chief Financial Officer (CFO)
- Senior Vice President (SVP), Customer Experience
- SVP, Human Resources (HR)
- SVP, Operations
- Chief Marketing Officer (CMO)
- Chief Revenue Officer (CRO)
- SVP, Product Management
- SVP, General Counsel, Legal

There are other departments within the organization which are relevant to the appropriate functioning of LastPass and its Information Security Management system:

- Product Management (PM) and User Experience (UX). The PM and UX functions are responsible for involvement in defining LastPass' product strategy, product roadmap and the end-to-end user experience (e.g., user interactions/usability, visual design, etc.) for LastPass products. PM and UX Teams define and prioritize specific requirements and collaborate with Product Development Teams for implementation. The PM and the UX functions report up to the SVP, Product Management.
- Customer Care. The Customer Care function includes horizontal customer support functions and customer success teams. This function is responsible for managing customer issues, satisfaction, and efforts to support retention and growth. Customer Care leadership reports to the SVP, Customer Experience.
- Finance. The Finance Department maintains the finances of the business through functions such as accounting, purchasing, planning, and analysis. Finance leadership reports directly to the CFO.

Data

Data Classification and Handling

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. Specifically, this electronic information, defined as Content in the LastPass Terms of Service (ToS), includes any files, documents, recordings, chat logs, transcripts, and similar data that LastPass maintains on behalf of its customers and their end-users, as well as any other information a LastPass customer may upload to their service account in connection with the LastPass services (referred to as Customer Content herein). 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, which may be found either on the applicable product-specific resource web pages and/or the TOMs documentation located on the LastPass Trust & Privacy Center web pages under Product Resources. This information is subject to the confidentiality controls in this report. Specifically, Customer Content shall be safeguarded through the implementation and use of administrative, technical, and physical measures designed to ensure its security, integrity, and availability. Customer Content shall be returned or deleted in accordance with the Retention, Archiving, and Disposal sections below.

Additionally, LastPass' Information Classification scheme describes pre-defined controls necessary to safeguard data in accordance with a sensitivity classification. Customer Content is considered confidential data and is protected according to relevant data protection controls, policies, and/or procedures.

Furthermore, connections to production applications and networks over the Internet or other public networks are encrypted. Appropriate network application safeguards are implemented to secure connections internally between production data centers. To the extent reasonable, Data Loss Prevention (DLP) software is used on corporate systems in order to reduce the likelihood that sensitive data is transported outside of the corporate network.

Retention, Archiving, and Disposal

LastPass reviews data retention and disposal policies and procedures on an ongoing basis to ensure compliance with applicable requirements. LastPass 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 & Privacy Center. When disposing of electronic data storage devices, LastPass evaluates against industry-standard practices and internal controls to determine the appropriate approach to ensure that data destruction is irreversible. When hard drives holding Customer Content are retired, they are wiped using appropriate software and/or discs are rendered unreadable and destroyed based on industry-standard practices and internal controls. Secure shred bins are located in every office and on every floor to enable appropriate and secure disposal of data that is determined to be of a sensitive nature (e.g., pertaining to LastPass customers).

Processes, Policies and Procedures

LastPass 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. LastPass 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.

Physical Security

LastPass has a physical security program in place which is designed to provide access control to global locations. The entrances to LastPass premises with network connections are secured using a transponder/badge system managed by the Facilities Team. Facilities and HR personnel manage the assignment and collection of access badges to each facility. New hires are granted access to applicable buildings as necessary for their role. Visitors at LastPass offices worldwide are required to check in at a reception desk, sign into a visitor management system, and be escorted by LastPass personnel. Where applicable, security guards are located on-site in multi-tenant buildings.

Environmental protections have been implemented in the data centers that house production servers (LastPass production data centers) and include the following control systems, as appropriate for the relevant system:

- Heating, ventilation, and air conditioning temperature control
- Fire suppression
- Uninterruptible power supply
- Smoke detectors
- Raised floors or comprehensive cable management

LastPass contracts with subservice organizations, such as co-location data center facilities, to provide physical security and environmental controls for the LastPass production data centers. GIS management regularly reviews access reports and logs for authorized and unauthorized access and failed access attempts. LastPass additionally has the ability to run access reports, on an ongoing and as-needed basis, through select data center portals.

Access to production data centers is limited to authorized LastPass personnel. Operations management reviews access logs for third-party hosting facilities, on no less than a quarterly basis, to verify that access was limited to only authorized individuals. A formal request process is designed to authorize and monitor access to physical data centers and is to be approved by GIS.

Access to any third-party hosting facilities requires submission of a request through a ticketing system and is to be approved by the management of Corporate IT and/or GIS. Access to on-premise server rooms is granted, if deemed appropriate, based on an individual's role. If an individual needs subsequent access, a ticket or e-mail is to be submitted to the Facilities Team with appropriate management approval and justification.

Upon termination, an automated process is executed between the HR resource management system and Corporate Active Directory (Corp AD) to terminate Corp AD access automatically in accordance with the termination date and time specified by HR. Additionally, a termination notification is automatically generated through a distribution list and is sent to system administrators for further processing and verification of access to subsequent systems. The corporate facilities security management system integrates with Corp AD and the terminated individual's badge is automatically disabled at office locations and on-premise server rooms. Access to subservice hosting provider locations is disabled by the GIS Team, upon notice.

Logical Access

Logical 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. Employees' 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. Minimum permissible password requirements follow industry-standard best practices.

LastPass employs internal tools and controls designed to manage and limit access to corporate applications containing or accessing sensitive or critical data sources. Authorized access to the corporate, application, and production environments is controlled using multi-tier authorizations, which are maintained in a central ticketing system for approval and tracking. Employee access to specified resources requires direct manager or HR approval and, in specific cases, application/data source owner approval. Employee application and data source access lists are reviewed, on at least a quarterly basis, in order to verify that current access levels for employees are authorized and appropriate for their position and that access is revoked promptly upon termination.

Logical access control policies and/or procedures, including the Information Security Policy and the Security Standard, are designed to prevent or mitigate unauthorized application access and data loss. GIS, IT, the Development Tools Team and software development management follow a set of policies and/or procedures to ensure that access to technical infrastructure is properly restricted to authorized personnel. Remote access to the Virtual Private Network (VPN) uses two-factor authentication. Two-factor authentication is also used when providing access to systems that are federated with AD, either internally or externally.

LastPass production servers are maintained in a separate environment from the Corporate IT environment. GIS management, product engineering, product DevOps, and engineering support functions review logical access to the production environment, on no less than a quarterly basis, to ensure that no unauthorized accounts have been added. When employee terminations are entered into the HR system, revocation of logical access to the corporate environment is processed through an automated job that disables access based on a specified date and time corresponding to the conclusion of employment. For applications dependent upon Corp AD, termination of the Corp AD account will effectively disable authentication for the application account.

Employee terminations are processed through a formal off-boarding process in which equipment, facility access cards, and logical access to critical systems are disabled by the termination date. Once an employee termination has been processed by HR, a termination ticket is created, and an automated termination notification is sent to the applicable departments to remove systems/physical access. This occurs through both automated and/or manual processes, contingent upon the level and type of access.

Computer Operations - Backups

Databases are backed up using automated backup strategies intended to allow for multiple copies to be available at any one time. Particular backup methods will vary and be dependent upon the types of databases used to support the specified product. In the event of a disaster or total site failure in any one of multiple active hosting locations, remaining locations are designed to balance application load. For more information on the supporting architectures for the individual products, please refer to the technical white papers and other reference documentation under the product-specific “Resources” web pages and the product or suite-specific LastPass Product Resources page available on the LastPass Trust & Privacy Center.

Failed backups are monitored and manually re-run, if determined necessary, and tracked to completion. Specific backup methodology may also be expanded upon in the relevant TOM documentation located in the LastPass Product Resources section of the LastPass Trust & Privacy Center. Access to stored backup media is restricted to authorized personnel based upon job responsibilities.

Computer Operations - Availability

LastPass has an Incident Response Plan designed to manage, identify, and resolve suspected security incidents. Procedures are implemented so that information security-related events and vulnerabilities are identified by technical personnel and escalated to management when deemed appropriate. The Incident Response Plan includes a process developed for employees to report incidents. Specific instructions are located on LastPass Intranet.

Critical components of the Security Incident Response Plan, which is aligned with the Critical Communication Playbook, include the Information Security Incident Management Policy and Standard Operating Procedures. Incidents are documented and escalated via a ticketing system and triaged based upon criticality. Incidents can be reported globally via ticket, e-mail, and phone call using international phone numbers.

Change Control

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.

Additional governing policies and/or procedures are in place to address the following:

- Implementation support for new customers
- Technical support and communication with customers
- Business continuity and disaster recovery
- Incident management

Changes to the LastPass Services System may be initiated by either a customer request or internal business decision. The proposed change request is entered into a ticketing system and appropriately prioritized. Changes are reviewed and approved by the product engineering teams, including the product owner.

Changes are approved and tested in a staging environment that exists separately from the production environment. Regression, manual, and/or automated testing is performed in a Quality Assurance (QA)/staging environment prior to being released into production. If testing is successful, changes are reviewed and approved for final release. Production servers are patched with supported operating system updates, as needed. Patching activity is, depending on the specific environment, performed by either GIS or DevOps. Material changes that can impact customers (e.g., new features, bug fixes, etc.) may be communicated on the relevant LastPass service website. Select product websites provide the option for customers to subscribe to service notifications and alerts via e-mail, text, and/or social media accounts.

Changes to policies and procedures are reviewed and approved by the Chief Information Security Officer (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.

Data Communications

Vulnerability management programs is incorporated into production and Corporate IT environments, which include both internal and external network system scanning, dynamic code analysis, and application-level penetration testing that is performed internally and externally by qualified third-parties. Significant or critical issues discovered through such programs are reported to leadership and stakeholders for appropriate prioritization. Events and vulnerabilities may be identified through staff and customer reports, security notification channels (public or private bug bounty programs), quarterly internal and external vulnerability scanning, application vulnerability testing, and penetration testing activities for targeted environments. External and internal vulnerability scans are performed on the network and the production environment at least quarterly. These scanning results are reported into network monitoring tools.

Corporate IT and production environment security is monitored using multiple industry-standard technologies, and relevant incidents are reported to the Security Operations Center (SOC). Once alerts or reports are analyzed, the SOC collaborates with relevant stakeholders to resolve identified issues -reporting and analysis are tracked and documented for management review. Resolutions are tracked through a ticketing system.

Intrusion Detection

Intrusion Protection Systems (IPS) are used in the Corporate IT network and specific LastPass production environments using multiple industry-standard tools. Corporate IT, GIS, and product engineering are automatically notified of discovered intrusion attempts against the network, and issues are addressed and resolved in accordance with criticality and risk. Suspicious server login activity is monitored by the SOC, and relevant identified issues are researched, documented, and resolved.

Firewalls are deployed on the Corporate IT network and production environments, and access to modify firewall settings is restricted to authorized IT and GIS personnel. On no less than an annual basis, firewall configuration reviews are performed.

Boundaries of the System

This description of the LastPass Services 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 the LastPass Services System operation(s). Compliance with laws and regulations for privacy, export or similar requirements are not included in the scope of this description.

This report does not include the cloud hosting services provided by AWS, Azure, and Switch.

Changes to the System in the Last 12 Months

During the period of September 1, 2022 to June 30, 2023, the following changes occurred to LastPass and the applicable LastPass Services System used to provide services, which should not impact the ability to meet the tested controls and criteria of this report:

In January of 2023, LastPass became an independent company from GoTo. As part of the separation process, LastPass has a shared services agreement with LastPass that allows for their usage of technical infrastructure (and associated change management, monitoring and incident response services) and physical offices.

Incidents in the Last 12 Months

In August 2022, the Company disclosed that a threat actor had gained access to a development environment and stole portions of source code, technical information, and certain internal company secrets. The Company later determined that the threat actor was able to leverage information obtained from this initial attack to launch a coordinated second attack which targeted the home network of a senior employee who had access to highly privileged credentials across the cloud-based infrastructure shared by LastPass and GoTo. The threat actor was able to first target the employee's home computer by exploiting a vulnerable third-party application which enabled the threat actor to remotely implant keylogger malware, bypass existing controls, and eventually capture the employee's privileged credentials needed to gain access to a cloud-based storage environment used by both LastPass and GoTo to store production backups. From there, the threat actor was able to access, decrypt and exfiltrate both encrypted and unencrypted data from within the cloud-based storage service (the "2022 Security Incident"). The Company has since completed its investigation and disclosed its findings in a March 2023 blog post (https://blog.lastpass.com/2023/03/security-incident-update-recommended-actions/).

Following the 2022 Security Incident, the company has deployed several new security technologies across its infrastructure, data centers, and cloud estates designed to further bolster its security and enhance existing monitoring capabilities in order to help detect and prevent any further threat actor activity.

Criteria Not Applicable to the System

All Common/Security, Availability, and Confidentiality criterion was applicable to LastPass' LastPass Services System.

Subservice Organizations

This report does not include the cloud hosting services provided by AWS, Azure, and Switch.

Subservice Description of Services

Cloud hosting services are provided by AWS, Azure, and Switch at various global locations.

Complementary Subservice Organization 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.

The following subservice organization controls have been implemented by AWS, Azure, and Switch and are not included in this report to provide additional assurance that the Trust Services Criteria are met:

Subservice Organization - AWS, Azure, and Switch		
Category	**Criteria**	**Control**
Common Criteria / Security	CC6.1, CC6.2, CC6.3	Policies and other relevant system documentation communicate descriptions of responsibilities and expected behavior with regard to system usage.
		Account creation and modifications are authorized by management and documented in a ticketing system.
		Production network, database server, and application server user access is revoked in a timely manner upon termination.
		Industry standard encryption algorithms are used to remotely manage production infrastructure.
		Appropriate identification and authentication are required to perform actions on the production infrastructure.
		Production network and server user accounts are reviewed by management on a quarterly basis. Suspicious accounts are investigated and resolved.
	CC6.4	Physical access to server rooms and secured areas within production data centers is granted based on management authorization.
		Physical access to server rooms and secured areas within production data centers is revoked upon termination.
		Physical access to server rooms and secured areas within production data centers is reviewed by management on a quarterly basis.
		Relevant identified issues are investigated and resolved.
	CC6.6, CC6.7	Industry standard encryption algorithms are used to remotely manage production infrastructure.
		Remote access to the corporate network is restricted through managed VPN concentrators.
		Approved networking ports and protocols are implemented in accordance with documented production network standards.
	CC8.1	Application changes are documented and tracked in an internal ticketing system.
		Application releases into production do not occur until appropriate signoffs are obtained and documented.
		Changes to infrastructure components are subject to peer review and/or approval by management.

Subservice Organization - AWS, Azure, and Switch		
Category	**Criteria**	**Control**
Availability	A1.2	Environmental protections have been implemented for LastPass designated spaces, including, as appropriate: • Fire suppression • Smoke detectors • Raised floors • Closed-circuit television (CCTV) monitoring • Locked entrances
Confidentiality	C1.1	The entity has processes and tools designed to ensure that confidential information will not be transmitted beyond the boundaries of the system unless otherwise authorized or provided to unauthorized user entity personnel.
		The entity establishes written policies related to retention periods for relevant confidential information it maintains. The entity, as applicable: has automated system processes in place to delete confidential information in accordance with specific retention requirements.
		The entity deletes backup information in accordance with a defined schedule.
		The entity requires approval for access to confidential information.
		The entity classifies information to be retained beyond its retention period and specifically marks such information for retention.
		The entity reviews information marked for retention annually.
	C1.2	The entity locates and removes or redacts specified confidential information as required.
		The entity regularly and systematically destroys, erases, or makes anonymous specified confidential information that is no longer required for the purposes identified in its confidentiality commitments or system requirements.
		The entity erases or destroys specified records in accordance with applicable retention policies, regardless of the method of storage (for example, electronic, optical media, or paper based).
		The entity disposes of original, archived, backup, and ad hoc or personal copies of records in accordance with applicable destruction policies documents the disposal of confidential information.

LastPass management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, LastPass performs monitoring of the subservice organization controls, including holding periodic discussions with vendors and subservice organizations.

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.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

Controls expected to be implemented at user entity organizations	Complemented Criteria Ref. Number
User entities are responsible for notifying LastPass of product issues, problems, or actual or suspected incidents detected in their environments for resolution.	CC2.2, CC2.3
User entities are responsible for notifying LastPass of any specific security, availability, or confidentiality related requirements.	CC2.2, CC2.3
User entities are responsible for ensuring that their employees comply with customer-related policies and procedures when using workstations or terminals that may be used to access LastPass products.	CC6
User entities are responsible for notifying LastPass of application unavailability or inaccessibility from their customer environment and whether any downtime affects the terms of use.	CC2.3, A1.2
User entities are responsible for using LastPass products based on their intended purpose, as specified in the relevant terms of service (or agreement for LastPass services), and in compliance with applicable laws, regulations, and policies.	CC1.3, CC2.2
User entities are responsible for periodically checking LastPass managed user entity support channels, forums, articles, community pages, and/or knowledgebases for release and upgrade information.	CC2.2
User entities are responsible for implementing physical access security controls over their own environments and any workstations that the user entity may use to access LastPass products.	CC6.4
User entities are responsible for configuring application password settings in accordance with their own policies and procedures as each system permits.	CC6.1, CC6.2
User entities are responsible for implementing secure user authentication credentials, including individual user IDs and passwords, when setting up and managing account access to in-scope systems.	CC6.1, CC6.2
User entities are required to securely store authentication credentials. These include but are not limited to: User Account IDs, Passwords, or other access control, encryption, and security measures. LastPass will provide a means for resetting passwords.	CC6.1, CC6.2
User entities are responsible for ensuring that user (employee) data is kept private, secured adequately, and maintained appropriately for accuracy and completeness, including the timely removal of user accounts as required.	CC6.3, C1.1, C1.2

Controls expected to be implemented at user entity organizations	Complemented Criteria Ref. Number
User entities are responsible for communicating user (employee) responsibilities regarding the use of the system.	CC2.2