Lob.com, Inc.
Type 2 SOC 3
2020

SOC 3 FOR SERVICE ORGANIZATIONS REPORT

June 15, 2020 To September 15, 2020

Table of Contents

SECTION 1

ASSERTION OF LOB.COM, INC. MANAGEMENT

ASSERTION OF LOB.COM, INC. MANAGEMENT

October 15, 2020

We are responsible for designing, implementing, operating, and maintaining effective controls within Lob.com, Inc.'s ('Lob' or 'the Company') Print and Mail and Address Verification Automation Software Services System throughout the period June 15, 2020 to September 15, 2020, to provide reasonable assurance that Lob's service commitments and system requirements relevant to Security (applicable trust services criteria) were achieved. Our description of the boundaries of the system is presented below in "Lob.com, Inc.'s Description of Its Print and Mail and Address Verification Automation Software Services System Throughout The Period June 15, 2020 To September 15, 2020" 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 June 15, 2020 to September 15, 2020, to provide reasonable assurance that Lob's service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Confidentiality, Processing Integrity and Privacy* (AICPA, *Trust Services Criteria*). Lob's objectives for the system in applying 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 "Lob.com, Inc.'s Description of Its Print and Mail and Address Verification Automation Software Services System Throughout The Period June 15, 2020 To September 15, 2020".

Lob uses Amazon Web Services, Inc. ('AWS' or 'subservice organization') 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 Lob, to achieve Lob's service commitments and system requirements based on the applicable trust services criteria. The description presents Lob's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Lob's controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary to achieve Lob'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 Lob'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 June 15, 2020 to September 15, 2020 to provide reasonable assurance that Lob's service commitments and system requirements were achieved based on the applicable trust services criteria.

Paul Senechko
Director of Engineering
Lob.com, Inc.

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Lob.com, Inc.

Scope

We have examined Lob's accompanying description of Print and Mail and Address Verification Automation Software Services System titled "Lob.com, Inc.'s Description of Its Print and Mail and Address Verification Automation Software Services System Throughout The Period June 15, 2020 To September 15, 2020" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period June 15, 2020 to September 15, 2020, to provide reasonable assurance that Lob's service commitments and system requirements were achieved based on the trust services criteria relevant to Security (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*).

Lob uses AWS 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 Lob, to achieve Lob's service commitments and system requirements based on the applicable trust services criteria. The description presents Lob's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Lob's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, 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 Lob, to achieve Lob's service commitments and system requirements based on the applicable trust services criteria. The description presents Lob's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Lob'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

Lob 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 Lob's service commitments and system requirements were achieved. Lob has provided the accompanying assertion titled "Assertion of Lob.com, Inc. Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. Lob is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. 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, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- 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 the description is presented in accordance with the description criteria
- 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
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Evaluating the overall presentation of the description

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 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 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 Lob's Print and Mail and Address Verification Automation Software Services System were suitably designed and operating effectively throughout the period June 15, 2020 to September 15, 2020, to provide reasonable assurance that Lob's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

The SOC logo for Service Organizations on Lob'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 Lob, user entities of Lob's Print and Mail and Address Verification Automation Software Services System during some or all of the period June 15, 2020 to September 15, 2020, business partners of Lob subject to risks arising from interactions with the Print and Mail and Address Verification Automation Software Services System, and those who have sufficient knowledge and understanding of the complementary user entity controls and complementary subservice organization 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.

A-LIGN ASSURANCE

Tampa, Florida
October 15, 2020

SECTION 3

LOB.COM, INC.'S DESCRIPTON OF ITS PRINT AND MAIL AND ADDRESS VERIFICATION AUTOMATION SOFTWARE SERVICES SYSTEM THROUGHOUT THE PERIOD JUNE 15, 2020 TO SEPTEMBER 15, 2020

OVERVIEW OF OPERATIONS

Company Background

Lob uses cloud software to help businesses send smarter mail, faster through automation. Since launching in 2015, more than 7,000 companies have trusted Lob's Application Programming Interfaces ('APIs') to send mail and create new growth opportunities.

The organization is headquartered in San Francisco, California, with a Global Print Delivery Network all over the world.

Description of Services Provided

Lob provides two primary services: Print & Mail APIs and Address Verification APIs.

The Print & Mail API allows users to programmatically send postcards, letters, and checks. With a single API request, users can send a custom Hypertext Markup Language ('HTML') page (or image/pdf), which Lob will render and transmit to the Global Print Delivery Network. The print partner will physically print the mail piece and hand it off to the local mail carrier (United States Postal Service ('USPS') in the United States ('US'), Royal Post in the UK, etc.). Along the way Lob will receive events about the mail piece status such as when it gets handed off to the carrier, when the carrier scans the mail piece in different cities' delivery hubs, etc. For each of these delivery events the system will send a webhook with the full details, allowing the customer to track their mail piece from start to finish if the customer has subscribed to receiving webhook events.

The Address Verification APIs allow users to cleanse, enrich, and geocode address information. It's a fast, performant, and easy way for address autocomplete forms, looking up the latitude and longitude of addresses, verifying address deliverability as determined by the local mail carrier, etc., and can be used for both US and international addresses.

Principal Service Commitments and System Requirements

Lob designs its processes and procedures related to its APIs to meet its objectives for its Print & Mail services. Those objectives are based on the service commitments that Lob makes to user entities, the laws and regulations that govern the provision of Print & Mail services, and the financial, operational, and compliance requirements that Lob has established for the services. The Print & Mail services of Lob are subject to the security and privacy requirements of the Health Insurance Portability and Accountability Act Administrative Simplification, as amended and where applicable clients with Business Associate Agreements ('BAAs'), as well as state privacy security laws and regulations in the jurisdictions in which Lob operates.

Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of the Print & Mail API that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role
- Use of encryption technologies to protect customer data both at rest and in transit

Lob establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Lob's system policies and procedures, system design documentation, and contracts with customers. Lob ensures contracts with its print partners outline security, compliance and data handling requirements.

Components of the System

Infrastructure

Primary infrastructure used to provide Lob's Print and Mail and Address Verification Automation Software Services System includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Web Servers	AWS c5.4xlarge	Hosts files to support the web application, background jobs, and other functions necessary for services
Load Balancers	AWS Application Load Balancer ('ALB')	Load balances traffic across servers
Databases	AWS db.m5.12xlarge	Hosts application data

Software

Primary software used to provide Lob's Print and Mail and Address Verification Automation Software Services System includes the following:

Primary Infrastructure		
Software	**Operating System**	**Purpose**
NodeJS, Golang, Elixir	Linux	Runs application code
AWS Elastic Container Services ('ECS')	Linux	Runs all containerized services, handles deployments and load balancing, auto-scaling, logging, etc.
Okta	Not applicable	Secure identity management
1Password	Not applicable	Password manager/vault
Red Canary	Not applicable	Endpoint protection and threat detection
Cloudsploit	Not applicable	Automated security and configuration monitoring tool

People

Lob has a staff of 105 employees organized in the following functional areas:

- Product and Engineering: Builds product roadmap and feature set, drives all the engineering and infrastructure work, builds integrations with print partners and mail carriers and generally maintains Lob's services
- Customer Experience and Customer Success: Manages any support issues customers have
- People: Runs Human Resources ('HR') and Recruiting functions. Manages benefits, employee development, recruiting, and other programs
- Partner Operations: Manages the print partner network and onboarding new print partners
- Finance: The finance team manages finance and accounting functions
- Sales & Marketing: The sales team works on closing inbound and outbound deals, and the marketing team works on brand awareness and building inbound deals pipeline

Data

To send Print & Mail documents, customers need to pass at a minimum:

- Recipient name
- Recipient mailing address
- Sender's mailing address (only for letters; optional for postcards)
- Content of mailings

When sending checks Lob would also receive:

- Sender bank account and routing numbers
- Memo line and amount
- Sender and recipient mailing address
- Optional content of mailings

When sending postcards, the entire mail content is publicly viewable and would likely be marketing material.

When sending letters or checks, the mail content is entirely up to the customer. Customers can send marketing mail which contains non-Personally Identifiable Information ('PII') data, or operational and transaction mail which contains data specific for that end user (i.e. bills, medical statements, insurance documents, legal documents, etc.).

Processes, Policies and Procedures

Formal Information Technology ('IT') policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. All teams are expected to adhere to the Lob policies and procedures that define how services should be delivered. These are located on Lob's intranet and can be accessed by any Lob team member.

Physical Security

The in-scope system and supporting infrastructure is hosted by AWS. As such, AWS is responsible for the physical security controls for the in-scope system.

Logical Access

Lob uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. Resources are protected through the use of native system security and add-on software products that identify and authenticate users and validate access requests against the users' authorized roles.

Employees and approved vendor personnel sign on to the Lob network using federated access via an identity and access management system requiring two-factor authentication. Passwords must conform to defined password standards and are enforced through parameter settings when available.

Customer employees access Print & Mail services through the Internet using the Transport Layer Security ('TLS') functionality of their web-browser. These customer employees must supply a valid user ID and password to gain access to customer cloud resources. Passwords must conform to password configuration requirements configured on the virtual devices using the virtual server administration account. Virtual devices are initially configured in accordance with Lob's configuration standards, but these configuration parameters may be changed by the virtual server administration account.

Computer Operations - Backups

Customer data is backed up and monitored every 24 hours by operations personnel for completion and exceptions. In the event of an exception, operations personnel perform troubleshooting to identify the root cause and then re-run the backup job immediately or as part of the next scheduled backup job depending on customer indicated preference within the documented work instructions.

Computer Operations - Availability

Incident response policies and procedures are in place to guide personnel in reporting and responding to information technology incidents. Procedures exist to identify, report, and act upon system security breaches and other incidents. Incident response procedures are in place to identify and respond to incidents on the network.

Lob monitors the capacity utilization of physical and computing infrastructure both internally and for customers to ensure that service delivery matches SLA. Lob evaluates the need for additional infrastructure capacity in response to growth of existing customers and/or the addition of new customers. Infrastructure capacity monitoring includes, but is not limited to, the following infrastructure:

- Disk storage
- Network bandwidth
- API capacity
- Print partner capacity

Lob has implemented a patch management process to ensure systems are patched in accordance with vendor recommended operating system patches. Customers and Lob system owners review proposed operating system patches to determine whether the patches are applied. Customers and Lob systems are responsible for determining the risk of applying or not applying patches based upon the security and availability impact of those systems and any critical applications hosted on them. Lob staff validate that all patches have been installed and if applicable that reboots have been completed.

Change Control

Lob maintains documented Systems Development Life Cycle ('SDLC') policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality assurance testing and User Acceptance Testing ('UAT') results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

Data Communications

Firewall systems are in place to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized. Network Address Translation ('NAT') functionality is utilized to manage internal Internet Protocol ('IP') addresses. Administrative access to the firewall is restricted to authorized employees.

Redundancy is built into the system infrastructure supporting the data center services to help ensure that there is no single point of failure. In the event that a primary system fails, the redundant hardware is configured to take its place.

Lob has a bug bounty program allowing security researchers to test Lob's platform and report vulnerabilities responsibly. Vulnerabilities are investigated, triaged, and remediated in a timely manner.

Vulnerability scanning is performed by a third-party vendor on a continuous 6-hour basis in accordance with Lob policy. The third-party vendor uses industry standard scanning technologies and a formal methodology specified by Lob. These technologies are customized to test the organization's infrastructure and software in an efficient manner while minimizing the potential risks associated with active scanning. Retests and on-demand scans are performed on an as needed basis.

Boundaries of the System

The scope of this report includes the Lob Print and Mail and Address Verification Automation Software Services System performed in the San Francisco, California facility.

This report does not include the Cloud Hosting Services provided by AWS at multiple facilities.

Changes to the System Since the Last Review

No significant changes have occurred to the services provided to user entities since the organization's last review.

Incident Since the Last Review

No significant incidents have occurred to the services provided to user entities since the organization's last review.

Criteria Not Applicable to the System

All Common Criterion/Security was applicable to the Lob Print and Mail and Address Verification Automation Software Services System.

Subservice Organizations

This report does not include the cloud hosting services provided by AWS at multiple facilities.

Subservice Description of Services

AWS provides cloud hosting services, which includes implementing physical security controls to protect the housed in-scope systems. Controls include, but are not limited to, visitor sign-ins, required use of badges for authorized personnel, and monitoring and logging of the physical access to the facilities.

Complementary Subservice Organization Controls

Lob 's services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to Lob 's services to be solely achieved by Lob control procedures. Accordingly, the subservice organization, in conjunction with the services, should establish their own internal controls or procedures to complement those of Lob.

The following subservice organization controls should be implemented by AWS to provide additional assurance that the trust services criteria described within this report are met:

Subservice Organization - AWS		
Category	**Criteria**	**Control**
Common Criteria/Security	CC6.1 CC6.6 CC6.7	Key Management Services ('KMS')-Specific - The key provided by KMS to integrated services is a 256-bit key and is encrypted with a 256-bit AES master key unique to the customer's AWS account.
	CC6.4 CC7.2	Physical access to data centers is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
		Physical access points to server locations are recorded by closed circuit television camera ('CCTV'). Images are retained for 90 days, unless limited by legal or contractual obligations.
		Physical access points to server locations are managed by electronic access control devices.
		Electronic intrusion detection systems ('IDS') are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.
		Key Management Service ('KMS')-Specific - Recovery key materials used for disaster recovery processes by KMS are physically secured offline so that no single AWS employee can gain access to the key material.
		KMS-Specific - Access attempts to recovery key materials are reviewed by authorized operators on a cadence defined in team processes.
	CC6.7 CC7.5	RDS-Specific - If enabled by the customer, RDS backs up customer databases, stores backups for user-defined retention periods, and supports point-in-time recovery.
		Critical AWS system components are replicated across multiple Availability Zones and backups are maintained.
		Backups of critical AWS system components are monitored for successful replication across multiple Availability Zones.

Lob 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 SLA. In addition, Lob performs monitoring of the subservice organization controls, including the following procedures:

- Reviewing attestation reports over services provided by vendors and subservice organization
- Monitoring external communications, such as customer complaints relevant to the services provided by the subservice organization

COMPLEMENTARY USER ENTITY CONTROLS

Lob's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the Trust Services Criteria related to Lob's services to be solely achieved by Lob control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Lob's.

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.

1. User entities are responsible for understanding and complying with their contractual obligations to Lob.
2. User entities are responsible for notifying Lob of changes made to technical or administrative contact information.
3. User entities are responsible for ensuring the completeness and accuracy of data entered into Lob.
4. User entities are responsible for maintaining their own system(s) of record.
5. User entities are responsible for ensuring the supervision, management, and control of the use of Lob services by their personnel.
6. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Lob services.
7. User entities are responsible for immediately notifying Lob of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.