Lob, Inc.
Type 1 SOC 2
2019

REPORT ON LOB, INC.'S DESCRIPTION OF ITS SYSTEM AND ON THE SUITABILITY OF THE DESIGN OF ITS CONTROLS RELEVANT TO SECURITY

Pursuant to Reporting on System and Organization Controls 2 (SOC 2)
Type 1 examination performed under AT-C 105 and AT-C 205

July 30, 2019

Table of Contents

SECTION 1

ASSERTION OF LOB, INC. MANAGEMENT

ASSERTION OF LOB, INC. MANAGEMENT

August 19, 2019

We have prepared the accompanying description of Lob, Inc.'s ('Lob' or 'the Company') Print & Mail and Address Verification Automation Software services system titled "Lob, Inc.'s Description of Its Print & Mail and Address Verification Automation Software services system as of July 30, 2019" (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). The description is intended to provide report users with information about the Print & Mail and Address Verification Automation Software services system that may be useful when assessing the risks arising from interactions with Lob's system, particularly information about system controls that Lob has designed, implemented, and operated to provide reasonable assurance that its 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 Amazon Web Services ('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 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.

We confirm, to the best of our knowledge and belief, that

a. the description presents Lob's Print & Mail and Address Verification Automation Software services system that was designed and implemented as of July 30, 2019, in accordance with the description criteria.
b. the controls stated in the description were suitably designed as of July 30, 2019, to provide reasonable assurance that Lob's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of that date, and if the subservice organization and user entities applied the complementary controls assumed in the design of Lob's controls as of that date.

Arkadiy Tetelman

Arkadiy Tetelman
Application Security Engineer
Lob, Inc.

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Lob, Inc.

Scope

We have examined Lob's accompanying description of its Print & Mail and Address Verification Automation Software services system titled "Lob, Inc.'s Description of Its Print & Mail and Address Verification Automation Software Services System as of July 30, 2019" (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 of controls stated in the description as of July 30, 2019, 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, Inc. Management" (assertion) about the description and the suitability of the design 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 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 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 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
- 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 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 report users may consider important to meet their informational needs.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. The projection to the future of any conclusions about the suitability of the design 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.

Other Matter

We did not perform any procedures regarding the operating effectiveness of controls stated in the description and, accordingly, do not express an opinion thereon.

Opinion

In our opinion, in all material respects,

a. the description presents Lob's Print & Mail and Address Verification Automation Software Services System that was designed and implemented as of July 30, 2019, in accordance with the description criteria.
b. the controls stated in the description were suitably designed as of July 30, 2019, to provide reasonable assurance that Lob's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of that date and if the subservice organization and user entities applied the complementary controls assumed in the design of Lob's controls as of that date.

Restricted Use

This report is intended solely for the information and use of Lob, user entities of Lob's Print & Mail and Address Verification Automation Software Services System as of July 30, 2019, business partners of Lob subject to risks arising from interactions with the Print & Mail and Address Verification Automation Software Services System, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties

- Internal control and its limitations
- 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
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

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

A-LIGN ASSURANCE

Tampa, Florida
August 19, 2019

SECTION 3

LOB, INC.'S DESCRIPTION OF ITS PRINT & MAIL AND ADDRESS VERIFICATION AUTOMATION SOFTWARE SERVICES SYSTEM AS OF JULY 30, 2019

OVERVIEW OF OPERATIONS

Company Background

Lob was founded in May 2013 as part of YCombinator's Summer-2013 cohort, with the objective of making the offline world programmable. The two flagship products are a print-and-mail API and an address verification API. The organization is headquartered in San Francisco, California, with a global print partner network all over the world.

Industries served by Lob include financial services, healthcare, insurance, legal services, telecommunications, and marketing.

Description of Services Provided

Lob provides two primary services: a print-and-mail API and an address verification API.

The print-and-mail API allows users to programmatically send postcards, letters, and checks. With a single API request, users can send a custom html page (or image/pdf), which Lob will render and transmit to the global print partner network. The print partner will physically print the mail piece and hand it off to the local mail carrier (USPS in the United States, 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.

The address verification API allows users to sanitize, enrich, and geocode address information. It's a fast, performant, and easy way for building address autocomplete forms, looking up the latitude/longitude of addresses, verifying address deliverability as determined by the local mail carrier, etc., and works 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--and--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-and-mail services, and the financial, operational, and compliance requirements that Lob has established for the services. The print and mail services of Lob are subject to the security and privacy requirements of the Health Insurance Portability and Accountability Act Administrative Simplification, as amended, including relevant regulations, 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-and-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.

Components of the System

Infrastructure

Primary infrastructure used to provide Lob's Print & Mail and Address Verification Automation Software 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 ALB	Load balances traffic across servers.
Databases	AWS db.m5.12xlarge	Hosts application data.

Software

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

Primary Software		
Software	**Operating System**	**Purpose**
NodeJS, Golang	Linux	Runs application code.
Kubernetes	Linux	Runs all containerized services, handles deployments and load balancing, auto-scaling, authentication, rate-limiting, logging, etc.

People

Lob has a staff of approximately 80 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 the Lob service
- Customer Experience: Manages any support issues that customers have
- People: Runs HR and Recruiting functions. Manages payroll, benefits, employee development, recruiting, and other programs
- Partner Operations: works on managing the print partner network and onboarding new print partners
- Finance: The finance team works on managing 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-and-mail documents, customers need to pass at a minimum:

- Recipient name
- Recipient mailing address

When sending checks Lob would also receive:

- Sender bank account and routing numbers
- Memo line and amount

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

When sending letters, the mail content is entirely up to the customer. Customers can send marketing mail which contains non-PII data, or operational/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 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 these policies and procedures that define how services should be delivered. These are located on the Company's intranet and can be accessed by any 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 in access control lists. In the event incompatible responsibilities cannot be segregated, Lob implements monitoring of one or more of the responsibilities. Monitoring must be performed by a superior without responsibility for performing the conflicting activities or by personnel from a separate department.

All resources are managed in the asset inventory system and each asset is assigned an owner. Owners are responsible for approving access to the resource and for performing periodic reviews of access by role.

Employees and approved vendor personnel sign on to the Lob network using federated access via Okta. Users are also required to separately sign on to any systems or applications that do not use the shared sign-on functionality of Okta. Passwords must conform to defined password standards and are enforced through parameter settings when available.

Employees accessing the system from outside the Lob network are required to use a token-based two-factor authentication system. Employees are issued tokens upon employment and must return the token during their exit interview. Vendor personnel are not permitted to access the system from outside the Lob network.

Customer employees' access print-and-mail services through the Internet using the 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.

Customer employees may sign on to their systems using virtual server administration accounts. These administration accounts use a two-factor authentication system.

Upon hire, employees are assigned to a position in the HR management system. Two days prior to the employees' start date, the HR management system creates a report of employee user IDs to be created and access to be granted. The report is used by the security help desk to create user IDs and access rules. Access rules have been pre-defined based on the defined roles. The system lists also include employees with position changes and the associated roles to be changed within the access rules.

On a quarterly basis, access rules for each role are reviewed by a working group composed of security help desk, data center, customer service, and HR personnel. In evaluating role access, group members consider job description, duties requiring segregation, and risks associated with access. Completed rules are reviewed and approved by the CISO. As part of this process, the CISO reviews access by privileged roles and requests modifications based on this review.

On a quarterly basis, managers review roles assigned to their direct reports. Role lists are generated by security and distributed to the managers via the event management system. Managers review the lists and indicate the required changes in the event management record. The record is routed back to the security help desk for processing. The security help desk manager identifies any records not returned within two weeks and follows up with the manager. As part of this process, the CISO reviews employees with access to privileged roles and requests modifications through the event management system.

Computer Operations - Backups

Customer data is backed up and monitored 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.

Backup infrastructure and on-site backup tape media are physically secured in locked cabinets and/or caged environments within the third-party data centers. The backup infrastructure resides on private networks logically secured from other networks.

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 service level agreements. 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:

- Data center space, power and cooling
- Disk storage
- Tape storage
- Network bandwidth
- API capacity
- Print partner capacity

Lob has implemented a patch management process to ensure contracted customer and infrastructure 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 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 that includes firewalls, routers, and servers. In the event that a primary system fails, the redundant hardware is configured to take its place.

Penetration testing is conducted to measure the security posture of a target system or environment. The third-party vendor uses an accepted industry standard penetration testing methodology specified by Lob. The third-party vendor's approach begins with a vulnerability analysis of the target system to determine what vulnerabilities exist on the system that can be exploited via a penetration test, simulating a disgruntled/disaffected insider or an attacker that has obtained internal access to the network. Once vulnerabilities are identified, the third-party vendor attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing includes network and application layer testing as well as testing of controls and processes around the networks and applications and occurs from both outside (external testing) and inside the network.

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. Tools requiring installation in the Lob system are implemented through the Change Management process.

Authorized employees may access the system through from the Internet through the use of leading VPN technology. Employees are authenticated through the use of a token-based two-factor authentication system.

Boundaries of the System

The scope of this report includes the Print & Mail and Address Verification Automation Software system performed in the San Francisco, California facilities.

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

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION, AND MONITORING

Control Environment

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of Lob's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Lob's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

Specific control activities that the service organization has implemented in this area are described below:

- Formally, documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel
- Policies and procedures require employees sign an acknowledgment form indicating they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employee handbook
- Reference checks are performed for employees as a component of the hiring process

Commitment to Competence

Lob's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into the requisite skills and knowledge.

Specific control activities that the service organization has implemented in this area are described below:

- Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements
- Training is provided to maintain the skill level of personnel in certain positions

Management's Philosophy and Operating Style

Lob's management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks, and management's attitudes toward information processing, accounting functions, and personnel.

Specific control activities that the service organization has implemented in this area are described below:

- Management is periodically briefed on regulatory and industry changes affecting the services provided
- Executive management meetings are held to discuss major initiatives and issues that affect the business as a whole

Organizational Structure and Assignment of Authority and Responsibility

Lob's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

Lob's assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

Specific control activities that the service organization has implemented in this area are described below:

- Organizational charts are in place to communicate key areas of authority and responsibility
- Organizational charts are communicated to employees and updated as needed

Human Resources Policies and Practices

Lob's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top quality personnel who ensures the service organization is operating at maximum efficiency. Lob's human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

Specific control activities that the service organization has implemented in this area are described below:

- New employees are required to sign acknowledgement forms for the employee handbook and a confidentiality agreement following new hire orientation on their first day of employment
- Evaluations for each employee are performed on an annual basis
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist

Risk Assessment Process

Lob's risk assessment process identifies and manages risks that could potentially affect Lob's ability to provide reliable services to user organizations. This ongoing process requires that management identify significant risks inherent in products or services as they oversee their areas of responsibility. Lob identifies the underlying sources of risk, measures the impact to organization, establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks.

This process has identified risks resulting from the nature of the services provided by Lob, and management has implemented various measures designed to manage these risks. Risks identified in this process include the following:

- Operational risk - changes in the environment, staff, or management personnel
- Strategic risk - new technologies, changing business models, and shifts within the industry
- Compliance - legal and regulatory changes

Lob has established an independent organizational business unit that is responsible for identifying risks to the entity and monitoring the operation of the firm's internal controls. The approach is intended to align the entity's strategy more closely with its key stakeholders, assist the organizational units with managing uncertainty more effectively, minimize threats to the business, and maximize its opportunities in the rapidly changing market environment. Lob attempts to actively identify and mitigate significant risks through the implementation of various initiatives and continuous communication with other leadership committees and senior management.

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of Lob's print-and-mail system; as well as the nature of the components of the system result in risks that the criteria will not be met. Lob addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meeting the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, Lob's management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

Information and Communications Systems

Information and communication is an integral component of Lob's internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations. This process encompasses the primary classes of transactions of the organization, including the dependence on, and complexity of, information technology. At Lob, information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, regulators, and employees.

Various weekly meetings are held, and status e-mails are sent to discuss operational efficiencies within the applicable functional areas and to disseminate new policies, procedures, controls, and other strategic initiatives within the organization. General updates to entity-wide security policies and procedures are usually communicated to the appropriate Lob personnel via e-mail messages.

Specific information systems used to support Lob print-and-mail system are described in the Description of Services section above.

Monitoring Controls

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. Lob's management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

On-Going Monitoring

Lob's management conducts quality assurance monitoring on a regular basis and additional training is provided based upon results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Management's close involvement in Lob's operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of Lob's personnel.

Reporting Deficiencies

An internal tracking tool is utilized to document and track the results of on-going monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

Changes to the System in the Last 12 Months

No significant changes have occurred to the services provided to user entities in the 12 months preceding the review date.

Incidents in the Last 12 Months

No significant incidents have occurred to the services provided to user entities in the 12 months preceding the review date.

Criteria Not Applicable to the System

All Common criterion was applicable to the Lob's Print & Mail and Address Verification Automation Software Services System.

Subservice Organizations

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

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, subservice organizations, 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	CC6.4	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.

Subservice Organization - AWS		
Category	**Criteria**	**Control**
		Physical access points to server locations are recorded by closed circuit television cameras (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.

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

- Reviewing and reconciling output reports
- Reviewing attestation reports over services provided by vendors and subservice organization
- Monitoring external communications, such as customer complaints relevant to the services 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 maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of Lob services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Lob services.
6. User entities are responsible for providing Lob with a list of approvers for security and system configuration changes for data transmission.
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.

TRUST SERVICES CATEGORIES

In-Scope Trust Services Categories

Common Criteria (*to the Security Category*)
Security refers to the protection of i. information during its collection or creation, use, processing, transmission, and storage and ii. systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

CONTROL ACTIVITIES SPECIFIED BY THE SERVICE ORGANIZATION

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Control Environment		
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	An employee handbook is documented and reviewed on an annual basis to outline workforce conduct standards and enforcement procedures. Core values are communicated from the leadership team to personnel through the employee handbook. Personnel are required to acknowledge the employee handbook upon hire. Prior to employment, personnel are required to have successful reference checks completed. Employee performance is evaluated on an annual basis by management, a peer, and a self-review. Employees are directed on how to report unethical behavior in a confidential manner. Entity policies include probation, suspension, and termination as potential sanctions for employee misconduct.
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Leadership team roles and responsibilities are documented and reviewed annually. Leadership team performance is evaluated on an annual basis and the results are distributed to internal personnel. The leadership team maintains independence from those that operate the key controls within the environment. The leadership team meets monthly with operational management to assess the effectiveness and performance of key controls within the environment. Operational management assigns responsibility for and monitors the effectiveness and performance of controls implemented in the environment.
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	A documented organizational chart is in place to communicate organizational structures, lines of reporting, and areas of authority. The organizational chart updates on an automated basis as changes are made to the organizational structure and lines of reporting in the HR portal.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Control Environment		
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's intranet. Management reviews job descriptions when updates are needed. Upon hire, personnel are required to acknowledge the employee handbook which requires adherence to the personnel's job role and responsibilities. IT departments have career progression plans in place to guide personnel in performing job responsibilities. The leadership team has established proper segregations of duties for key job functions and roles within the organization. Employee performance is evaluated on an annual basis by management, a peer, and a self-review. The entity evaluates the competencies and experience of candidates prior to hiring and of personnel transferring job roles or responsibilities. Job requirements are documented in the job descriptions and candidates' abilities to meet these requirements are evaluated as part of the hiring or transfer evaluation process. The entity has a recruiting department that is responsible for attracting individuals with competencies and experience that align with the entity's goals and objectives. Management has created a training program for its employees. Employees are required to complete information security and awareness training upon hire. Current employees that deal with sensitive information are required to complete information security awareness training on an annual basis. Prior to employment, personnel are required to have successful reference checks completed. An employee handbook is documented and reviewed on an annual basis to outline workforce conduct standards and enforcement procedures.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Control Environment		
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	A documented organizational chart is in place to communicate organizational structures, lines of reporting, and areas of authority. Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's intranet. Upon hire, personnel are required to acknowledge the employee handbook which requires adherence to the personnel's job role and responsibilities. Personnel are required to stay in compliance with the employee handbook as updates are made. Policies and procedures are in place that outline the competency and training requirements for personnel. Employee performance is evaluated on an annual basis by management, a peer, and a self-review. Entity policies include probation, suspension, and termination as potential sanctions for employee misconduct.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Information and Communication		
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Information security policies and procedures are documented for supporting the functioning of controls and processes and made available to its personnel through the entity's intranet. Validation checks are in place to prevent incomplete or incorrect data from being entered into the system. Data flow diagrams, process flowcharts, and narratives are documented and maintained by management to identify the relevant internal and external information sources of the system. Data entered into the system, processed by the system, and output from the system is protected from unauthorized access.
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's intranet. The entity's policies and procedures and employee handbook are made available to employees through the entity's intranet. Employees are required to complete information security and awareness training upon hire. Upon hire, personnel are required to acknowledge the employee handbook which requires adherence to the personnel's job role and responsibilities. Personnel are required to stay in compliance with the employee handbook as updates are made. Documented incident response policies and procedures are in place to guide personnel in the event of an incident. The entity's objectives and system changes are communicated to its personnel via bi-monthly company-wide meetings.
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	The entity's third-party agreement delineates the boundaries of the system and describes relevant system components. The entity's third-party agreement communicates the system commitments and requirements of third parties.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Information and Communication		
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**
		The entity's third-party agreement outlines and communicates the terms, conditions and responsibilities of third parties. Customer commitments, requirements and responsibilities are outlined and communicated through service agreements. Documented escalation procedures for reporting failures incidents, concerns and other complaints are in place and shared with external parties.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Risk Assessment		
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	Organizational goals are developed in alignment with company objectives and strategies. Objective key results are established for operational and internal controls effectiveness, including the acceptable level of control operation and failure and reviewed on a quarterly basis. Responsible parties are defined and assigned to coordinate and monitor compliance and audit activities. Business plans and budgets align with entity strategies and objectives. Entity strategies, objectives and budgets are assessed on a monthly basis. Management reviews and addresses repeated control failures.
CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	Documented policies and procedures are in place to guide personnel when performing the risk assessment process. Management has defined a formal risk management process that specifies the process for evaluating risks based on identified threats and the specified tolerances. A formal risk assessment is performed on an annual basis to identify threats that could impair systems security commitments and requirements. The entity's risk assessment process includes: • Identifying the relevant information assets that are critical to business operations • Prioritizing the criticality of those relevant information assets • Identifying and assessing the impact of the threats to those information assets • Identifying and assessing the impact of the vulnerabilities associated with the identified threats • Assessing the likelihood of identified threats and vulnerabilities • Determining the risks associated with the information assets • Addressing the associated risks identified for each identified vulnerability Identified risks are rated using a risk evaluation process and rating are reviewed by management.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Risk Assessment		
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**
		Management develops risk mitigation strategies to address risks identified during the risk assessment process. For gaps and vulnerabilities identified from the risk assessment, remediation efforts, including the implementation of controls, are assigned to process owners based on roles and responsibilities. A vendor risk assessment is performed for third-party providers on an annual basis which includes reviewing the activities performed by third-parties.
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	Management identifies and assesses the types of fraud (e.g. fraudulent reporting, loss of assets, unauthorized system access, overriding controls) that could impact their business and operations on an annual basis. As part of management's assessment of fraud risks, management considers key fraud factors such as incentives, pressures, opportunity for unauthorized access or use of data, and employee morale and attitude. Management has defined a formal risk management process that specifies the process for evaluating risks based on identified threats and the specified tolerances. A formal risk assessment is performed on an annual basis to identify threats that could impair systems security commitments and requirements. Identified risks are rated using a risk evaluation process and ratings are reviewed by management. Management develops risk mitigation strategies to address risks identified during the risk assessment process.
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	Changes to the business structure and operations are considered and evaluated as part of the annual comprehensive risk assessment. Changes in key management and personnel are considered and evaluated as part of the annual comprehensive risk assessment. Changes to the entity's systems, applications, technologies, and tools are considered and evaluated as part of the annual comprehensive risk assessment.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Risk Assessment		
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**
		Management has defined a formal risk management process that specifies the process for evaluating risks based on identified threats and the specified tolerances. A formal risk assessment is performed on an annual basis to identify threats that could impair systems security commitments and requirements. Identified risks are rated using a risk evaluation process and rating are reviewed by management. Management develops risk mitigation strategies to address risks identified during the risk assessment process.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Monitoring Activities		
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity. The monitoring software is configured to alert the Infrastructure and Security Team when thresholds have been exceeded. On an annual basis, management reviews the controls implemented within the environment for operational effectiveness and identifies potential control gaps and weaknesses. Key systems, tools, and applications are reviewed internally for compliance against documented policies and procedures continuously using a compliance monitoring tool. Control self-assessments that include, but are not limited to, logical access reviews, and backup restoration tests are performed on at least an annual basis. Vulnerability scans are performed quarterly on the network and application environment to identify control gaps and vulnerabilities. A third-party performs penetration testing annually to identify and exploit vulnerabilities identified within the environment. Employee performance is evaluated on a semi-annual basis by management, a peer, and a self-review. Management obtains and reviews attestation reports of vendors and third parties to evaluate the effectiveness of controls within the vendor or third-party's environment. A formal risk assessment is performed on an annual basis to identify threats that could impair systems security commitments and requirements.
CC4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	Management develops risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process. Vulnerabilities, deficiencies, and control gaps identified as part of the evaluations performed are communicated to those parties responsible for taking corrective actions.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Monitoring Activities		
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**
		Management tracks whether vulnerabilities, deficiencies and control gaps identified as part of the evaluations performed are addressed in a timely manner.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Control Activities		
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Controls within the environment are modified and implemented to mitigate vulnerabilities, deviations and control gaps identified as part of the various evaluations. Performance of the controls implemented within the environment are assigned to appropriate process owners and operational personnel based on roles and responsibilities. Management has documented the relevant controls in place for each key business or operational process. Management has incorporated a variety of controls into their environment that include manual, automated, preventive, detective, and corrective controls. Business continuity and disaster recovery plans are developed and updated on an annual basis. Business continuity and disaster recovery plans are tested on an annual basis.
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	Organizational and information security policies and procedures are documented for supporting the functioning of controls and processes and made available to its personnel through the company's intranet. Management has established controls around the entity's technology infrastructure to address the risks of incomplete, inaccurate, and unavailable technology processing. As part of the risk assessment process, the use of technology in business processes is evaluated by management. The internal controls implemented around the entity's technology infrastructure include, but are not limited to: • Restricting access rights to authorized users • Limiting services to what is required for business operations • Authentication of access • Protecting the entity's assets from external threats

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Control Activities		
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Organizational and information security policies and procedures are documented for supporting the functioning of controls and processes and made available to its personnel through the company's intranet. Process owners and key management are assigned ownership to each key control implemented within the entity's environment. Performance of the controls implemented within the environment are assigned to appropriate process owners and operational personnel based on roles and responsibilities.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Logical and Physical Access Controls		
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Documented policies and procedures are in place regarding systems authentication, access, and security monitoring. Logical access to systems is granted to an employee as a component of the hiring process. Logical access to systems is revoked as a component of the termination process. The API key is rotated as a component of the offboarding process. Control self-assessments that include logical access reviews are performed on a quarterly basis. External access by employees is permitted only through a virtual private connection (VPN) which requires Okta credentials, and multi-factor authentication (MFA). The system is accessed only via encrypted connection. User access is restricted via role-based security privileges defined within the access control system. Privileged access to sensitive resources is restricted to defined user roles. CloudTrail audit logging settings are in place to track system events. CloudTrail audit logs are maintained and reviewed at least annually. VPN audit logging settings are in place to track system events. VPN audit logs are maintained and reviewed at least annually.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	Documented policies and procedures are in place regarding systems authentication, access, and security monitoring. Logical access to systems is granted to an employee as a component of the hiring process. Logical access to systems is revoked as a component of the termination process. The API key is rotated as a component of the offboarding process.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Logical and Physical Access Controls		
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**
		Control self-assessments that include logical access reviews are performed on a quarterly basis. Privileged access to sensitive resources is restricted to defined user roles.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	Documented policies and procedures are in place regarding systems authentication, access, and security monitoring. Logical access to systems is granted to an employee as a component of the hiring process. Logical access to systems is revoked as a component of the termination process. The API key is rotated as a component of the offboarding process. Control self-assessments that include logical access reviews are performed on a quarterly basis. Privileged access to sensitive resources is restricted to defined user roles. User access is restricted via role-based security privileges defined within the access control system.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	This criterion is managed by the subservice organization. Please refer to the 'Subservice Organizations' section for further details.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	Policies and procedures are in place to guide personnel in data, hardware and software disposal and destruction. Data that is no longer required for business purposes is rendered unreadable. Policies and procedures are in place for removal of media storing critical data or software.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	VPN, SSL and other encryption technologies are used for defined points of connectivity. External access by employees is permitted only through a VPN which requires Okta credentials, and MFA.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Logical and Physical Access Controls		
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**
		Server certificate-based authentication is used as part of the SSL encryption with a trusted certificate authority. VPN user access is restricted via role-based security privileges defined within the access control system. Logical access to stored data is restricted to authorized personnel. A firewall is in place to filter unauthorized inbound network traffic from the internet. The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule. An intrusion detection system (IDS) is utilized to analyze network events and report possible or actual network security breaches. The IDS is configured to notify personnel upon intrusion detection. System monitoring logs are stored indefinitely and can be pulled at any time for reviewal. Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software. The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available. The antivirus software is configured to scan workstations in real time.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	Logical access to stored data is restricted to authorized personnel. VPN, SSL and other encryption technologies are used for defined points of connectivity. External access by employees is permitted only through a VPN which requires Okta credentials, and MFA. Server certificate-based authentication is used as part of the SSL encryption with a trusted certificate authority.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Logical and Physical Access Controls		
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	A firewall is in place to filter unauthorized inbound network traffic from the internet. The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule. An IDS is utilized to analyze network events and report possible or actual network security breaches. The IDS is configured to notify personnel upon intrusion detection. Documented change control policies and procedures are in place to guide personnel in the change management process. The ability to migrate changes into the production environment is restricted to authorized and appropriate users. Alerts are generated in slack when completed deployment changes are made. A file integrity monitoring (FIM) is in place to ensure only authorized changes are deployed into the production environment. The FIM application is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected. Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software. The antivirus software pushes updates to the installed antivirus software as new updates/signatures are available. The antivirus software is configured to scan workstations in real time. Vulnerability scans are performed quarterly on the network and application environment to identify control gaps and vulnerabilities. A third-party performs penetration testing annually to identify and exploit vulnerabilities identified within the environment. An IDS is utilized to analyze network events and report possible or actual network security breaches.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Logical and Physical Access Controls		
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**
		The IDS is configured to notify personnel upon intrusion detection.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
System Operations		
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity. The monitoring software is configured to alert the Infrastructure and Security Team when thresholds have been exceeded. Management has defined configuration standards in the information security policies and procedures. A FIM is in place to ensure only authorized changes are deployed into the production environment. The FIM application is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected. Policies and procedures are in place for removal of media storing critical data or software. A firewall is in place to filter unauthorized inbound network traffic from the internet. The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule. An IDS is utilized to analyze network events and report possible or actual network security breaches. The IDS is configured to notify personnel upon intrusion detection. Policies and procedures are in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment. Vulnerability scans are performed quarterly on the network and application environment to identify control gaps and vulnerabilities. A third-party performs penetration testing annually to identify and exploit vulnerabilities identified within the environment.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
System Operations		
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints. Policies and procedures are in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment. Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity. The monitoring software is configured to alert the Infrastructure and Security Team when thresholds have been exceeded. A firewall is in place to filter unauthorized inbound network traffic from the internet. The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule. An IDS is utilized to analyze network events and report possible or actual network security breaches. The IDS is configured to notify personnel upon intrusion detection. A FIM is in place to ensure only authorized changes are deployed into the production environment. The FIM application is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected. Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software. The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available. The antivirus software is configured to scan workstations in real time. Policies and procedures are in place for removal of media storing critical data or software.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
System Operations		
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**
		CloudTrail audit logging settings are in place to track system events. CloudTrail audit logs are maintained and reviewed at least annually. VPN audit logging settings are in place to track system events. VPN audit logs are maintained and reviewed at least annually. Documented incident response policies and procedures are in place to guide personnel in the event of an incident.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints. The incident response and escalation procedures are reviewed at least annually for effectiveness. The incident response and escalation procedures define the classification of incidents based on its severity. Resolution of incidents is communicated to users within the corresponding ticket. Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution. Management reviews reports summarizing incidents, root cause of incidents, and corrective action plans.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints. Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution. The actions taken to address identified vulnerabilities are documented and communicated to affected parties.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
System Operations		
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**
		Documented incident response policies and procedures are in place to guide personnel in the event of an incident. Resolution of incidents are documented within the ticket and communicated to affected users. Remediation actions taken for security incidents are documented within the ticket and communicated to affected users. Identified incidents are analyzed, classified and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach. Management reviews reports summarizing incidents, root cause of incidents, and corrective action plans.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Change management requests are opened for incidents that require permanent fixes. Backup restoration tests are performed on an ad-hoc basis during the normal course of business. Management reviews reports summarizing incidents, root cause of incidents, and corrective action plans. Business continuity and disaster recovery plans are developed and updated on an annual basis. Business continuity and disaster recovery plans are tested on an annual basis.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Change Management		
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Documented change control policies and procedures are in place to guide personnel in the handling system changes. System changes are communicated to both internal and external users. The ability to migrate changes into the production environment is restricted to authorized and appropriate users. System changes are authorized and approved by two team members prior to implementation. System change requests are documented and tracked in a ticketing system. System changes are tested prior to implementation. Types of testing performed depend on the nature of the change. Development and test environments are physically and logically separated from the production environment. A FIM is in place to ensure only authorized changes are deployed into the production environment.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Risk Mitigation		
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Documented policies and procedures are in place to guide personnel when performing the risk assessment process. Management has defined a formal risk management process that specifies the process for evaluating risks based on identified threats and the specified tolerances. A formal risk assessment is performed on an annual basis to identify threats that could impair systems security commitments and requirements. Identified risks are rated using a risk evaluation process and ratings are reviewed by management. Management develops risk mitigation strategies to address risks identified during the risk assessment process. The entity has purchased insurance to offset the financial loss that could result from a critical security incident or exploitation of a vulnerability.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	Management has defined a third-party vendor risk management process that specifies the process for evaluating third-party risks based on identified threats and the specified tolerances. A vendor risk assessment is performed for third-party providers on an annual basis which includes reviewing the activities performed by third-parties. Management develops third-party risk mitigation strategies to address risks identified during the risk assessment process. Identified third-party risks are rated using a risk evaluation process and ratings are reviewed by management. The entity's third-party agreement outlines and communicates: • The scope of services • Roles and responsibilities • Terms of the business relationship • Communication protocols • Compliance requirements • Service level • Just cause for terminating the relationship

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Risk Mitigation		
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**
		Management obtains and reviews attestation reports of vendors and third parties to evaluate the effectiveness of controls within the vendor or third-party's environment. The entity has documented procedures for addressing issues identified with third parties. The entity has documented procedures for terminating third-party relationships.

SECTION 4

INFORMATION PROVIDED BY THE SERVICE AUDITOR

GUIDANCE REGARDING INFORMATION PROVIDED BY THE SERVICE AUDITOR

A-LIGN ASSURANCE's examination of the controls of Lob was limited to the Trust Services Criteria, related criteria and control activities specified by the management of Lob and did not encompass all aspects of Lob's operations or operations at user entities. Our examination was performed in accordance with American Institute of Certified Public Accountants (AICPA) AT-C 105 and AT-C 205.

Our examination of the control activities was performed using the following testing methods:

TEST	DESCRIPTION
Inquiry	The service auditor made inquiries of service organization personnel. Inquiries were made to obtain information and representations from the client to determine that the client's knowledge of the control and corroborate policy or procedure information.
Observation	The service auditor observed application of the control activities by client personnel.
Inspection	The service auditor inspected among other items, source documents, reports, system configurations to determine performance of the specified control activity and in some instances the timeliness of the performance of control activities.
Re-performance	The service auditor independently executed procedures or controls that were originally performed by the service organization as part of the entity's internal control.

In determining whether the report meets the criteria, the user auditor should perform the following procedures:

- Understand the aspects of the service organization's controls that may affect the service commitments and system requirements based on the applicable trust services criteria;
- Understand the infrastructure, software, procedures and data that are designed, implemented and operated by the service organization;
- Determine whether the criteria are relevant to the user entity's assertions; and
- Determine whether the service organization's controls are suitably designed to provide reasonable assurance that its service commitments and system were achieved based on the applicable trust services criteria.