LISTRAK INC.

SOC 3 REPORT ON THE DIGITAL MARKETING SYSTEM
RELEVANT TO SECURITY

FOR THE PERIOD
MAY 1, 2019 THROUGH OCTOBER 31, 2019

McKONLY & ASBURY

LISTRAK INC.

TABLE OF CONTENTS

I. INDEPENDENT SERVICE AUDITOR’S REPORT PROVIDED BY McKONLY & ASBURY, LLP

McKONLY & ASBURY

BEST PLACES to work in PA · BEST ACCOUNTING FIRMS TO WORK FOR · BEST ACCOUNTING FIRMS FOR WOMEN · BEST of Accounting CLIENT SATISFACTION 2019

MEMBERS
AMERICAN AND PENNSYLVANIA INSTITUTES
OF CERTIFIED PUBLIC ACCOUNTANTS

INDEPENDENT MEMBER OF
PrimeGlobal

INDEPENDENT SERVICE AUDITOR'S REPORT

The Management Team
Listrak Inc.
Lititz, Pennsylvania

Scope

We have examined Listrak Inc.'s (Listrak's) accompanying assertion titled "Assertion of Listrak Inc.'s Management" (assertion) that the controls within Listrak's Digital Marketing System (system) were effective throughout the period May 1, 2019, to October 31, 2019, to provide reasonable assurance that Listrak'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).*

Service Organization's Responsibilities

Listrak 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 Listrak's service commitments and system requirements were achieved. Listrak has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Listrak is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.

- Assessing the risks that controls were not effective to achieve Listrak's service commitments and system requirements based on the applicable trust services criteria.

- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Listrak's service commitments and system requirements based the applicable trust services criteria.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Listrak's digital marketing system were effective throughout the period May 1, 2019, to October 31, 2019, to provide reasonable assurance that Listrak's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

McKonly & Asbury, LLP

Camp Hill, Pennsylvania
December 3, 2019

II. MANAGEMENT’S ASSERTION

ASSERTION OF LISTRAK INC.'S MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within Listrak Inc.'s (Listrak's) digital marketing system (system) throughout the period May 1, 2019 to October 31, 2019, to provide reasonable assurance that Listrak's service commitments and system requirements relevant to security were achieved. Our description of the boundaries of the system is presented in Section III 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 May 1, 2019 to October 31, 2019, to provide reasonable assurance that Listrak'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*). Listrak's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Section IV.

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 May 1, 2019 to October 31, 2019, to provide reasonable assurance that Listrak's service commitments and system requirements were achieved based on the applicable trust services criteria

/s/Brian Sload
Brian Sload
Director of Information Security

III. LISTRAK’S DESCRIPTION OF THE DIGITAL MARKETING SYSTEM

LISTRAK INC.

LISTRAK'S DESCRIPTION OF THE DIGITAL MARKETING SYSTEM

OVERVIEW OF LISTRAK INC. OPERATIONS

Listrak Inc. (Listrak) is a privately-held eCommerce/digital marketing and SaaS company. As an industry-leading marketing cloud focused solely on retailers, Listrak delivers results for its clients with the power of 1:1 interactions that drive incremental revenue, engagement, lifetime value, and growth. Fueled by artificial intelligence, actual human intelligence, machine learning, and predictive analytics, the Listrak platform boasts a comprehensive set of marketing automation and CRM solutions that unify, interpret, and personalize data to engage customers across channels and devices.

Listrak serves more than 1,000 clients and works with leading brands. The company has been offering its services and solutions since 1999. For more information, visit www.listrak.com.

THE CONTROL ENVIRONMENT – ORGANIZATION AND MANAGEMENT

Listrak uses reasonable care and maintains appropriate policies and procedures to protect data from loss, misuse, unauthorized access, disclosure, alteration, or destruction. The control environment at Listrak provides employees with the company's overall philosophy on professional conduct and operating style. It provides the framework for other aspects of internal control. The control environment at Listrak involves the following areas:

- Employee Handbook.
- Organizational Structure.
- Policies and Procedures.
- Job Descriptions.

Listrak maintains its corporate headquarters in Lititz, Pennsylvania, with satellite offices in King of Prussia, Pennsylvania and Newport Beach, California. The company also has approximately twenty employees working remotely, across a number of functions. The organizational structure is designed along functional lines, which provides an adequate segregation of duties or the effective application of mitigating or compensating controls, as well as clearly defined areas of responsibility relating to the control environment components.

COMMUNICATIONS AND INFORMATION

Documentation of the application and training is made available to authorized external users via Listrak's application administration page and the Training Department's website. Internal users/employees can access the same training and documentation available to external users. In addition, internal users also have access to implementation documentation, additional training resources, and have a team member representing their department to bring and take information related to security items to and from their team.

Security commitments regarding the system are included in the customer master services agreement and customer specific service level agreements. Acceptable Use Policy (AUP) and Privacy Policies are available on the Listrak marketing site (www.listrak.com). Personnel are required to read and accept the code of conduct and the statement of confidentiality and privacy practices upon their hire and must reaffirm them annually thereafter. Management monitors compliance with training requirements, including the annual security awareness training.

Policy and procedures documents for significant processes, which include responsibility for reporting operational failures, incidents, system problems, concerns, and user complaints (and the process for doing so), are published and made available on the intranet, and are provided in the annual security training.

RISK ASSESSMENT

Management maintains insurance coverage against various risks, including errors and omissions; as well as other general liability and employment insurance, as required by law. Coverage is maintained at levels that management considers reasonable, given the size and scope of operations.

Listrak maintains a risk management program to continually discover, research, plan, resolve, monitor, and optimize information security risks that impact business objectives and customers using a Risk Log. The Risk Log is updated regularly and uses a rating system to prioritize risks.

Playbooks, plans, and policies around incident response are also maintained, updated, and followed. The Listrak contingency plan is tested annually. Listrak performs internal and external vulnerability assessments at least quarterly to identify weaknesses and risks. The results are used to patch and/or fix the vulnerabilities that are discovered.

MONITORING ACTIVITIES

Listrak's Director of Information Security (IS Director) (and the IS Department) is responsible for monitoring the quality of internal control performance and assessments as related to audit requirements. Results are communicated with the Director of Information Technology (IT Director) for monitoring and corrective actions.

Listrak also conducts a third-party penetration test on an annual basis. The findings are then tracked through resolution. Quarterly internal and external vulnerability scans are also conducted, and the findings are submitted for resolution.

CONTROL ACTIVITIES

Listrak maintains formal policies that provide guidance for information security within the organization and the supporting IT environment. The policies are reviewed and approved on a regular basis, and if necessary, modified to accommodate any changes at Listrak.

Roles and responsibilities for security are defined and communicated to personnel, as well as to third-parties. Additionally, designated security advocates are assigned in each business unit and report indirectly to the security team. Management monitors compliance with training requirements including annual security awareness training.

LOGICAL AND PHYSICAL ACCESS CONTROLS

Access control and perimeter control policies are documented and in place. The policies address logical access and security to applications and network infrastructure. Password policies require passwords to be complex, expire after a defined period of days, and enforce invalid attempt and lockout rules. Logical access to systems and applications requires approval of the user's manager and secondary approval by the IT Director – depending on the access requested.

All elevated user ID requests require approval by the user's manager, and the IS Director and/or the IT Director. This process helps ensure the enforcement of the separation of duties policy. Access is not granted without the prior approval by these parties.

Physical access to all Listrak facilities requires the use of an electronic access card. The facility perimeter is monitored 24x7 by closed circuit cameras at all ingress locations and any sensitive locations inside the facilities. Elevated physical access requests require approval by the user's manager and the IT Director.

External points of connectivity are protected by firewall clusters implementing access policies and Intrusion Prevention Systems, network segmentation, and several layers of defense to prevent unauthorized external users from gaining access to the organizations internal systems and devices.

The ability to install software on employee workstations and laptops is restricted to IT Support personnel. Antivirus software is installed on all workstations, laptops, and servers supporting such software.

SYSTEM OPERATIONS

Listrak's computerized operations environment includes the use of workstations for all employees, as well as servers that provide a platform for data serving, application development, supporting administrative services, and shared resources within the company.

Information Technology staff are the only users with access to servers to facilitate production, development, maintenance, and user support functions. Listrak servers are in secure colocation facilities, which utilize biometrics and electronic badge access to gain access to the interior of the building, with additional restricted access to the Listrak cage space in those data centers. Two additional cloud sites are hosted in two Amazon regions. All communication between the production, Amazon, and corporate locations transfer securely over site-to-site encrypted VPN tunnels.

Vulnerabilities

Listrak performs monthly routine patching of its operating environments. There is a scheduled release, approval, and installation process with all OS and backend supporting systems. All planned maintenance windows are posted seven days prior to their occurrence on the Listrak Admin site (admin.listrak.com) as well as on the status page (status.listrak.com).

Internal and external vulnerability scans are performed at least quarterly. IT management takes appropriate action based on the results of the scans. Logging/monitoring software is used to collect data from system infrastructure components and production systems; to monitor system performance, potential security threats and vulnerabilities, and resource utilization.

Data Breaches and Incident Response

Listrak has an incident response policy that is followed to resolve and escalate any reported or detected event. These events may span from a suspected virus on a PC to a potentially exploited server to a possible loss of customer data. Each are considered critical, since many data breaches begin as a phishing email or social engineering attack, then make entry into an environment and expand from there.

Disaster Recovery

Listrak has a robust system and data backup environment. Backup durations and frequency vary depending on requirements. All system and data backups are replicated offsite, in addition to the local backup. Those backups are transferred over secured and encrypted site-to-site SSL VPN tunnels.

Live and backup data are replicated from the primary data center to the disaster recovery data center. The Amazon region deployments are fully redundant within their own region (multiple AWS Availability Zones), as well as between the two regions. This allows for a total outage of one AWS Availability zone or an entire AWS Region with no impact to Listrak's application services.

System Development, Deployment, and Maintenance

Listrak's Application Development department operates in a continuous deployment environment. The continuous deployment process allows Listrak to implement new features and software maintenance updates quickly and efficiently. Listrak utilizes three completely separated environments for this process. Initial development/testing is performed in a development environment. Prior to production deployment, the changes are tested in a staging environment. An implementation process that includes verification of operation and back out steps is used for every deployment.

CHANGE MANAGEMENT

Application change requests must be reviewed and approved by the Application Manager prior to work beginning on the request. Segregation of duties exists between personnel responsible for authorizing, developing, and testing changes. Change requests are evaluated to determine the potential effect of the change on security, availability, processing integrity, confidentiality, and system requirements throughout the change management process.

Post implementation procedures are designed to verify the operation of system changes were performed for a defined period, as determined during the project planning, after the implementation for other than minor changes, and results are shared with internal and external users and customers as required to meet commitments and system requirements.

Segregation of duties also exists between IT Infrastructure personnel responsible for authorizing, implementing, and testing IT changes. IT Infrastructure changes are tracked, approved, and tested prior to implementation. Access to implement infrastructure changes is limited to the IT Engineering team.

During the ongoing risk assessment process and the periodic planning and budgeting processes, infrastructure, data, software, and procedures are evaluated for needed changes. Policies and procedures surrounding application and infrastructure change management exist and are periodically updated as needed.

RISK MITIGATION

Listrak maintains a risk management program to continually discover, research, plan, resolve, monitor, and optimize information security risks that impact business objectives and customers. The Risk Log is updated regularly and uses a rating system to prioritize risks. Incident response procedures are defined for resolving and escalating reported events. Playbooks, plans, and policies around incident response are also maintained, updated, and followed.

IV. PRINCIPLE SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

LISTRAK INC.

PRINCIPLE SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Listrak designs its processes and procedures related to the Listrak Platform to meet its objectives for its digital marketing services. Those objectives are based on the service commitments that Listrak makes to user entities, the laws and regulations that govern the provision of digital marketing services and the financial, operational, and compliance requirements that Listrak has established for the services.

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 Listrak Platform 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.

Listrak establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Listrak's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the Listrak Platform.

BEST of Accounting
CLIENT SATISFACTION
2019

BEST PLACES to work in PA

BEST ACCOUNTING FIRMS TO WORK FOR

BEST ACCOUNTING FIRMS FOR WOMEN

www.macpas.com

MEMBERS
AMERICAN AND PENNSYLVANIA INSTITUTES
OF CERTIFIED PUBLIC ACCOUNTANTS

INDEPENDENT MEMBER OF
PrimeGlobal