Tab Service Company

SOC 3 Report

Management's Assertion Regarding the Effectiveness of Controls Relevant to Security, Processing Integrity, and Confidentiality for the period December 1, 2017 to May 31, 2018

plante moran | Audit. Tax. Consulting. Wealth Management.

Contents

Plante & Moran, PLLC
10 South Riverside Plaza
9th floor
Chicago, IL 60606
Tel: 312.207.1040
Fax: 312.207.1066
plantemoran.com

Section 1. Independent Service Auditor's Report

Tab Service Company
Chicago, Illinois

Scope

We have examined Tab Service Company's (Tab Service) accompanying assertion entitled "Tab Service Company's Assertion" (assertion) that the controls within Tab Service's 1099 Processing System (1099PS) were effective throughout the period December 1, 2017 to May 31, 2018, to provide reasonable assurance that Tab Service's service commitments and system requirements were achieved based on trust services criteria relevant to security, processing integrity, and confidentiality set forth in TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2016)* (AICPA, *Trust Services Criteria*) (2016 trust services criteria) (applicable trust services criteria). Management's description of the aspects of the 1099PS covered by its assertion is attached. We did not examine this description, and accordingly, we do not express an opinion on it.

Tab Service uses XL.net for information technology management services, Off-Site LLC for colocation services, and Rackspace US, Inc. for email exchange server hosting. A list of these subservice organizations is provided in the description of the 1099PS. The description indicates that certain applicable trust services criteria can be met only if certain types of controls that management expects to be implemented at the subservice organizations are suitably designed and operating effectively. The description presents Tab Service's system; its controls relevant to the applicable trust services criteria; and the types of controls that the service organization expects to be implemented, suitably designed, and operating effectively at the subservice organizations to meet certain applicable trust services criteria. The description does not include any of the controls expected to be implemented at the subservice organizations. Our examination did not extend to the services provided by the subservice organizations, and we have not evaluated whether the controls management expects to be implemented at the subservice organizations have been implemented or the suitability of the design or operating effectiveness of such subservice organization controls.

The description indicates that certain applicable trust services criteria specified in the description can be met only if complementary user entity controls assumed in the design of Tab Service's controls are suitably designed and operating effectively along with related controls at the service organization. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service organization's responsibilities

Tab Service is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls to provide reasonable assurance that Tab Service's service commitments and system requirements were achieved. Tab Service has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Tab Service is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of 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 December 1, 2017 to May 31, 2018 to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust service 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 Tab Service'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 Tab Service's service commitments and system requirements based on the applicable trust services criteria

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

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 service 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 controls in conditions or that the degree of compliance with the policies and procedures may deteriorate.

Basis for qualification

Tab Service states in its description that controls have been implemented to monitor and review data retention requirements on an annual basis and to purge all documents exceeding retention requirements. However, review for data retention requirements and purging of records exceeding retention requirements was not performed during the period December 1, 2017 to May 31, 2018. As a result, controls were not operating effectively to achieve the Confidentiality Criteria 1.8 “The entity disposes of confidential information to meet the entity’s confidentiality commitments and system requirements.”

Opinion

In our opinion, except for the matter described in the preceding paragraph, management’s assertion that the controls within Tab Service’s 1099 PS were effective throughout the period December 1, 2017 to May 31, 2018 , to provide reasonable assurance that Tab Service’s service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Emphasis of a matter

As noted in management’s description, there were no new vendors or contractors incorporated as part of the system during the period December 1, 2017 to May 31, 2018. Therefore, we did not test the operating effectiveness of controls related to Confidentiality 1.4, “The entity obtains confidentiality agreements that are consistent with the entity’s confidentiality system requirements from vendors and other third parties whose products and servers are part of the system and have access to confidential information.”

Plante & Moran, PLLC

October 31, 2018

Chicago, Illinois

TAB
SERVICE
COMPANY

October 31, 2018

Plante & Moran, PLLC
10 South Riverside Plaza
Chicago, IL 60606

To Service Auditors:

We are responsible for designing, implementing, operating, and maintaining effective controls within Tab Service Company's (Tab Service) 1099 Processing System (1099 PS) throughout the period December 1, 2017 to May 31, 2018 to provide reasonable assurance that Tab Service's service commitments and system requirements relevant to security, processing integrity and confidentiality were achieved.   Our description of the boundaries of the system is presented in Section 3 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 December 1, 2017 to May 31, 2018, to provide reasonable assurance that Tab Service's service commitments and system requirements were achieved based on the trust services criteria relevant to security, processing integrity and confidentiality set forth in TSP section 100A, Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2016) (AICPA, Trust Services Criteria) (2016 trust services criteria) (applicable trust services criteria). Tab Service's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and systems 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 3.

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.

A review for data retention requirements and purging of records exceeding retention requirements was not performed during the period December 1, 2017 to May 31, 2018. As a result, controls were not operating effectively to achieve the Confidentiality Criteria 1.8 "The entity disposes of confidential information to meet the entity's confidentiality commitments and system requirements."

We assert, except for the matter described in the preceding paragraph, that the controls within the system were effective throughout the period December 1, 2017 to May 31, 2018, to provide reasonable assurance that Tab Service's service commitments and system requirements were achieved based on the applicable trust services criteria.

Robert Lambert

Robert Lambert, President

Section 3. Tab Service Company's Description of its 1099 Processing System Throughout the Period December 1, 2017 to May 31, 2018

A. Company Overview

Tab Service Company ("Tab Service") is a data processing service bureau based in Chicago, Illinois. Founded in 1960, Tab Service provides outsourced information management solutions to organizations that go outside for specific IT services.

Tab Service provides an array of data processing services:

- Document scanning
- Data entry
- Forms processing
- PDF scanning
- Litigation scanning
- 1095 processing
- 1098T processing
- 1099 processing
- Database management
- Data and media conversion
- Survey processing

Tax forms processing is a major line of business provided to customers. Tab Service is an approved IRS vendor for 1095, 1098, and 1099 filing and processing services and has a long history of serving the tax reporting needs of large organizations throughout the United States that are required to send tax forms to recipients and e-file with the IRS. Tab Service's 1099 Processing System (1099PS) gives customers a complete, end to end solution for 1095, 1098, and 1099 reporting and compliance, including 1099 printing, mailing and e-filing. It features built-in tools that ensure compliance with the latest government reporting requirements.

B. Scope of the Report

Report Framework

This report is considered a Service Organization Control 3 (SOC 3) report under the internal control reporting framework established by the American Institute of Certified Public Accountants (AICPA).

Scope

The scope of the report is limited to Tab Service's 1099 Processing System (1099PS). This report covers the 1099PS described above and the suitability of the design of controls to meet the criteria for the security, processing integrity and confidentiality principles set forth in TSP section 100, *Trust Services Principles,* *Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, Technical Practice Aids), effective for periods ending on or after December 15, 2016 (applicable trust services criteria) throughout the period December 1, 2017 to May 31, 2018.

Subsequent Events

Management is not aware of any relevant events that occurred subsequent to May 31, 2018 through the date of the service auditor's report that would have a significant effect on management's assertion.

C. Applicable Trust Services Principles and Relevant Criteria

The applicable trust services criteria have been included in Section IV. Tab Service's internal control process is designed to provide reasonable assurance for the achievement of reliable, effective operations and compliance with the criteria.

D. Summary of the 1099 Processing System

The 1099PS consists of computer servers, network file systems, PCs, databases, and applications used for processing tax form data. Software is limited to the MS Office 2010 suite, MS Access and two applications listed below. Tab Service employees utilize MS Windows 7 on Company issued personal computers and the following applications:

- TSC1099 – Web-based application that was developed and maintained internally
- AccountAbility – Commercial tax form processing software that was developed by IDMS in Melville, New York

E. Subservice Organizations

Tab Service uses subservice organizations to outsource web application hosting, information technology functions, and email server hosting services. The subservice organization and services provided are described below:

XL.Net (XL) is a service provider that contracts with Tab Service for the outsourcing of Tab Service's information technology management and support. XL complements the Tab Service Staff and provides the following services:

- Remote Managed Perimeter Security Service
- Local and Remote Network and System Management
- Local and Remote Desktop Support
- Virus Protection Service
- Patch Management, Monitoring, and Distribution
- Email Security Services
- User Management

On a monthly basis, Tab service meets with XL to review user access rights on its systems and to review information system status and trends in security related events, as well as to discuss potential areas of improvement for the XL network and systems.

The TSC 1099 web application is hosted by third party data center colocation service provider Off-Site LLC (Off-Site). Tab service obtains and reviews Off-Site service organization reports on the design and operating effectiveness of controls over the outsourced services.

Tab Service's email exchange server is hosted by Rackspace US, Inc. (Rackspace). The physical and environmental controls over the email exchange servers are managed by Rackspace while the configuration and management of the email exchange server is performed by XL.

F. Overview of 1099PS and Its Boundaries

Boundaries of the 1099PS

The boundaries of the 1099PS include applications (described above) and infrastructure that directly support the tax forms processing services provided by Tab Service to customers, including infrastructure, software, people, procedures, and data. Any applications, databases, and infrastructure that indirectly support the tax form processing services provided to customers are not included within the boundaries of 1099PS.

Infrastructure

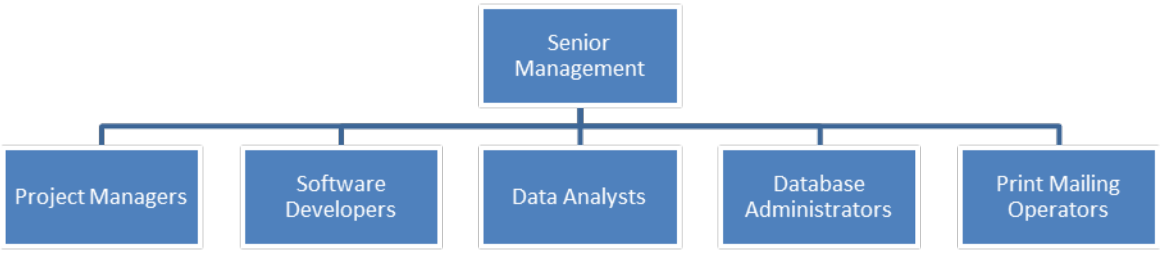
Tab Service's facilities are located in the city of Chicago. There are appropriate security controls limiting physical access to its office space and its on-site data center. Tab Service has several servers and work stations which utilize the Windows Operating System to manage security on the IT resources, applications and data. Tab Service utilizes firewalls and virus detection to monitor its network, application and data.

Software

The 1099PS is comprised of internally and third-party developed applications as described above. Tab Service separately maintains an information technology infrastructure and specific software applications to effectively operate and support 1099PS.

People

Management has developed an organizational structure within each operating unit, which sets forth roles and respective reporting lines for all employees. Each function within the organization aligns its roles to key processes and objectives. This structure is based on the size of the business and its operating activity.



Procedures

Information Security (IS) policies and procedures are formally documented by Senior Management to detail policies and procedures related to system security, confidentiality and processing integrity. The IS policies and procedures are reviewed, updated, and approved by management on a quarterly basis or as changes occur.

Data

The IS policies and procedures formally document policies for classifying data based on its criticality and sensitivity, as well as procedures detailing how classifications are used to define protection requirements, access rights, access restrictions, data retention, and data destruction requirements.

Data is collected from customers through a secure, SSL web-based connection. Tab Service maintains a robust and defined workflow ensuring complete and accurate processing. Tax forms are generated by 1099PS either electronically or paper-based form at the direction of the customer.

Confidentiality Commitments

As noted in management's description, there were no new vendors or contractors incorporated as part of the system during the period December 1, 2017 to May 31, 2018. Therefore, we did not perform any tests of the operating effectiveness of controls related to Confidentiality Criteria 1.4, "The entity obtains confidentiality agreements that are consistent with the entity's confidentiality system requirements from vendors and other third parties whose products and services are part of the system and have access to confidential information."

Section 4. Trust Service Principles and Criteria

Criteria Common to All Security, Processing Integrity and Confidentiality Principles

CC1.0	**Common Criteria Related to Organization and Management**
CC1.1	The entity has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance and monitoring of the system enabling it to meet its commitments and requirements as they relate to security, processing integrity, or confidentiality.
CC1.2	Responsibility and accountability for designing, developing, implementing, operating, maintaining, monitoring, and approving the entity's system controls and other risk mitigation strategies are assigned to individuals within the entity with authority to ensure policies and other system requirements are effectively promulgated and implemented to meet the entity's commitments and system requirements as they relate to security, processing integrity, or confidentiality.
CC1.3	The entity has established procedures to evaluate the competency of personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring the system affecting security, processing integrity, or confidentiality and provides resources necessary for personnel to fulfill their responsibilities.
CC1.4	The entity has established workforce conduct standards, implemented workforce candidate background screening procedures, and conducts enforcement procedures to enable it to meet its commitments and system requirements as they relate to security, processing integrity, or confidentiality.

CC2.0	**Common Criteria Related to Communications**
CC2.1	Information regarding the design and operation of the system and its boundaries has been prepared and communicated to authorized internal and external users of the system to permit users to understand their role in the system and the results of system operation.
CC2.2	The entity's security, processing integrity, or confidentiality commitments are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal users to enable them to carry out their responsibilities.
CC2.3	The responsibilities of internal and external users and others whose roles affect system operation are communicated to those parties.

CC2.4	Information necessary for designing, developing, implementing, operating, maintaining, and monitoring controls, relevant to the security, processing integrity, or confidentiality of the system, is provided to personnel to carry out their responsibilities.
CC2.5	Internal and external system users have been provided with information on how to report security, processing integrity, or confidentiality failures, incidents, concerns, and other complaints to appropriate personnel.
CC2.6	System changes that affect internal and external users' responsibilities or the entity's commitments and system requirements relevant to security, processing integrity, or confidentiality are communicated to those users in a timely manner.

CC3.0	**Common Criteria Related to Risk Management and Design and Implementation of Controls**
CC3.1	The entity (1) identifies potential threats that could impair system security, processing integrity, or confidentiality commitments and system requirements (including threats arising from the use of vendors and other third parties providing goods and services, as well as threats arising from customer personnel and others with access to the system); (2) analyzes the significance of risks associated with the identified threats; (3) determines mitigation strategies for those risks (including implementation of controls, assessment and monitoring of vendors and other third parties providing goods or services, as well as their activities, and other mitigation strategies); (4) identifies and assesses changes (for example, environmental, regulatory, and technological changes and results of the assessment and monitoring of controls) that could significantly affect the system of internal control; and (5) reassesses, and revises as necessary, risk assessments and mitigation strategies based on the identified changes.
CC3.2	The entity designs, develops, implements, and operates controls, including policies and procedures, to implement its risk mitigation strategy, reassesses the suitability of the design and implementation of control activities based on the operation and monitoring of those activities, and updates the controls, as necessary.

CC4.0	**Common Criteria Related to Monitoring of Controls**
CC4.1	The design and operating effectiveness of controls are periodically evaluated against the entity's commitments and system requirements as they relate to security, processing integrity, or confidentiality, and corrections and other necessary actions relating to identified deficiencies are taken in a timely manner.

CC5.0	**Common Criteria Related to Logical and Physical Access Controls**
CC5.1	Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access to meet the entity's commitments and system requirements as they relate to security, processing integrity, or confidentiality.
CC5.2	New internal and external users, whose access is administered by the entity, are registered and authorized prior to being issued system credentials and granted the ability to access the system to meet the entity's commitments and system requirements as they relate to security, processing integrity, or confidentiality. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.
CC5.3	Internal and external users are identified and authenticated when accessing the system components (for example, infrastructure, software, and data) to meet the entity's commitments and system requirements as they relate to security, processing integrity, or confidentiality.
CC5.4	Access to data, software, functions, and other IT resources is authorized and modified or removed based on roles, responsibilities, or the system design and changes to meet the entity's commitments and system requirements as they relate to security, processing integrity, or confidentiality.
CC5.5	Physical access to facilities housing the system (for example, data centers, backup media storage, and other sensitive locations, as well as sensitive system components within those locations) is restricted to authorized personnel to meet the entity's commitments and system requirements as they relate to security, processing integrity, or confidentiality.
CC5.6	Logical access security measures have been implemented to protect against security, processing integrity, or confidentiality threats from sources outside the boundaries of the system to meet the entity's commitments and system requirements.
CC5.7	The transmission, movement, and removal of information is restricted to authorized internal and external users and processes and is protected during transmission, movement, or removal, enabling the entity to meet its commitments and system requirements as they relate to security, processing integrity, or confidentiality.

CC5.8	Controls have been implemented to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity’s commitments and system requirements as they relate to security, processing integrity, or confidentiality.

CC6.0	**Common Criteria Related to System Operations**
CC6.1	Vulnerabilities of system components to security, processing integrity, or confidentiality breaches and incidents due to malicious acts, natural disasters, or errors are identified, monitored, and evaluated, and countermeasures are designed, implemented, and operated to compensate for known and newly identified vulnerabilities to meet the entity’s commitments and system requirements as they relate to security, processing integrity, or confidentiality.
CC6.2	Security, processing integrity, or confidentiality incidents, including logical and physical security breaches, failures, and identified vulnerabilities, are identified and reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity’s commitments and system requirements.

CC7.0	**Common Criteria Related to Change Management**
CC7.1	The entity’s commitments and system requirements, as they relate to security, processing integrity, or confidentiality are addressed during the system development lifecycle, including the authorization, design, acquisition, implementation, configuration, testing, modification, approval, and maintenance of system components.
CC7.2	Infrastructure, data, software, and policies and procedures are updated as necessary to remain consistent with the entity’s commitments and system requirements as they relate to security, processing integrity, or confidentiality.
CC7.3	Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and are monitored to meet the entity’s commitments and system requirements as they relate to security, processing integrity, or confidentiality.
CC7.4	Changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented to meet the entity’s security, processing integrity, or confidentiality commitments and system requirements.

Additional Criteria for Processing Integrity Principles

P1.0	**Additional Criteria for Processing Integrity**
PI1.1	Procedures exist to prevent, or detect and correct, processing errors to meet the entity's processing integrity commitments and system requirements.
PI1.2	System inputs are measured and recorded completely, accurately, and timely to meet the entity's processing integrity commitments and system requirements.
PI1.3	Data is processed completely, accurately, and timely as authorized to meet the entity's processing integrity commitments and system requirements.
PI1.4	Data is stored and maintained completely, accurately, and in a timely manner for its specified life span to meet the entity's processing integrity commitments and system requirements.
PI1.5	System output is complete, accurate, distributed, and retained to meet the entity's processing integrity commitments and system requirements.
PI1.6	Modification of data is authorized, other than routine transaction processing, is authorized and processed to meet with the entity's processing integrity commitments and system requirements.

Additional Criteria for Confidentiality Principles

C1.0	**Additional Criteria for Confidentiality**
C1.1	Confidential information is protected during the system design, development, testing, implementation, and change processes to meet the entity's confidentiality commitments and system requirements.
C1.2	Confidential information within the boundaries of the system is protected against unauthorized access, use, and disclosure during input, processing, retention, output, and disposition to meet the entity's confidentiality commitments and system requirements.
C1.3	Access to confidential information from outside the boundaries of the system and disclosure of confidential information is restricted to authorized parties to meet the entity's confidentiality commitments and system requirements.

C1.4	The entity obtains confidentiality commitments that are consistent with the entity’s confidentiality system requirements from vendors and other third parties whose products and services are part of the system and have access to confidential information.
C1.5	Compliance with the entity’s confidentiality commitments and system requirements by vendors and others third parties whose products and services are part of the system is assessed on a periodic and as-needed basis, and corrective action is taken, if necessary.
C1.6	Changes to the entity’s confidentiality commitments and system requirements are communicated to internal and external users, vendors, and other third parties whose products and services are part of the system.
C1.7	The entity retains confidential information to meet the entity’s confidentiality commitments and system requirements.
C1.8	The entity disposes of confidential information to meet the entity’s confidentiality commitments and system requirements.

plante moran | Audit. Tax. Consulting. Wealth Management.

For more information regarding the report, contact:

Bob Lambert | President
Tab Service Company
312.527.4306
blambert@tabservice.com

For more information on Plante Moran, contact:

Timothy R. Bowling, CPA, CCSK | Partner
Plante & Moran, PLLC
312.980.2927
tim.bowling@plantemoran.com