SOC 3 Report

Report on Rev's Description of its Transcription, Captioning, and Subtitling System and on the Suitability of the Design and Operating Effectiveness of Its Controls Related to Security and Availability Throughout the Period

October 1, 2023 to September 30, 2024

TABLE OF CONTENTS

Acronym Table

➢ AI	Artificial Intelligence
➢ AICPA	American Institute of Certified Public Accountants
➢ AWS	Amazon Web Services
➢ CEO	Chief Executive Officer
➢ CIO	Chief Information Officer
➢ CSO	Chief Security Officer
➢ CTO	Chief Technology Officer
➢ EC2	Elastic Compute Cloud
➢ EKS	Elastic Kubernetes Service
➢ IAM	Identity and Access Management
➢ IT	Information Technology
➢ MFA	Multi-Factor Authentication
➢ RCA	Root Cause Analysis
➢ RDS	Relational Database Service
➢ Rev	Rev.com
➢ S3	Simple Storage Service
➢ SaaS	Software as a Service
➢ SOC	System and Organizational Controls
➢ SVP	Senior Vice President
➢ TSP	Trust Services Principle
➢ VP	Vice President

Section 1

Assertion of Rev's Management

Assertion of Rev's Management

We are responsible for designing, implementing, operating, and maintaining effective controls within Rev's Transcription, Captioning, and Subtitling System throughout the period October 1, 2023 to September 30, 2024, to provide reasonable assurance that Rev 's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (in AICPA, *Trust Services Criteria*). Our description of the boundaries of the system is presented in attachment A 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 October 1, 2023 to September 30, 2024, to provide reasonable assurance that Rev's service commitments and system requirements were achieved based on the applicable trust services criteria. Rev'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 attachment B.

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 October 1, 2023 to September 30, 2024, to provide reasonable assurance that Rev's service commitments and system requirements were achieved based on the applicable trust services criteria.

/s/ Brian Byrne

Chief Security Officer

Rev

February 24, 2025

Section 2

Independent Service Auditors' Report

Independent Service Auditors' Report

To: Rev

Scope

We have examined Rev's accompanying assertion titled "Assertion of Rev's Management" (assertion) that the controls within Rev's Transcription, Captioning, and Subtitling System (system) were effective throughout the period October 1, 2023 to September 30, 2024, to provide reasonable assurance that Rev's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (in AICPA Trust Services Criteria).

Service Organization's Responsibilities

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

Service Auditors' Responsibilities

Our responsibility is to express an opinion, based on our examination, on management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects.

We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

Our examination included the following:

- 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 Rev'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 Rev'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 any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the 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 Rev's Transcription, Captioning, and Subtitling System were effective throughout the period October 1, 2023 to September 30, 2024, to provide reasonable assurance that Rev's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

CBIZ CPA's

CBIZ CPAs P.C.

Tampa, FL
February 24, 2025

Attachment A

Rev's Description of the Boundaries of its Transcription, Captioning, and Subtitling System

Company Overview and Services Provided

Infrastructure

Rev's Transcription, Captioning, and Subtitling System (including rev.com, rev.ai, and VoiceHub) is hosted in AWS, using AWS' cloud infrastructure for production servers and databases. Access to the AWS management console is restricted via a unique username and password, with MFA required for all users. Access to the infrastructure supporting Rev's systems is controlled through the AWS IAM console. Rev's infrastructure is monitored for performance and uptime.

Software

The following provides a summary of the software and related services used in the delivery of the Transcription, Captioning, and Subtitling System services:

- AWS IAM – utilized as a cloud-based identity and access management service
- AWS EC2 – utilized as cloud-based infrastructure provisioning service
- AWS S3 – utilized as cloud-based logging and storage service
- AWS RDS – utilized as cloud-based relational database management system for application data
- AWS DynamoDB – utilized as cloud-based NoSQL database system
- AWS EKS – utilized to manage Rev's cloud-based Kubernetes cluster

People

People involved in the operation and use of the system are:

- Chief Executive Officer (CEO) – responsible for leading the organization and managing the day-to-day operations of Rev.
- Chief Product & Technology Officer (CPTO) – responsible for Rev's overall product vision and design.
- Chief Technology Officer (CTO) – responsible for the system architecture and infrastructure.
- Chief Information Officer (CIO) – responsible for Rev's internal hardware and back-office infrastructure.
- Chief Security Officer (CSO) – responsible for security, security-related compliance, risk management, system security and incident response.
- VP Engineering – responsible for engineering organization and technical talent management.
- VP Operations – manages customer support and observes customer transactions to identify fraudulent activity such as account take over, friendly fraud, theft and similar other risks.
- Security Staff - responsible for day-to-day security operations, including maintaining and enforcing security policies and procedures, monitoring incident and vulnerability alerts, performing regular risk assessments over Rev's environment and key vendors, and maintaining compliance with regulatory and contractual requirements.
- Support and Professional Staff – responsible for providing day-to-day IT operations. Provides internal and external customer support of applications and systems and ensures that systems are maintained and operating as expected.

- Accounting Staff – responsible for the daily maintenance of general ledger balances, including cash held for other accounts, operating cash, accounts receivable, accounts payable, fixed assets, and prepaid expenses; reconciliation of balance sheet accounts to subsidiary ledger balances; assisting in budget preparation; and participation in the formation of policies and procedures.

Processes and Procedures

Rev leadership maintains key policies and standard procedure documents outlining key controls related to the secure operation of Rev's Transcription, Captioning, and Subtitling System. These documents are updated and reviewed at least annually, or as changes are required, and include the following:

- Acceptable Use Policy
- Access Control Policy
- Asset Management Policy
- Change Management Policy
- Data Types & Classification Policy
- Disaster Recovery Policy
- Incident Response Policy
- Information Security Policy
- Internal Audit Policy
- Risk Management Policy
- Vulnerability Management Policy

Data

Data is stored utilizing Amazon RDS and S3 services. Sensitive customer data is maintained only within production databases, or a database with the same security controls as the production environment. Access controls are in place around the database that restrict access to only approved administrators. Rev databases are backed up daily and are continually monitored for performance and uptime.

Any decommissioned physical storage media containing confidential, or copyright information must be destroyed, and non-physical media must be destroyed, deleted, or overwritten using techniques to make the original information non-retrievable, to help ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.

System Boundaries

System boundaries, pertaining to collection, use, retention, disclosure, and disposal or anonymization or personalization of data, are governed by terms of service provisions for particular service engagements.

Subservice Organization

AWS

Rev uses AWS to host its production systems. AWS is responsible for the uptime, management, and logical security of their infrastructure that supports the delivery of production hosting services and environmental conditions that provide power and cooling to their devices. AWS is also responsible for providing physical security controls, administration of their hardware equipment, and reporting any logical or physical security incidents.

On an annual basis, Rev receives AWS's attestation reports in order to review controls at the subservice organization to determine if the appropriate controls were implemented. In the event there are exceptions

or controls not operating effectively at a subservice organization, this risk is incorporated into a risk assessment and appropriate actions are taken to mitigate risks in the future.

Risk Assessment

Rev management has defined a Risk Management Team, comprised of leaders from core business units and members of the executive team, to identify, respond to, and monitor risks to Rev. The Risk Management Team performs an annual risk assessment, which requires management to identify risks in its areas of responsibility and to implement appropriate measures to address those risks. Identified risks and mitigation plans are then tracked by the Risk Management Team on a Risk Register and discussed as part of monthly Risk Management Team meetings. Rev management, including the Risk Management Team, evaluate and re-assess open risks at least annually to determine whether the identified risk or surrounding threat landscape have changed, and update the Risk Register accordingly.

The risk assessment process consists of the following phases:

- Identification – The identification phase includes identifying risks (including threats and vulnerabilities) that exist in the environment. This phase provides a basis for all other risk management activities.
- Assessment – The assessment phase considers the potential impact(s) of identified risks to the business, its likelihood of occurrence, and strategies to minimize or mitigate the risk.
- Mitigation – The mitigation phase includes implementing controls, processes, and other physical and virtual safeguards in place to prevent and detect identified and assessed risks.
- Reporting – The reporting phase results in risk reports provided to managers with the necessary data to make effective business decisions and to comply with internal policies and applicable regulations.
- Monitoring – The monitoring phase includes Rev management performing monitoring activities to evaluate whether processes, initiatives, functions and/or activities are mitigating the risk as designed.

Communication

Rev's CSO conducts quarterly meetings with executive leadership to review internal controls and any deficiencies to those internal controls in addition any proposed corrective action plans. Security incidents are required to be communicated to the security team as soon as the incident has been identified. Incidents are required to be formally documented upon notification. An externally facing service desk portal is available for users to communicate security-related incidents or concerns. .

Internal Communications

Rev has implemented various methods of communication to help employees understand their individual roles and responsibilities, and to communicate significant events within the organization. Security awareness training is included in the Rev' employee training curriculum and is required annually for all employees.

Security events, such as an incident or breach, are required to be reported to the Security team. Incidents will then be investigated, prioritized, and documented in accordance with the Rev Incident Response Policy. As a result of the investigation, a root-cause analysis (RCA) is performed over any critical security incident,

and a corrective action plan or preventative action plan put in place to mitigate or minimize the likelihood of recurrence.

External Communications

Rev has implemented communication methods to help provide assurance that customers understand their roles and responsibilities in communication of significant events. A service desk is available on the company website where clients can communicate any inquiries or security events.

Attachment B

Principal Service Commitments and System Requirements

Principal Service Commitments and System Requirements

Rev designs its processes and procedures related to its Transcription, Captioning, and Subtitling System to meet its objectives. Those objectives are based on the service commitments that Rev makes to user entities, the laws and regulations that govern SaaS providers, and the financial, operational, and compliance requirements that Rev has established for the services.

Security commitments to user entities are documented in appropriate agreements. Security commitments are standardized and include, but are not limited to, the following:

- ➢ Security principles within the fundamental designs of the Transcription, Captioning, and Subtitling System that are designed to permit system users to access the information they need based on the permission of least privilege provisioning.
- ➢ Use of encryption protocols to protect customer data at rest and in transit.
- ➢ Security awareness training on how to implement and comply with Rev's Information Security Program for all employees.
- ➢ Policies and procedures to detect, respond to, and otherwise address security incidents, including procedures to monitor systems and to detect actual and attempted attacks.
- ➢ Policies and procedures for responding to an emergency, disaster, or other threat to the availability of Rev services.

Availability commitments to user entities are documented in appropriate agreements. Availability commitments are standardized and include, but are not limited to, the following:

- ➢ Managing capacity demand through the monitoring and evaluation of current processing capacity and usage rates.
- ➢ Meeting company objectives through authorization, design, development, and monitoring of data backup processes and recovery infrastructure.