Westamerica Communications

System and Organization Controls (SOC) 3 Report

Report on Westamerica Communications, Inc.'s Print, Direct Mail, and Digital Services Relevant to Security

For the period September 1, 2023 to November 30, 2023

Modern Assurance

The report accompanying this description was issued by Modern Assurance, LLC.

Table of Contents

Section I: Independent Service Auditor's Report

Modern Assurance

Independent Service Auditor's Report

To Management of Westamerica Communications, Inc.,

Scope

We have examined Westamerica Communications, Inc.'s (Westamerica's) accompanying assertion, titled "Westamerica Communications, Inc.'s Management Assertion" (assertion) that the controls within Westamerica's Print, Direct Mail, and Digital Services (system) were effective throughout the period September 1, 2023 to November 30, 2023 to provide reasonable assurance that Westamerica'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 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity,* Confidentiality, and Privacy (AICPA, Trust Services Criteria).

The information included within the Boundaries of Westamerica Communications, Inc.'s System (Attachment A) indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Westamerica, to achieve the service commitments and system requirements of Westamerica based on the applicable trust service criteria. 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

Westamerica 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 Westamerica's service commitments and system requirements were achieved. Westamerica has provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Westamerica 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 Auditor's 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.

Our examination included:

- obtaining an understanding of the system and the service organization's service commitments and system requirements.
- assessing the risks that the controls were not effective to achieve Westamerica'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 Westamerica'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.

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

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 were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Westamerica's print, direct mail, and digital services were effective throughout the period September 1, 2023 to November 30, 2023 to provide reasonable assurance that Westamerica's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Modern Assurance, LLC

December 8, 2023
Bend, Oregon

Section II: Westamerica Communications, Inc.'s Management Assertion

Westamerica Communications, Inc.'s Management Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within Westamerica Communications, Inc.'s (Westamerica's) print, direct mail, and digital services (system) throughout the period September 1, 2023 to November 30, 2023 to provide reasonable assurance that Westamerica'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)*. Our description of the boundaries of the system is presented in Attachment A and identifies the aspects of the system covered by our assertion.

The information included within the Boundaries of Westamerica Communications, Inc.'s System (Attachment A) indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Westamerica, to achieve the service commitments and system requirements of Westamerica based on the applicable trust service criteria. Attachment A presents those complementary user entity controls assumed in the design of Westamerica's controls.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period September 1, 2023 to November 30, 2023 to provide reasonable assurance that Westamerica's service commitments and system requirements would be achieved based on the applicable trust services criteria, if user entities applied the complementary controls assumed in the design of Westamerica's controls throughout that period. Westamerica'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 September 1, 2023 to November 30, 2023 to provide reasonable assurance that Westamerica's service commitments and system requirements were achieved based on the applicable trust services criteria.

Attachment A

Boundaries of Westamerica Communications, Inc.'ssystem

Attachment B

Westamerica Communications, Inc.'s Service Commitments and System Requirements

Attachment A: Boundaries of Westamerica Communications, Inc.'s System

Westamerica Communications, Inc.'s Print, Direct Mail, and Digital Services

Overview of the Company and Types of Services Provided

Westamerica Communications, Inc. ("Westamerica" or "the Company") was founded in 1977 and is one of Orange County, California's leading commercial printers. Westamerica services clients across all industries and provides real solutions for its clients communication needs. Its services include design and print strategy, direct mail, packaging, wide-format display graphics, and commercial litho, with expert finishing and fulfillment in-house. Westamerica fulfills its services for clients everywhere from its Orange County location.

Components of the System

Infrastructure

The Print, Direct Mail, and Digital Services is comprised of the following components:

Component	Description	Infrastructure
OTView-Print and SecureUpload, WebFTP client upload portals	Web application for clients to upload and retrieve the data and files needed for services provided by Westamerica	On Premise- HyperV environment
BCC software and Filemaker	Software used to process client data	On Premise- HyperV environment

Software

Westamerica utilizes the following software to support the platform:

Function	Software used
Human resources	Paycom
Password management	1Password
Change management and deployment	NinjaOne
Monitoring and logging	SonicWall
Vulnerability scanning	Qualys, Crowdstrike

Data

Data is classified in accordance with the written Data Classification Policy. The platform ingests customer data through the SecureUpload portal, WebFTP portal, and email. Data is stored in Westamerica's HyperV Environment, including the SQL Server Database and File Server Database. The databases housing sensitive customer data are encrypted at rest **(AC-10)**. Sensitive data is not transmitted outside of Westamerica's environment. The Company uses SHA256 to encrypt confidential and sensitive data when transmitted over public networks **(AC-11)**.

People

Westamerica's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored.

Westamerica has established an organizational structure that includes consideration of key areas of authority and responsibility, as well as appropriate lines of reporting.

Policies

Westamerica has implemented the following policies, which serve as the basis for Company procedures, are made accessible to all relevant employees and contractors, and are reviewed annually:

- Acceptable Use Policy - defines standards for appropriate and secure use of company hardware and electronic systems including storage media, communication tools, and internet access. This policy is acknowledged by new hire employees and contractors upon hire **(ORG-10).**
- Access Control and Termination Policy - governs authentication and access to applications, resources, and tools **(AC-04).**
- Change Management Policy - governs the documentation, tracking, testing, and approving of system, network, security, and infrastructure changes for applications, resources, and tools **(CM-07).**
- Code of Conduct - outlines ethical expectations, behavior standards, and ramifications of non compliance. This policy is acknowledged by new hire employees and contractors upon hire **(ORG-01).**
- Configuration and Asset Management Policy - governs configurations for new applications, resources, and tools **(CM-06).**
- Encryption and Key Management Policy - supports the requirements for secure encryption and decryption of app secrets, and governs the use of cryptographic controls **(AC-12).**
- Information Security Policy - establishes the security requirements for maintaining the security of applications, resources, and tools **(ORG-12).**

- Internal Control Policy - identifies how a system of controls should be maintained to safeguard assets, promote operational efficiency, and encourage adherence to prescribed managerial policies **(ORG-14).**
- Network Security Policy - identifies the requirements for protecting information and systems within and across networks **(NET-06).**
- Performance Review Policy - provides personnel context and transparency into their performance and career development processes **(ORG-15).**
- A Physical Security Policy that details the physical security requirements for the company facilities is accessible to all relevant employees and contractors, and is reviewed annually **(PHYS-01).**
- Risk Assessment and Treatment Policy - governs the process for conducting risk assessments to account for threats, vulnerabilities, likelihood, and impact with respect to assets, team members, customers, vendors, suppliers, and partners **(RA-01).**
- Secure Development Policy - defines the requirements for secure software and system development and maintenance **(CM-08).**
- Security Incident Response Plan - outlines the process of identifying, prioritizing, communicating, assigning, and tracking confirmed incidents through to resolution **(IR-01).**
- Vendor Risk Management Policy - defines a framework for the onboarding and management of the vendor relationship cycle **(RA-04).**
- Vulnerability Management and Patch Management Policy - outlines the processes to identify and respond to vulnerabilities **(VM-01).**

Control Environment

The objectives of internal control as it relates to the print, direct mail, and digital services are to provide reasonable, but not absolute, assurance that controls are suitably designed and operating effectively to meet the relevant control objectives, that assets are protected from unauthorized use or disposition, and that transactions are executed in accordance with management's authorization and client instructions. Management has established and maintains controls designed to monitor compliance with established policies and procedures. The remainder of this subsection discusses the tone at the top as set by management, the integrity, ethical values, and competence of Westamerica employees, the policies and procedures, the risk management process and monitoring, and the roles of significant control groups. The internal control structure is established and refreshed based on Westamerica's assessment of risk facing the organization.

Integrity and ethical values are essential elements of the control environment, affecting the design, administration and monitoring of key processes. Integrity and ethical behavior are the products of Westamerica's ethical and behavioral standards, how they are communicated, and

how they are monitored and enforced in its business activities. They include management's actions to remove or reduce incentives/pressures, and opportunities that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of the entity's values and behavioral standards to personnel through policy statements and Code of Conduct, and by the examples the executives set. Westamerica's executive management recognizes their responsibility to foster a strong ethical environment within Westamerica to determine that its business affairs are conducted with integrity, and in accordance with high standards of personal and corporate conduct. This responsibility is characterized and reflected in the Code of Conduct, which is distributed to all applicable personnel of the organization.

Risk Assessment Process

Westamerica has defined a risk management framework for evaluating information security risk and other relevant forms of business risk. A formal risk assessment is performed at least annually to identify, update, and assess relevant internal and external threats related to security, which also considers the potential for fraud **(RA-02).** A risk register is maintained to record the risk mitigation strategies for identified risks, and to track the development or modification of controls consistent with the risk mitigation strategy **(RA-03).**

Monitoring Activities

Westamerica performs several types of monitoring to assess the security of health of the in-scope environment and the related controls. The company leverages a continuous monitoring solution that monitors internal controls used in the achievement of service commitments and system requirements. The tool identifies instances of non-compliance for management to resolve **(ORG-05).**

Logging is enabled and monitoring software is configured to collect metrics from ingested logs to detect potential security threats, unusual system activity, and monitor system performance, as applicable **(NET-04).** Alerting software is used to notify impacted teams of potential security events, and identified events are tracked to resolution **(NET-05).** The Security Steering Committee meets quarterly to coordinate security initiatives and review network security, management of infrastructure and discuss security risks **(NET-07)**. Virtual machines that intake files are configured with antivirus scanning **(NET-09).**

Incident Response

The Company employs multiple mechanisms to identify potential security incidents as discussed in the *Communication* and *Monitoring* sections above. Confirmed incidents are documented, tracked, and responded to according to the Security Incident Response Plan **(IR-02).** Following an incident, a 'lessons learned' document is created and shared with relevant internal personnel to make any required changes **(IR-03).** The Security Incident Response Plan is tested annually to assess effectiveness, and management makes changes to the Security Incident Response Plan based on the test results **(IR-04).**

Complementary User Entity Controls

The following user entity controls are assumed to be implemented by user entities and are necessary for the service organization's service commitments and system requirements to be achieved.

User Entity Control
User entities are responsible for understanding and complying with their contractual obligations to Westamerica.
User entities are responsible for removing personal data from the files sent to Westamerica.
User entities are responsible for maintaining the data needed for (used in) projects.
User entities are responsible for only sending data via the secure methods provided by Westamerica.

Attachment B: Westamerica Communications, Inc.'s Service Commitments and System Requirements

Westamerica Communications, Inc.'s Service Commitments and System Requirements

Westamerica and its customers have a shared responsibility in maintaining the security of the print, direct mail, and digital services. Westamerica has established principal service commitments, which are communicated via service agreements and consist of the following:

- Defines and documents roles and responsibilities related to the Company's Information Security Program and the protection of customer data. Requires team members to review and accept all of the security policies.
- Requires team members to go through employee security awareness training covering industry standard practices and information security topics such as phishing and password management.
- Performs background checks on all new team members in accordance with local laws.
- Maintains commercially reasonable administrative and technical controls to protect data stored in its servers from unauthorized access, accidental loss, or unauthorized modification.
- Requires all team members to adhere to a minimum set of password requirements and complexity for access, and utilizes 2-factor authentication (2FA) where available.
- Encrypts all databases at rest.
- Implements network intrusion detection tools and firewalls.
- Undergoes at least annual risk assessments to identify any potential threats, including considerations for fraud.
- Establishes a process for handling information security events which includes escalation procedures, rapid mitigation and communication.

Westamerica has established system requirements, which are communicated via service agreements and consist of the following:

- Employee provisioning and deprovisioning standards
- User access reviews
- Logical access controls, such as the use of user IDs and passwords to access systems
- Encryption standards for data at rest and in transit
- Incident response plan