affinity

REPORT ON CONTROLS RELEVANT TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY

SOC 3

linford&co llp
cpa firm

linford&co llp
cpa firm

▪ linford&co llp
1550 wewatta st, 2nd floor
denver, co 80202

▪ tel: +1 (720) 330 7201
email: info@linfordco.com
www.linfordco.com

Section I – Independent Service Auditor's Report

To the Board of Directors of Project Affinity, Inc.:

Scope

We have examined Project Affinity, Inc.'s (Affinity or the Company) accompanying assertion titled "Assertion of Affinity Management" (assertion) that the controls within Affinity's relationship intelligence services (system) were effective throughout the period November 1, 2021 to October 31, 2022 to provide reasonable assurance that Affinity's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality 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

Affinity 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 Affinity's service commitments and system requirements were achieved. Affinity has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Affinity 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 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 service organization's service commitments and system requirements.
- ✓ Assessing the risks that controls were not effective to achieve Affinity'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 Affinity'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 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 Affinity's relationship intelligence services were effective throughout the period November 1, 2021 to October 31, 2022 to provide reasonable assurance that Affinity's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

linford&co llp

November 14, 2022
Denver, Colorado

Section II – Assertion of Affinity Management

November 14, 2022

We are responsible for designing, implementing, operating, and maintaining effective controls within Project Affinity, Inc.'s (Affinity or the Company) relationship intelligence services throughout the period November 1, 2021 to October 31, 2022, to provide reasonable assurance that Affinity's service commitments and system requirements relevant to security, availability, and confidentiality 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 prepared an evaluation of the effectiveness of the controls within the system throughout the period November 1, 2021 to October 31, 2022 to provide reasonable assurance that Affinity's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). Affinity'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 III.

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 November 1, 2021 to October 31, 2022, to provide reasonable assurance that Affinity's service commitments and system requirements were achieved based on the applicable trust services criteria.

Peter Romano

Peter Romano
Chief Information Security Officer

Section III – Project Affinity's Description of Its Relationship Intelligence Services

Overview of Operations

Project Affinity, Inc. develops network and customer relationship management solutions for enterprises. Its solutions feature relationship management, email detection, network search, network intelligence, automatic data capture, collaboration and reminders, and a browser extension. The Company was founded in 2014 and is based in San Francisco, California.

Components of the System Used to Provide the Services

The system used by Affinity to deliver its relationship intelligence services is comprised of a combination of components that include the products and the data processed, but also extends to the underlying infrastructure, the subservice organization's hosting services, the Company's employees and contractors, as well as the policies and procedures followed to maintain the security, availability, and confidentiality of Affinity's services and client data. The following is a summary of the components that comprise the system. Specific processes and controls relevant to the security criteria are described in the remainder of this section of the report.

Infrastructure

Subservice Organizations: Affinity uses subservice organizations to achieve operating efficiency and to obtain specific expertise. The following are the principal subservice organizations used by Affinity:

- ✓ **Amazon Web Services (AWS)** – AWS hosts Affinity's production IT environment and provides certain managed services including firewall management and data backup services. AWS undergoes an annual Type II SOC 2 examination and the report may be obtained directly from them. Affinity obtains and reviews the SOC 2 report provided by AWS related to their hosting operations to determine whether controls are designed and operating effectively AWS. Additionally, any listed complementary user entity controls in the AWS SOC reports are also reviewed and addressed by Affinity.

Software

Affinity's relationship intelligence services are enabled by its privately owned applications, and the use of reputable and SOC examined third party tools and applications. The relationship intelligence services are supported by Affinity's applications, servers, and tools. The Affinity applications are run on Windows servers and are developed and maintained by Affinity's IT personnel and third-party resources. Role-based access controls govern the capabilities employees and users can execute within the Affinity applications and tools.

People
Affinity has a staff of personnel organized into functional areas so personnel understand their responsibilities within the organization.

Data
Client data is stored within Affinity's production database instances in their colocation facilities. Affinity has implemented security controls to protect the confidentiality of the data. Client data within the databases is encrypted at rest. Additionally, all data transfers between users and Affinity are secured using Transport Layer Security and industry standard encryption.

Processes and Procedures
Affinity has established and maintains security policies and procedures over the relationship intelligence services. Affinity makes these internal policies and procedures, including security policies, available to its personnel on its internal shared drives to provide direction regarding their responsibilities related to the functioning of internal control.

Principal Service Commitments and System Requirements

Affinity designs its processes and procedures to meet objectives for its relationship intelligence services. Those objectives are based on the service commitments that Affinity makes to user entities and the compliance requirements that Affinity has established for their services.

Security, availability, and confidentiality commitments to user entities are documented and communicated in their customer agreements, as well as in the description of the service offering provided online. Security, availability, and confidentiality commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental design of the relationship intelligence services are implemented 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.
- Controlled access to the production environment and the supporting infrastructure.
- Segregation of client data.
- Monitoring of system performance metrics and critical application services.
- Developing, implementing, and testing activities to recover from events or incidents that may disrupt client services or system availability.
- Identify, designate, and protect confidential data against unauthorized access and dissemination.

Affinity establishes operational requirements that support the achievement of security, availability, and confidentiality commitments and other system requirements. Such requirements are communicated in Affinity 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 networks are managed, and how employees are hired and trained.