SOC 3 Report
For EntityScan AI LLC

An Independent Service Auditor's Report
on Controls Relevant to Security
January 15, 2026 to April 15, 2026

AUDIT AND ATTESTATION BY

PRESCIENT
ASSURANCE

Prescient Assurance LLC.
1900 Church Street, Suite 300
Nashville, TN, 37203

CPA

www.prescientassurance.com
info@prescientassurance.com
+1 646 209 7319

Table of Contents

Management's Assertion 4
Attachment A **6**
Company Overview and Types of Products and Services Provided 7
COMPANY BACKGROUND 7
DESCRIPTION OF SERVICES OVERVIEW OR SERVICES PROVIDED 7
The components of the system used to provide the services 7
Primary Infrastructure 7
Primary Software 8
People 8
Security Processes and Procedures 9
Physical Security 9
Logical Access 9
Computer Operations - Backups 9
Computer Operations - Availability 10
Change Management 10
Data Communications 10
Data 10
System Boundaries 11
Complementary Subservice Organization Controls (CSOCs) 12
Complementary User Entity Controls (CUECs) 12
Attachment B **13**
The principal service commitments and system requirements 14
Independent Service Auditor's Report **16**
Scope 16
Service Organization's Responsibilities 16
Service Auditor's Responsibilities 16
Inherent Limitations 17
Opinion 17



SECTION 1

Management's Assertion

EntityScan AI

AI-Powered Borrower Entity Document Analysis

Management's Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within EntityScan AI LLC's ("EntityScan AI") EntityScan AI Platform (the system) throughout the period January 15, 2026, to April 15, 2026, to provide reasonable assurance that EntityScan AI LLC's service commitments and system requirements relevant to Security were achieved. 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 controls within the system throughout the period January 15, 2026, to April 15, 2026, to provide reasonable assurance that EntityScan AI LLC'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, in AICPA Trust Services Criteria (With Revised Points of Focus - 2022). EntityScan AI LLC'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.

EntityScan AI LLC uses a subservice organization for cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at EntityScan AI LLC, to achieve EntityScan AI LLC's service commitments and system requirements based on the applicable trust services criteria. The description presents EntityScan AI LLC's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of EntityScan AI LLC's controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at EntityScan AI LLC, to achieve EntityScan AI LLC's service commitments and system requirements based on the applicable trust services criteria. The description presents EntityScan AI LLC's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of EntityScan AI LLC's controls.

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.

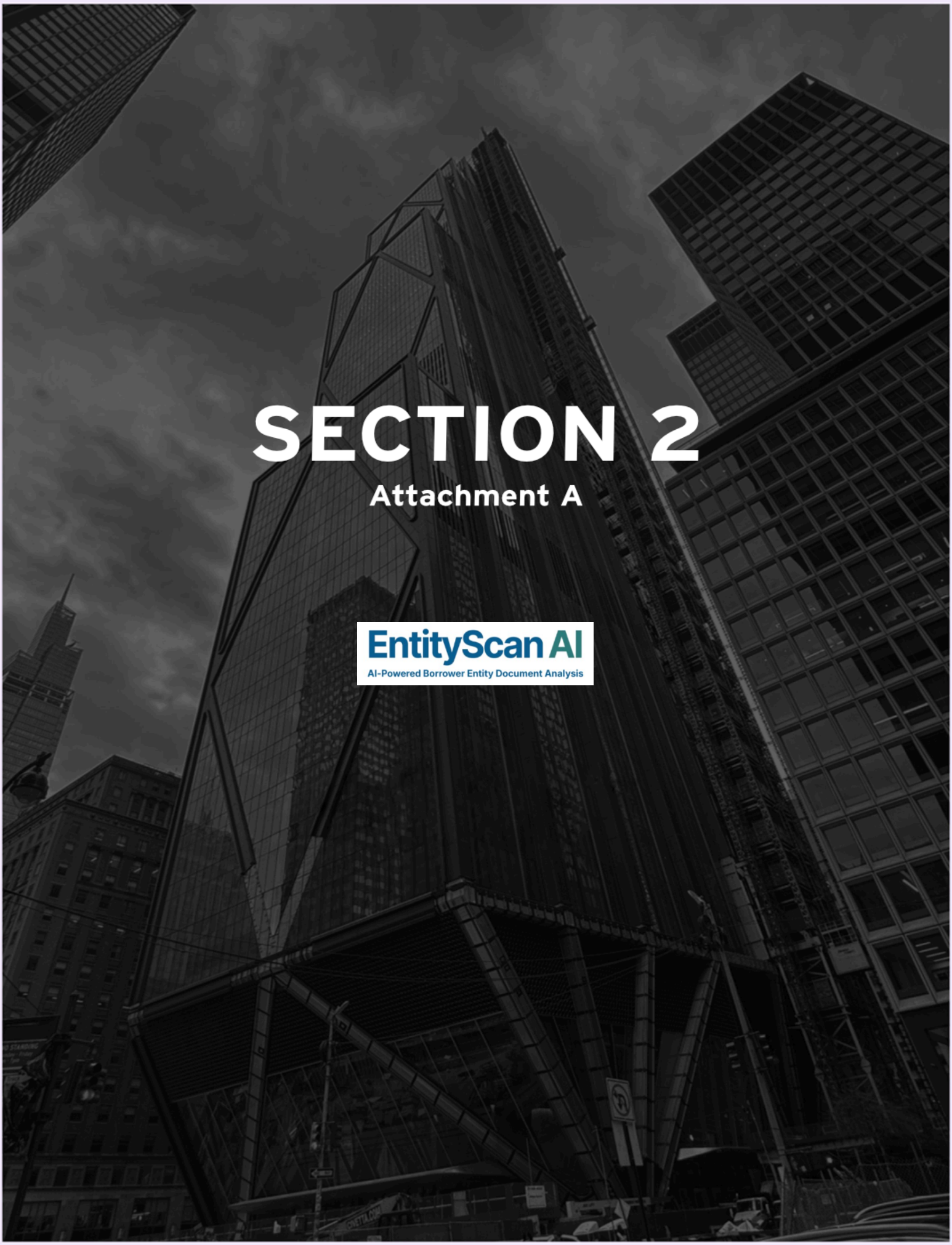
We assert that the controls within the system were effective throughout the period January 15, 2026, to April 15, 2026, to provide reasonable assurance that EntityScan AI LLC's service commitments and system requirements were achieved based on the applicable trust services criteria.

Signed by:
Gary Highland
0C9DE74AF18F479...

Gary Highland

CEO

EntityScan AI LLC



SECTION 2

Attachment A

EntityScan AI

AI-Powered Borrower Entity Document Analysis

Company Overview and Types of Products and Services Provided

Company Background

EntityScan AI LLC ("EntityScan" or "EntityScan AI" or the "Company") is a financial technology company that provides software to support lenders during underwriting and loan closing for business borrowers. EntityScan AI LLC is headquartered in Newport Coast, California, with no additional office locations, and it conducts business with customers in the United States. EntityScan AI operates in the lending and financial services industry and provides subscription access to its cloud-based platform, along with customer onboarding and support services for implementation and ongoing use.

Description Of Services Overview Or Services Provided

EntityScan AI's primary service, EntityScan AI, is a cloud-based software platform that analyzes borrower business-entity documents and produces a structured report used in lending workflows. The system is designed for financial institutions and private lenders that originate or service loans to business entities such as limited liability companies and corporations. Users upload borrower entity documents through the EntityScan AI customer portal, and the system generates an EntityScan report that extracts and summarizes entity information and highlights document-related risks relevant to underwriting and closing (for example, missing approvals, inconsistencies, or authority-related documentation gaps). Core features include customer administrators adding and managing their own users and deactivating a user immediately, without contacting EntityScan AI, secure user authentication, role-based access controls, encrypted transmission and storage of customer-uploaded documents, and audit logging of user and system activity. Common use cases include streamlining borrower entity document review during loan origination, identifying exceptions that require follow-up verification or documentation before closing, and standardizing internal review processes to reduce turnaround time and operational risk.

The components of the system used to provide the services

Primary Infrastructure

Microsoft Azure provides the cloud infrastructure used to host the organization's applications and data. EntityScan AI maintains a system inventory that includes virtual machines, computers (desktops and laptops), and cloud resources. The inventory documents device name, inventory type, description and owner. EntityScan AI LLC leverages Microsoft Azure as its cloud service provider.

Infrastructure	Type	Purpose
Microsoft Azure	Cloud Hosting Service	Provides the underlying cloud infrastructure for EntityScan AI

Primary Software

EntityScan AI is responsible for managing the development and operation of the EntityScan AI Platform including infrastructure components such as servers, databases, and storage systems. The in-scope infrastructure and software components are shown in the table provided below:

System/ Application	Type	Purpose
Microsoft Entra ID	SaaS	User authentication, identity management, and MFA
Microsoft Power Apps	SaaS	Supports internal or user-facing business application functions, where enabled
Microsoft 365	SaaS	Business productivity, collaboration, and administrative support
Microsoft Power Automate	SaaS	Automates workflows and exchanges data between authorized application components
OpenAI	SaaS	Process prompts generated in Power Automate flows, which analyze legal entity documents such as LLC operating agreements, articles of organization, and bylaws.

People

EntityScan AI LLC employs dedicated team members to handle major product functions, including operations, and support. The CEO monitors the environment, as well as manages data backups and recovery. EntityScan AI LLC focuses on hiring the right people for the right job as well as training them both on their specific tasks and on the ways to keep the company and its data secure.

EntityScan AI has a staff of approximately 3 organized in the following functional areas:

Management: Individuals who are responsible for enabling other employees to perform their jobs effectively and for maintaining security and compliance across the environment. This includes:

- CEO - Gary Highland
- Director of Sales & Marketing - Meredith MacIver

Operations: Responsible for maintaining the availability of production infrastructure and managing access and security for production infrastructure. Only members of the Operations team have access to the production environment. Members of the Operations team may also be members of the Engineering team.

Engineering: Responsible for managing laptops, software, and other technology involved in employee productivity and business operations.

Product Development: Responsible for the development, testing, deployment, and maintenance of the source code for the system. Responsible for the product life cycle, including adding additional product functionality.

Due to the organization's size, certain responsibilities are performed by the same individual. Management has evaluated the associated risks and implemented compensating controls appropriate to the organization's size and complexity.

Security Processes and Procedures

Management has developed and communicated policies and procedures to manage the information security of the system. Changes to these procedures are performed annually and authorized by management, the executive team, and control owners. These procedures cover the following key security life cycle areas:

- Physical Security
- Logical Access
- Backups
- Availability
- Change Control
- Data Communications

Physical Security

EntityScan AI's production servers are maintained by Microsoft Azure. The physical and environmental security protections are the responsibility of Microsoft Azure. EntityScan AI reviews the attestation reports and performs a risk analysis of Microsoft Azure on at least an annual basis.

Logical Access

EntityScan AI provides employees and contractors access to infrastructure via a role-based access control system, to ensure uniform, least privilege access to identified users and to maintain simple and repeatable user provisioning and deprovisioning processes.

Access to these systems is split into admin roles, user roles, and no access roles. User access and roles are reviewed on a quarterly basis to ensure least privilege access. Management is responsible for provisioning access to the system based on the employee's role and performing a background check. The employee is responsible for reviewing EntityScan AI's policies, completing security training. These steps are required to be completed within 30 days of hire. When an employee is terminated, Management is responsible for deprovisioning access to all in scope systems within 3 business days of that employee's termination.

Computer Operations - Backups

Customer data is backed up and monitored by the engineering team for completion and exceptions. If there is an exception, the CEO will perform troubleshooting to identify the root cause and either rerun the backup or include it as part of the next scheduled backup job. Backup infrastructure is maintained in Microsoft Azure with physical access restricted according to the policies. Backups are encrypted, with access restricted to key personnel.

Computer Operations - Availability

EntityScan AI maintains an incident response plan to guide employees on reporting and responding to any information security or data privacy events or incidents. Procedures are in place for identifying, reporting and acting upon breaches or other incidents. EntityScan AI internally monitors all applications, including the web UI, databases, and cloud storage to ensure that service delivery matches internal policy requirements.

Change Management

EntityScan AI maintains documented change management and secure development practices to support the implementation of application and infrastructure changes. Changes are reviewed, tested, and approved in accordance with the Operations Security Policy prior to deployment to production. Changes are tracked using the organization's approved development workflow, which may include the source code repository, ticketing system, CI/CD platform, or other engineering tools, as appropriate.

Production, staging, and development environments are logically segregated, and version control software is used to maintain source code history, support collaboration, and facilitate rollback when necessary. Quality assurance testing and User Acceptance Testing (UAT) results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

Data Communications

EntityScan AI communicates through Microsoft-managed cloud services and does not operate a traditional internal network. Users connect to the public Power Pages portal over the internet using HTTPS with TLS 1.2 or later. Authentication is performed through Microsoft Entra ID, with multi-factor authentication required. After authentication and authorization, the portal exchanges application data with Microsoft Dataverse through protected Power Platform service connections. Power Automate, Power Apps, and any approved Microsoft Azure Functions communicate with Dataverse or other authorized services using authenticated, encrypted connections. Data is encrypted both in transit and at rest, and Dataverse role-based and row-level security limited users to records they own or are explicitly permitted to access. Backend services are not directly exposed to the public internet. Microsoft provides the underlying boundary protection, traffic filtering, DDoS mitigation, logical segregation, monitoring, redundancy, and failover controls for the Microsoft Azure and Power Platform environment.

Data

Data as defined by EntityScan AI, constitutes the following:

Customer Data consists of borrower entity documents uploaded by customers (such as articles of organization or incorporation, operating agreements, bylaws, partnership agreements, and related governing documents), the information extracted from those documents, and the EntityScan reports generated from them. These documents may contain personal information about borrower principals,

such as names, addresses, titles, and ownership interests. The system also stores limited user account information (such as work email addresses, usernames, and authentication-related data) required to authenticate users, manage access permissions, and administer customer accounts.

Data is categorized in the following major types of data used by EntityScan AI

Category	Description	Examples
Public	Public information is not confidential and can be made public without any implications for EntityScan AI.	• Press releases • Public website
Internal	Access to internal information is approved by management and is protected from external access.	• Internal memos • Design documents • Product specifications • Correspondences
Customer data	Information received from customers for processing or storage by EntityScan AI. EntityScan AI upholds the highest possible levels of integrity, confidentiality, and restricted availability for this information.	• Customer operating data • Customer PII • Customers' customers' PII • Anything subject to a confidentiality agreement with a customer
Company data	Information collected and used by EntityScan AI. EntityScan AI upholds the highest possible levels of integrity, confidentiality, and restricted availability for this information.	• Legal documents • Contractual agreements • Employee PII • Employee salaries

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer agreements, policies and terms and conditions. Customer Data is captured which is utilized by EntityScan AI LLC in delivering its services. All personnel and contractors of EntityScan AI are obligated to respect and, in all cases, to protect customer data. Additionally, EntityScan AI has policies and procedures in place for proper and secure handling of customer data. These policies and procedures are reviewed on at least an annual basis.

System Boundaries

The boundaries of the EntityScan AI Platform are the specific aspects of the EntityScan AI's infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of the EntityScan AI Platform.

This report does not include the Cloud Hosting Services provided by Microsoft Azure at multiple facilities.

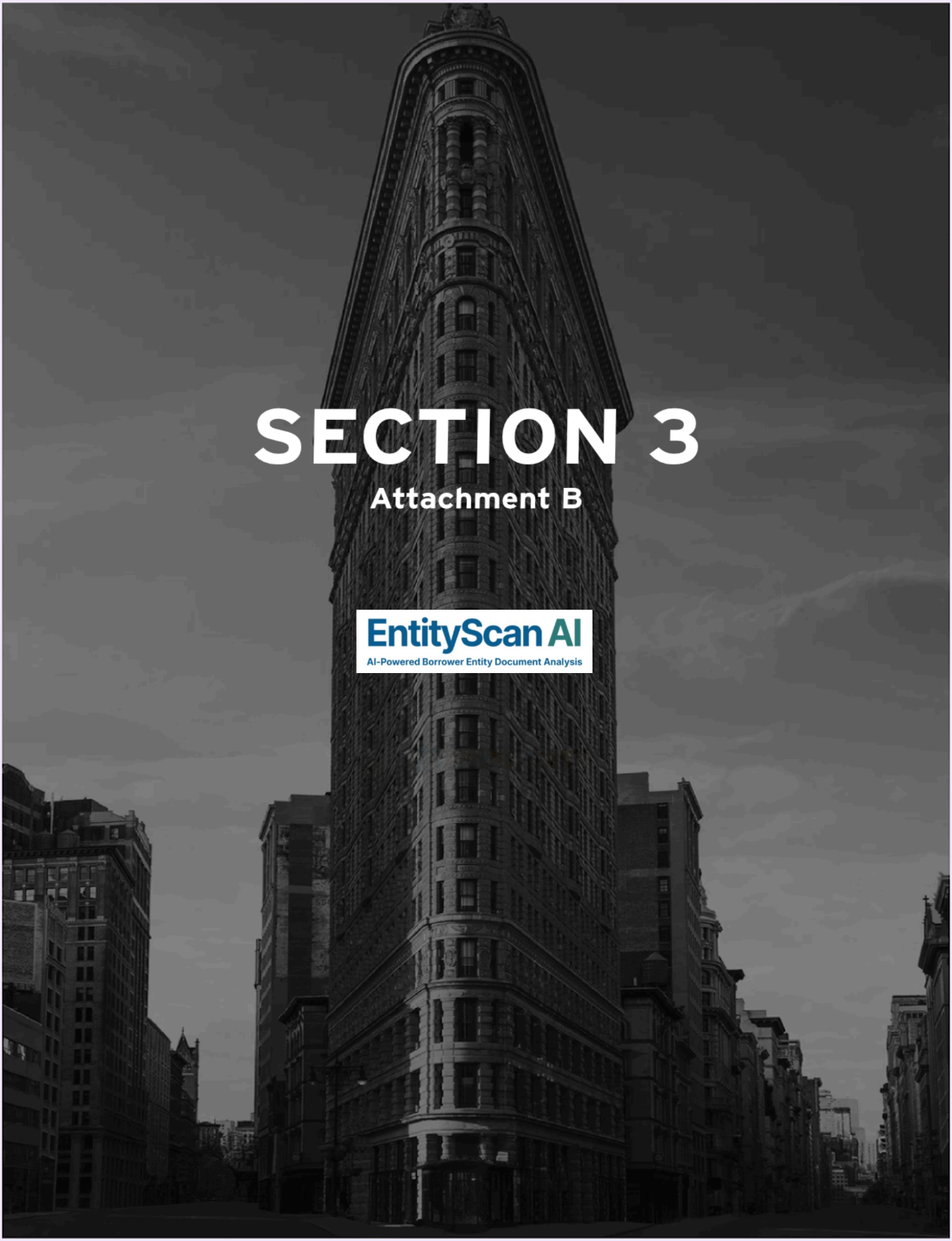
Complementary Subservice Organization Controls (CSOCs)

EntityScan AI LLC uses Microsoft Azure as a subservice organization for cloud infrastructure hosting. EntityScan AI LLC.'s controls related to their system cover only a portion of the overall internal control for each user entity of the System. The description does not extend to the services provided by the subservice organization that provides colocation services for IT infrastructure.

Although the subservice organization has been "carved out" for the purposes of this report, certain Trust Services Criteria are intended to be met by controls at the subservice organization. Complementary Subservice Organization Controls (CSOCs) are expected to be in place at Microsoft Azure related to physical security and environmental protection, as well as backup, recovery, and redundancy controls related to availability. Microsoft Azure physical security controls mitigate the risk of fires, power loss, climate, and temperature variabilities. Management of EntityScan AI LLC receives and reviews the Microsoft Azure SOC 2 report annually. In addition, through its operational activities, EntityScan AI LLC management monitors the services performed by Microsoft Azure to determine whether operations and controls expected to be implemented at the subservice organization are functioning effectively. Management also has communication with the subservice organization to monitor compliance with the service agreement, stay abreast of changes planned at the hosting facility, and relay any issues or concerns to Microsoft Azure management.

Complementary User Entity Controls (CUECs)

Complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at EntityScan AI LLC, to achieve EntityScan AI LLC's service commitments and system requirements based on the applicable trust services criteria.

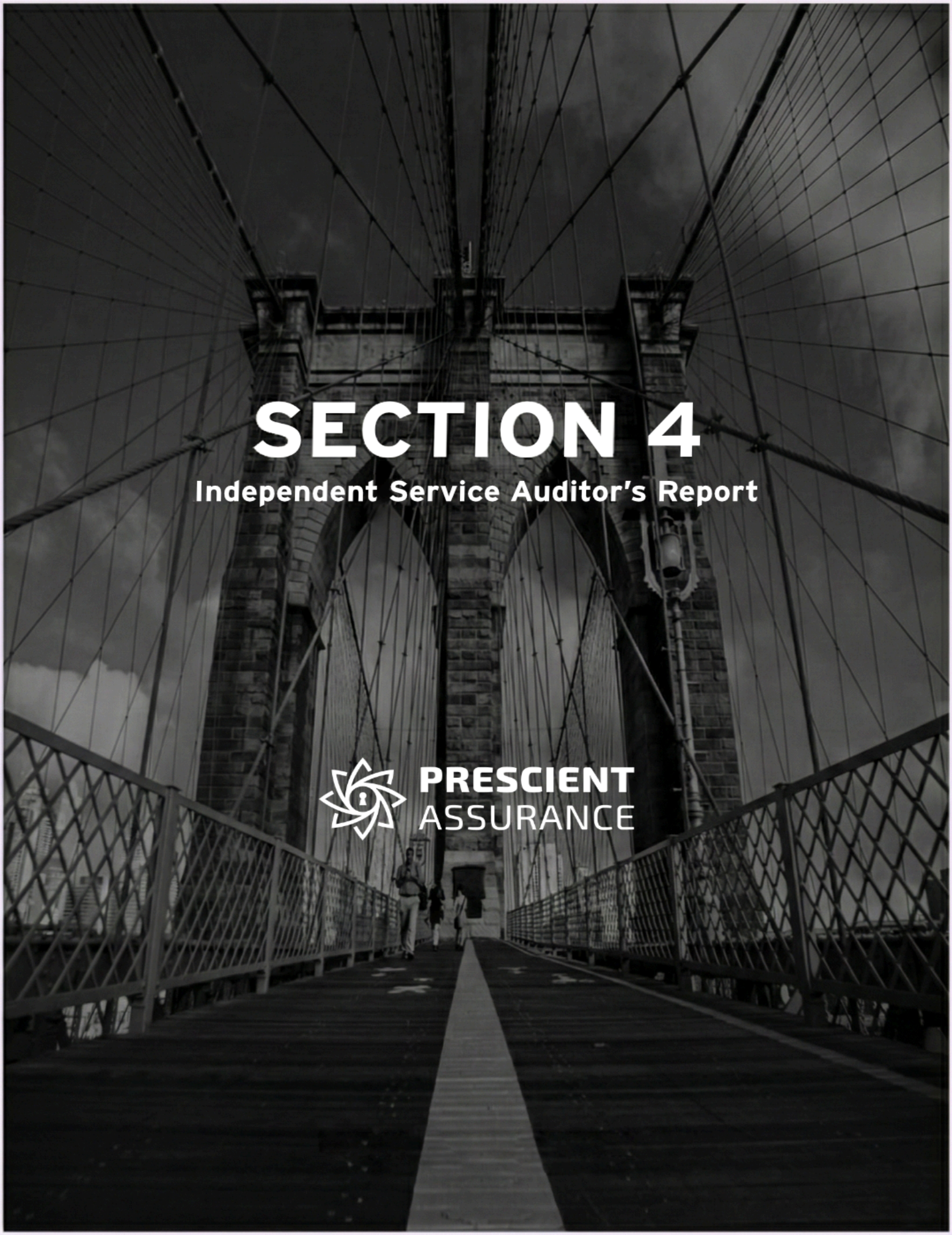

SECTION 3
Attachment B
EntityScan AI
AI-Powered Borrower Entity Document Analysis

The principal service commitments and system requirements

EntityScan AI designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that EntityScan AI makes to user entities, the laws, and regulations that govern the provision of the services, and the financial, operational, and compliance requirements that EntityScan AI has established for the services. The system services are subject to the security commitments established internally for its services. EntityScan AI's commitments to users are communicated through its online Terms of Service, online Privacy Policy and in the description of the service offering provided online.

Security commitments include, but are not limited to, the following:

- System features and configuration settings designed to authorize user access while restricting unauthorized users from accessing information not needed for their role.
- Use of logical segregation and application-level access controls to prevent customers from accessing data belonging to other customers.
- Use of intrusion detection and monitoring capabilities to identify and respond to potential security threats.
- Annual penetration testing of the production environment.
- Operational procedures for managing security incidents and breaches, including notification procedures.
- Use of encryption technologies to protect customer data both at rest and in transit.
- Use of data retention and secure data disposal practices.



SECTION 4

Independent Service Auditor's Report

PRESCIENT ASSURANCE

Independent Service Auditor's Report

To: EntityScan AI LLC

Scope

We have examined EntityScan AI LLC's ("EntityScan AI") accompanying assertion in Section 1, titled "Management's Assertion" (the assertion) that the controls within EntityScan AI LLC's EntityScan AI Platform (the system) were effective throughout the period January 15, 2026, to April 15, 2026, to provide reasonable assurance that EntityScan AI LLC'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, in AICPA Trust Services Criteria (With Revised Points of Focus - 2022).

EntityScan AI LLC uses a subservice organization for cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at EntityScan AI LLC, to achieve its service commitments and system requirements based on the applicable trust services criteria. The description presents EntityScan AI LLC's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of EntityScan AI LLC's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that certain complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at EntityScan AI LLC, to achieve EntityScan AI LLC's service commitments and system requirements based on the applicable trust services criteria. The description presents EntityScan AI LLC's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of EntityScan AI LLC's controls. 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 complementary user entity controls.

Service Organization's Responsibilities

EntityScan AI LLC 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 EntityScan AI LLC's service commitments and system requirements were achieved. In Section 1, EntityScan AI LLC has provided the accompanying assertion about the effectiveness of the controls within the system. When preparing its assertion, EntityScan AI LLC 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.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the 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 the controls were not effective to achieve EntityScan AI LLC'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 EntityScan AI LLC'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 risks 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 EntityScan AI LLC's EntityScan AI Platform were effective throughout the period January 15, 2026, to April 15, 2026, to provide reasonable assurance that EntityScan AI LLC's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Signed by:
Prescient Assurance
3E21CA8A15DE434...

Prescient Assurance LLC

Nashville, TN

October 9, 2026