HaystackID, LLC
Chicago, IL

System and Organization Controls Report Relevant to the Discovery Management System

SOC 3® Report

August 1, 2023 to July 31, 2024

The report, including the title page, table of contents, and sections, constitutes the entire report and should be referred to only in its entirety and not by its component parts. The report contains proprietary information and is considered confidential.

HaystackID, LLC

SOC 3 Report

August 1, 2023 to July 31, 2024

Table of Contents

Section 1
HaystackID, LLC’s Assertion

HAYSTACK

HaystackID, LLC's Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within HaystackID, LLC's (HaystackID) Discovery Management System (the "system") throughout the period August 1, 2023 to July 31, 2024, to provide reasonable assurance that HaystackID's service commitments and system requirements relevant to security, availability, processing integrity, confidentiality, and privacy 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 the controls within the system throughout the period August 1, 2023 to July 31, 2024, to provide reasonable assurance that HaystackID's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy (the "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*). HaystackID'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 August 1, 2023 to July 31, 2024, to provide reasonable assurance that HaystackID's service commitments and system requirements were achieved based on the applicable trust services criteria.

Section 2
Independent Service Auditor’s Report

WIPFLI

Independent Service Auditor’s Report

Management of HaystackID, LLC
Chicago, IL

Scope

We have examined HaystackID, LLC’s (“HaystackID”) accompanying assertion titled "HaystackID, LLC’s Assertion" (the “assertion”) that the controls within HaystackID’s Discovery Management System (the “system”) were effective throughout the period August 1, 2023 to July 31, 2024, to provide reasonable assurance that HaystackID’s service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy (the “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*).

Service Organization’s Responsibilities

HaystackID 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 HaystackID’s service commitments and system requirements were achieved. HaystackID has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, HaystackID 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 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 HaystackID’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 HaystackID’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 HaystackID's Discovery Management System were effective throughout the period August 1, 2023 to July 31, 2024, to provide reasonable assurance that HaystackID's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Wipfli LLP

Wipfli LLP

Atlanta, Georgia
August 29, 2024

Attachment A – Description of the Boundaries of HaystackID, LLC's Discovery Management System

Attachment A – Description of the Boundaries of HaystackID, LLC's Discovery Management System

General Overview

HaystackID solves complex data challenges related to legal, compliance, regulatory, and cyber events. Core offerings include Global Advisory, Data Discovery Intelligence, HaystackID Core® Platform, and AI-enhanced Global Managed Review powered by its proprietary platform, ReviewRight®. Repeatedly recognized as one of the world's most trusted legal industry providers by prestigious publishers such as Chambers, Gartner, IDC, and Legaltech News, HaystackID implements innovative cyber discovery, enterprise solutions, and legal and compliance offerings to leading companies and legal practices around the world. HaystackID offers highly curated and customized offerings while prioritizing security, privacy, and integrity. For more information about how HaystackID can help solve unique legal enterprise needs, please visit HaystackID.com.

Headquartered in Chicago, IL, HaystackID has served the legal industry since 2011. The Company also maintains additional offices and data centers in the United States and in Europe.

Infrastructure

HaystackID operates its IT infrastructure to maximize security, availability, confidentiality, process integrity, privacy, and service delivery performance. HaystackID leverages third-party colocation services from Equinix, Centersquare (Cyxtera), and Digital Realty (Interxion). These locations are configured in pairs to provide power, HVAC, fire suppression, and physical security to the data center. Each U.S. data center is Uptime Institute Tier III certified for high availability and disaster recovery. European Union (EU) data centers are International Organization for Standardization (ISO) 22301 certified for high availability and disaster recovery.

HaystackID data centers are ISO 27001 certified and have been subject to SOC 2 audits as well. HaystackID's Security team obtains and reviews third parties' ISO 27001 and SOC reports to evaluate the internal control environments and the impact of exceptions noted for relevant HaystackID controls.

Inside each data center, HaystackID deploys VMware hosts, switches, firewalls, Structured Query Language (SQL), and web servers in an N+1 or more configuration to help enable automated failover, which helps prevent availability disruptions.

HaystackID creates storage area network (SAN) volumes and virtual file servers and network-attached storage (NAS) shares at the client/case level and SQL databases at the case level to help enforce least-privilege access and help ensure the highest level of confidentiality. HaystackID performs scheduled SAN/NAS snapshots and replicas at predetermined intervals to address threats to data integrity.

HaystackID deploys redundant high-speed network connectivity among its data centers, its corporate headquarters, and its strategic offices.

HaystackID uses SAN to SAN replication of SQL volumes and servers and NAS to NAS replication of repository volumes. These resources enable HaystackID to run annual tests of disaster recovery plans to verify contractual recovery time objective (RTO) and recovery point objective (RPO) service level agreements can be met.

Attachment A – Description of the Boundaries of HaystackID, LLC's Discovery Management System

Software

The HaystackID discovery management system environment uses Relativity discovery management software to store and maintain its client data. This system is developed and maintained by the software provider, and updates and releases are deployed by the HaystackID support team.

People

HaystackID has approximately 309 full-time employees and 896 flex employees. The organizational structure provides the framework for planning, directing, and controlling operations. Personnel and business functions are separated into functional areas and then departments according to job function, except for the Executive Committee, which is comprised of Senior Management (Chief Executive Officer, President, Chief Operating Officer, Chief Financial Officer, Chief Technology Officer, Chief Information Security Officer, Chief Marketing Officer, Chief People Officer, Chief Innovation Officer). The structure provides for clearly defined responsibilities and lines of authority for reporting and communication. The Company is divided into five in-scope departments: Data Operations, Client Services, Cyber Incident Response and Advanced Technologies Group, Forensics, and Managed Review. The Electronically Stored Information (ESI) Collections aspect of Forensics is in scope, whereas the Consulting aspects are not within the scope of this engagement. These departments are supported by Enterprise Managed Services & Sales Operations, Sales, Marketing, Information Technology (IT), Security, Finance, and Human Resources (HR). HaystackID has one out-of-scope business unit, called the Business Solutions Group.

Functional Area	Responsibilities
Senior Management	The Senior Management team has the responsibility of managing the day-to-day operations of HaystackID. They are responsible for the strategic direction of the Company and provide oversight and guidance to the employees. The Senior Management team helps ensure HaystackID meets the needs of its clients, employees, and shareholders.
Forensics	The Forensics and Collections (Forensics First) organization is responsible for the engagement and support of forensics and collections activity for HaystackID worldwide. The organization is the primary contact for internal team and external clients in forensics and collections-related tasks ranging from on-site and remote collections to employer protection programs.
Data Operations	The Data Operations group is responsible for the technical aspects of processing, hosting, production of litigation, and investigation of data. They manage HaystackID's client-facing systems and are responsible for helping ensure clients' technical requirements are met.

Attachment A – Description of the Boundaries of HaystackID, LLC's Discovery Management System

Functional Area	Responsibilities
Client Services	Client Services is a vital link between HaystackID's external clients and internal operational staff. Client Services staff are the primary point of contact for HaystackID clients, from project initiation through closeout. A project manager is responsible for communication, planning, workflow design, hosted technology user training, status reporting, project deliverables, billing, and ensuring clients' needs and expectations are met. Client Services staff are responsible for ensuring projects are carried out to the standards, within relevant timelines, at an acceptable cost, and in line with overall company objectives while also meeting client requirements for deliverables. They are responsible for setting and meeting client expectations and communicating project progress to the stakeholders in the project, internal sales, and executive sponsors.
Cyber Incident Response and Advanced Technologies Group	The Cyber Incident Response and Advanced Technologies Group is responsible for the planning and execution of reactive capabilities to rapidly identify sensitive data (PII/PHI) during a security incident so that client organizations can understand and respond to regulatory risk arising from personal data compromise. The organization is the primary contact for internal teams and external clients in actions ranging from identification and scoping the extent of the breach notification burden associated with compromised data to the data classification, entity identification and extraction, data science, reporting and delivery of data necessary to affect the required notifications.
Managed Review	The Managed Review services (ReviewRight®) organization is responsible for planning, training, executing, and supporting data and legal document review activities for HaystackID worldwide. The organization is the primary contact for internal teams and external clients in actions regarding document reviews ranging from client onboarding processes to review task, project, and program security.
IT and Security	The IT and Security teams are dedicated to ensuring electronic hardware and software assets maximize confidentiality, integrity, and accessibility to meet business and client requirements.
Administrative Services	The Administrative Services team is responsible for hiring staff dedicated to maximizing confidentiality, integrity, and accessibility to meet business and client requirements.

Attachment A – Description of the Boundaries of HaystackID, LLC's Discovery Management System

Policies and Procedures

Management has developed and communicated organizational policies and procedures to employees and clients. These procedures are reviewed annually, and necessary changes are made and authorized by Senior Management. These policies and procedures cover the following key security life cycle areas:

- Acceptable Use Policy
- Access Control Policy
- Application and Data Container Security Policy
- Backup and Restoration Policy
- Bring Your Own Device (BYOD) Policy
- Business Continuity and Disaster Recovery Policy
- Change Management Policy
- Clean Desk and Clear Screen Policy
- Data Integrity Policy
- Data Retention and Disposal Policy
- Incident Management Policy
- Information Classification Policy
- Information Security Policy
- Internal Audit Policy
- IT Asset Management Policy
- Key Management and Cryptography Policy
- Logging and Monitoring Policy
- Mobile Device Management Policy
- Network Security Policy
- Personnel Security Policy
- Physical and Environmental Security Policy
- Privacy Policy for Websites
- Progressive Discipline Policy
- Remote Access Policy
- Risk Assessment and Risk Treatment Methodology
- Risk Assessment Policy
- Software Development Policy
- Technology Equipment Handling and Disposal Policy
- Vendor Management Policy
- Vulnerability and Penetration Testing Management Policy
- Workstation and Mobile Device Policy
- HR policies and practices
- Privacy policies and practices
- IT and Security procedures
- Business Continuity Plan
- Disaster Recovery Plan
- Incident Response Plan
- Risk Assessment

Attachment A – Description of the Boundaries of HaystackID, LLC's Discovery Management System

Data

Data, as defined by HaystackID, falls into one of the following classifications:

- Highly Confidential Information: Client data and information about the Company that is of special sensitivity such that its unauthorized disclosure could seriously harm the Company.
- Confidential Information: Information about the Company that is of some sensitivity such that its unauthorized disclosure could harm the Company.
- Non-Sensitive Internal Information: Information that has not been made public by the Company but that is non-sensitive such that its public release would not harm the Company.
- Public Information: Information that has been made public by the Company.

Client data (ESI and Case Strategy data) maintained by HaystackID can include Payment Card Industry (PCI), PII, PHI, and GDPR-related data. ESI and Case Strategy data is treated as Highly Confidential Information. HaystackID uses data loss prevention (DLP) policies to restrict the transmission, movement, and removal of confidential information. Except for intake and forensics machines, HaystackID does not allow writing to universal serial bus (USB) devices.

Subservice Organizations

HaystackID uses third-party subservice organizations and vendors to assist in running its business operations and IT platform.

Subservice Organization	Function
Equinix	Colocation facilities
Centersquare (Cyxtera)	Colocation facilities
Digital Realty (Interxion)	Colocation facilities
Lumen	Network support
Relativity	Software development and support of the Relativity discovery management software
Microsoft	Cloud-based infrastructure, Office365 services (O365), multi-factor authentication services, and device configuration management
Dizzion	Secure managed remote desktop service
Amazon (Amazon WorkSpaces)	Secure managed remote desktop service
Google	Google Suite
QuickBase	Enterprise Resource Planning (ERP)

Attachment A – Description of the Boundaries of HaystackID, LLC’s Discovery Management System

Complementary User Entity Control Considerations

HaystackID’s controls were designed with the assumption that certain complementary user entity controls would be operating effectively at user entities. The controls described in this report occur at HaystackID and cover only a portion of a comprehensive internal controls structure. Each user entity must address the various aspects of internal control that may be unique to its particular system. This section describes the complementary user entity controls that should be developed, placed in operation, and maintained at user entities as necessary to meet the trust services criteria stated in the description of HaystackID’s system. The table below identifies the criteria the complementary user entity controls relate to. User entities should determine whether adequate controls have been established to provide reasonable assurance that:

Complementary User Entity Controls
User entities are responsible for communicating regulatory, legal and compliance requirements to HaystackID and ensuring the controls and services implemented align with their requirements.
User entities are responsible for understanding and complying with their contractual obligations to HaystackID.
User entities are responsible for the implementation of sound and consistent internal controls regarding general IT system access and system usage for internal user entity components associated with HaystackID.
User entities are responsible for defining security policies for their environment.
User entities are responsible for determining whether HaystackID’s security infrastructure aligns with their needs and for notifying HaystackID of requested modifications.
User entities are responsible for ensuring the confidentiality of user accounts and passwords assigned to them for use with HaystackID’s services.
User entities are responsible for maintaining their own system(s) of record - for example, maintaining a current list of active and inactive users.
User entities are responsible for immediately notifying HaystackID of actual or suspected information related to security breaches, including compromised user accounts.
User entities are responsible for developing their own disaster recovery and business continuity plans that address their inability to access or use HaystackID’s services.
User entities are responsible for providing notice to data subjects about their privacy practices and updating these notices as needed.
User entities are responsible for communicating choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects.
User entities are responsible for obtaining explicit consent for the collection, use, retention, disclosure, and disposal of personal information, if required.
User entities are responsible for handling requests by data subjects to access their personal data.

Attachment A – Description of the Boundaries of HaystackID, LLC's Discovery Management System

Complementary Subservice Organization Controls

HaystackID's controls related to the Discovery Management System cover only a portion of overall internal control for each user entity of HaystackID. It is not feasible for the trust services criteria related to Discovery Management System to be achieved solely by HaystackID.

Complementary Subservice Organization Controls
Subservice organizations have implemented strong authentication controls to restrict access to the environment.
Subservice organizations have limited administrator access on a least-privilege basis for only those who require this access based on job duties.
Subservice organizations have put in place procedures to monitor for, detect, and respond to potential security events and incidents in their environments.
Subservice organizations have implemented procedures to secure HaystackID's processing environment by implementing environmental controls to monitor and control the processing environment.
Subservice organizations encrypt sensitive client data at rest and during transmission.
Subservice organizations have implemented procedures to create and maintain backups of their data.
Subservice organizations have implemented disaster recovery and business continuity procedures and test these procedures at least annually.

Attachment B – Service Commitments and System Requirements of HaystackID, LLC’s Discovery Management System

Attachment B – Service Commitments and System Requirements of HaystackID, LLC’s Discovery Management System

Service Commitments and System Requirements

HaystackID designs its processes and procedures related to its Discovery Management System to meet its objectives for the successful delivery of its services. Those objectives are based on the service commitments HaystackID makes to user entities, the laws and regulations that govern the provision of the Discovery Management System, and the financial, operational, and compliance requirements HaystackID has established for the system.

The Discovery Management System manages data from user entities that is covered by various regulations and frameworks, such as the Health Insurance Portability and Accountability Act (HIPAA), International Traffic in Arms Regulations (ITAR), General Data Protection Regulation (GDPR), amongst other regulations, as well as other regional, country and state privacy or security laws and regulations in the jurisdictions in which HaystackID operates.

Security, availability, processing integrity, confidentiality, and privacy commitments to user entities are documented and communicated in service level agreements (SLA) and other client agreements.

Security commitments include principles within the fundamental designs of the eDiscovery system that are designed to permit system users to access the information they need based on their roles in the system while restricting them from accessing information not needed for their role.

HaystackID establishes operational requirements that support the achievement of security commitments, compliance with relevant laws and regulations, and other system requirements. Such requirements are communicated in HaystackID’s system policies and procedures, system design documentation, and contracts with vendors and customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies related to how the service is designed and developed, the system is operated, the internal business systems and networks are managed, and employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required when providing eDiscovery services.