A-LIGN

A-LIGN.com

Type 2 SOC 3

Prepared for:
Signifyd, Inc.

Signifyd

Date:
2025

SOC 3 FOR SERVICE ORGANIZATIONS REPORT

July 1, 2024 to June 30, 2025

Table of Contents

SECTION 1

ASSERTION OF SIGNIFYD, INC. MANAGEMENT

ASSERTION OF SIGNIFYD, INC. MANAGEMENT

July 5, 2025

We are responsible for designing, implementing, operating, and maintaining effective controls within Signifyd, Inc.'s ('Signifyd' or 'the Company') Signifyd's Commerce Protection Platform System throughout the period July 1, 2024 to June 30, 2025, to provide reasonable assurance that Signifyd's service commitments and system requirements were achieved based on the Trust Services Criteria relevant to Security, Availability, Confidentiality, and Privacy (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*, and Signifyd's compliance with the commitments in its Privacy Notice. Our description of the boundaries of the system is presented below in "Signifyd, Inc.'s Description of Its Signifyd's Commerce Protection Platform System throughout the period July 1, 2024 to June 30, 2025" and identifies the aspects of the system covered by our assertion.

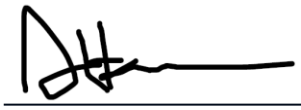
We have performed an evaluation of the effectiveness of the controls within the system throughout the period July 1, 2024 to June 30, 2025, to provide reasonable assurance that Signifyd's service commitments and system requirements were achieved based on the Trust Services Criteria. Signifyd's objectives 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 "Signifyd, Inc.'s Description of Its Signifyd's Commerce Protection Platform System throughout the period July 1, 2024 to June 30, 2025".

Signifyd uses Amazon Web Services, Inc. ('AWS' or 'subservice organization') to provide cloud hosting services, capacity management and backup services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Signifyd, to achieve Signifyd's service commitments and system requirements based on the applicable Trust Services Criteria and Signifyd's compliance with the commitments in its Privacy Notice. The description presents Signifyd's controls, the applicable Trust Services Criteria, and the types of complementary subservice organization controls assumed in the design of Signifyd's controls. The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary to achieve Signifyd's service commitments and system requirements based on the applicable Trust Services Criteria and Signifyd's compliance with the commitments in its Privacy Notice. The description presents the applicable Trust Services Criteria and the complementary user entity controls assumed in the design of Signifyd'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 July 1, 2024 to June 30, 2025 to provide reasonable assurance that Signifyd's service commitments and system requirements were achieved based on the applicable Trust Services Criteria and Signifyd's compliance with the commitments in its Privacy Notice, if complementary subservice organization controls and complementary user entity controls assumed in the design of Signifyd's controls operated effectively throughout that period.



Daniel Hammon
Director, Head of Info Security & Compliance
Signifyd, Inc.

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To Signifyd, Inc.:

Subject

We have examined Signifyd's ('Signifyd' or 'the Company') accompanying assertion titled "Assertion of Signifyd, Inc. Management" (assertion) that the controls within Signifyd's Commerce Protection Platform System were effective throughout the period July 1, 2024 to June 30, 2025, to provide reasonable assurance that Signifyd's service commitments and system requirements were achieved based on the Trust Services Criteria relevant to Security, Availability, Confidentiality, and Privacy (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*, and Signifyd's compliance with the commitments in its Privacy Notice.

Signifyd uses AWS to provide cloud hosting services, capacity management and backup services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Signifyd, to achieve Signifyd's service commitments and system requirements based on the applicable Trust Services Criteria and Signifyd's compliance with the commitments in its Privacy Notice. The description presents Signifyd's controls, the applicable Trust Services Criteria, and the types of complementary subservice organization controls assumed in the design of Signifyd's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Signifyd, to achieve Signifyd's service commitments and system requirements based on the applicable Trust Services Criteria and Signifyd's compliance with the commitments in its Privacy Notice. The description presents Signifyd's controls, the applicable Trust Services Criteria, and the complementary user entity controls assumed in the design of Signifyd'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 controls.

Service Organization's Responsibilities

Signifyd 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 Signifyd's service commitments and system requirements were achieved. Signifyd has also provided the accompanying assertion (Signifyd assertion) about the effectiveness of controls within the system. When preparing its assertion, Signifyd is responsible for selecting, and identifying in its assertion, the applicable Trust Services Criteria, for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system, and complying with the commitments in its Privacy Notice.

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 and its compliance with the commitments in its Privacy Notice. 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 description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its 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.

Independence and Ethical Responsibilities

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 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 are 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 Signifyd's Commerce Protection Platform System were suitably designed and operating effectively throughout the period July 1, 2024 to June 30, 2025, to provide reasonable assurance that Signifyd's service commitments and system requirements were achieved based on the applicable Trust Services Criteria is fairly stated, in all material respects, if complementary subservice organization controls and complementary user entity controls assumed in the design of Signifyd's controls operated effectively throughout that period.

The SOC logo for Service Organizations on Signifyd's website constitutes a symbolic representation of the contents of this report and is not intended, nor should it be construed, to provide any additional assurance.

Restricted Use

This report, is intended solely for the information and use of Signifyd, user entities of Signifyd's Commerce Protection Platform during some or all of the period July 1, 2024 to June 30, 2025, business partners of Signifyd subject to risks arising from interactions with the Signifyd's Commerce Protection Platform, and those who have sufficient knowledge and understanding of the complementary subservice organization controls and complementary user entity controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

A-LIGN ASSURANCE

Tampa, Florida
July 5, 2025

SECTION 3

SIGNIFYD, INC.'S DESCRIPTION OF ITS SIGNIFYD'S COMMERCE PROTECTION PLATFORM SYSTEM THROUGHOUT THE PERIOD JULY 1, 2024 TO JUNE 30, 2025

OVERVIEW OF OPERATIONS

Company Background

Founded in 2011, Signifyd's mission is to protect merchants from fraud, consumer abuse, and friction in the buying experience. The company provides an end-to-end Commerce Protection Platform utilizing big data, machine learning, and expert manual review to provide merchants with Signifyd's determination of whether an e-commerce order received by such a merchant is either a fraudulent / abusive or a legitimate order. Signifyd reimburses merchants who subsequently receive a "chargeback" on Signifyd approved orders.

A recognized market and strategy leader for its impactful solutions, Signifyd's top standing is validated by G2, the peer-to-peer business solutions review platform; recent G2 analysis places the company above competitors, ranking it first in market presence and naming it a market leader. Furthering its integration within the commerce ecosystem, strategic partnerships have been formed with key players, including leading commerce platforms and payment processors. Reflecting its established market trust, Signifyd's customer base includes numerous companies on the Fortune 1000 and Internet Retailer Top 500 lists.

The company is also known for its positive company culture and as a notable workplace, with a history of past distinctions such as listings in *Inc. Magazine's* Best Workplaces and repeated Bay Area Best Places to Work honors from the *San Francisco Business Times* and *Silicon Valley Business Journal*. Signifyd remains committed to cultivating a supportive and positive work environment for its employees.

Headquartered in San Jose, California, Signifyd operates globally with additional locations including Denver, New York, Seattle, London, Belfast, and Budapest.

Description of Services Provided

Signifyd provides an end-to-end Commerce Protection Platform that helps merchants maximize conversions, automate customer experience, and prevent fraud and customer abuse. The platform uses big data, machine learning, and expert manual review to provide merchants with Signifyd's determination of whether an e-commerce order received by such a merchant is either a fraudulent / abusive or a legitimate order. Signifyd reimburses merchants who subsequently receive a "chargeback" on Signifyd approved orders. In addition, Signifyd also provides chargeback recovery and management services.

Signifyd's Commerce Protection Platform is a cloud-native processing system that receives ecommerce transactions through Representational State Transfer (REST) Application Programming Interface API integrations or plugins from supported ecommerce platforms. Using machine learning, it analyzes transactions in real time and communicates decisions to merchants via webhooks. Merchants can access order decisions and reports through the Signifyd Console. In addition to the live system, Signifyd Engineering supports offline systems for model training, analytics, risk and claims management, chargeback handling, and business reporting.

Principal Service Commitments and System Requirements

Signifyd designs its processes and procedures for the Commerce Protection Platform to meet its core service objectives. These objectives are founded on the service commitments Signifyd makes to its user entities (also referred to as merchants or subscribers), the laws and regulations governing the provision of its services, and the financial, operational, and compliance requirements Signifyd has established for its platform.

Security commitments to user entities are documented and communicated through Service Level Agreements (SLAs) and the Privacy Notice, which is publicly available on the Signifyd website. Key security commitments include, but are not limited to:

- Protecting the confidentiality and privacy of subscriber personal data.
- Ensuring the Commerce Protection Platform and associated services achieve uptime and availability as stated in SLAs.
- Maintaining the security of the solution and the data processed therein.
- Upholding the security, confidentiality, and integrity of data when interacting with third parties.

To support these commitments and adhere to relevant laws and regulations, Signifyd establishes comprehensive operational and system requirements. These requirements are formally communicated through Signifyd's internal system policies and procedures, system design documentation, and in contracts with its Subscribers. Information security policies define an organization-wide approach to how systems and data are protected. Established and documented policies address how the Commerce Protection Platform is designed, developed, and operated; how internal business systems and networks are managed; and how employees are hired, trained, and managed throughout their tenure.

In addition to these policies, standard operating procedures have been documented for critical manual and automated processes. These procedures detail the implementation of controls covering areas such as:

- **Data Confidentiality:** Implementing measures like role-based access controls for production environments; segregation of production and non-production infrastructure; a defense-in-depth strategy (including network and application firewalls, load balancers, and threat monitoring); ensuring authentication and data transmission to the production environment take place over secure channels (e.g., Virtual Private Network (VPN), Secure Shell (SSH), Transport Layer Security (TLS)); and encryption of general data in transit over public networks (e.g., using TLS 1.2 or greater).
- **Platform Availability and Resilience:** Maintaining business continuity and disaster recovery plan processes with annual testing, ensuring a fault-tolerant, scalable, and highly available production system with load balancing across geographically dispersed availability zones, and robust data backup processes.
- **Solution Quality and Security:** Adhering to an established Software Development Lifecycle (SDLC) process with testing and quality assurance, conducting regular vulnerability scanning and annual penetration testing, segregating internet-facing systems from the production network, controlling system input/output via APIs, and performing periodic user access reviews.
- **Third-Party Risk Management:** Maintaining a third-party risk management program that includes pre-onboarding and annual reassessments of critical service providers, with Master Service Agreement (MSA) provisions for information security and confidentiality.

Components of the System

Infrastructure

Primary infrastructure used to provide Signifyd's Commerce Protection Platform System includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
AWS Elastic Cloud Compute (EC2)	Virtual machines running Linux Operating System	Hosts Signifyd's Commerce Protection Platform System runtime components
AWS	Cloud Infrastructure Platform	Primary cloud environment providing core computer, networking, storage, and foundational data services

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Signifyd Microservices	Proprietary Software	Core application components delivering the Commerce Protection Platform services
Managed Datastore & Search Services	Specialized Managed Services	Provide scalable datastores for investigation and enable platform-wide search functionalities
Elastic (for Elasticsearch)	Managed Search & Analytics Service	Enables search functionalities and data exploration within the platform
Tecton	Feature Store Platform	Manages and serves features for machine learning (ML) model operations
Databricks	Data warehouse	Used for large-scale Data Science analysis and ML model training

Software

Primary software used to provide Signifyd's Commerce Protection Platform System includes the following:

Primary Software		
Software	**Operating System**	**Purpose**
Datadog	Software-as-a-Service (SaaS) Platform / Cloud-Hosted	Provides comprehensive platform and infrastructure monitoring
PagerDuty	SaaS Platform / Cloud-Hosted	Manages on-call scheduling, alerting, and incident response coordination
Loggly	SaaS Platform / Cloud-Hosted	Centralizes application log collection, aggregation, and analysis
Rapid7	SaaS Platform / Cloud-Hosted	Provides Security Information and Event Management (SIEM) for threat detection and response
Jaeger	SaaS Platform / Cloud-Hosted	Enables distributed tracing for monitoring and troubleshooting microservices
LogRocket	SaaS Platform / Cloud-Hosted	Provides session replay and frontend monitoring for diagnosing user-facing application issues

People

Dedicated professionals across Signifyd ensure the quality and reliability of its services. Key teams involved in this effort include, but are not limited to:

- **Management / Executive Leadership:** Sets strategic direction, champions a security and compliance culture, and ensures resources are allocated to meet company objectives.
- **Security Team:** Manages the comprehensive information security and compliance program, addressing risks, threats, and vulnerabilities while ensuring policy adherence and business continuity.
- **Engineering Team:** Develops and secures company systems and applications, emphasizing secure coding, resilient infrastructure, vulnerability management, and data protection.

- **Information Technology (IT) Team:** Manages and secures corporate IT infrastructure, systems, and devices, overseeing access controls, endpoint protection, IT asset management, and operational policies.
- **Human Resources (HR) Team:** Oversees the employee lifecycle, ensuring policy adherence, facilitating training, and maintaining records to foster a compliant and secure work environment.
- **Legal / Privacy Team:** Drives legal, contractual, and regulatory compliance with a strong focus on data privacy, managing contracts, data subject rights, and privacy risk.

Data Collection and Privacy

In order to provide their services to their Subscribers, Signifyd collects and processes certain information about individuals who interact with their Subscriber e-commerce as end users ("End Users"). Signifyd obtains a User Data License from their Subscribers, allowing us to process information about transactions on a Subscriber's e-commerce storefront. They also collect behavioral, device and connection data through standard tracking technologies (their JavaScript and mobile software development kit (SDK)), which are embedded on the Subscriber Storefronts (collectively, "End User Data"). This data processing is solely for the purposes of fraud identification, prevention, dispute, and monitoring, as well as to analyze data for the purpose of building, maintaining, and improving their predictive models and fraud-related services. End User Data may include Personal Data, which includes data that identifies an End User and as described in further detail in their Privacy Notice (available at https://www.signifyd.com/privacy/).

Processes, Policies and Procedures

Policies and procedures are established to cover areas including, but not limited to, information security, logical access, computer operations, change control, and data communication standards. Teams are expected to adhere to Signifyd's policies and procedures, which are available on the Company's intranet and accessible to the employees.

Physical Security

As a remote-first company, the production systems are hosted on AWS, which hold multiple industry-recognized certifications and assurances. Physical access to the corporate office is restricted to only appropriate individuals with electronic key card access. Refer to the "Subservice Organizations" section below for controls managed by the subservice organization.

Logical Access

The Company utilizes role-based access controls (RBAC) to manage access to its information systems and data. Access privileges are granted based on job function, active employment status, and management approval, adhering to the principles of least privilege and need-to-know. System access requires unique usernames and passwords, with multifactor authentication (MFA) applied for user verification.

Access to the production network and infrastructure are similarly governed by job function and utilize the Company's established authentication methods. The production environment employs logical segmentation to isolate systems, and perimeter security is maintained through security groups with predefined access control lists (ACLs). Network monitoring systems alert administrators to potential issues based on defined thresholds. The Information Security Policy, supported by technical controls, dictates strong password complexity for user accounts. Periodic access reviews are conducted to ensure access rights remain appropriate, and user activity logging is implemented.

Computer Operations - Backups

Data backup processes are designed for resilience and reliability. The production environment leverages multiple AWS availability zones, utilizing distinct data centers within these zones to support continued operation in the event of a localized failure.

To validate the integrity and recoverability of data, backup and restoration tests of backup data from the production system are performed at least annually. System and Application Insights are integrated with monitoring tool sets to actively monitor for backup errors. In the event a backup job does not complete successfully, the failed backup is investigated, and procedures are in place to re-run the backup to ensure a successful copy of the data is secured.

Computer Operations - Availability

The Company maintains an Incident Response Plan (IRP) and a business continuity and disaster recovery plan. The IRP guides timely responses to security incidents and breaches - with procedures for identification, reporting, action, and communication - ensuring incidents are tracked to remediation, including root cause analysis. The BCDR plan facilitates service resumption following significant disruptions and is reviewed, tested, and updated annually.

To support ongoing service availability, application-level tools monitor for resource constraints, application errors, and other availability or network issues. Infrastructure redundancy for key components is implemented, with hardware configured for failover. System integrity is further addressed through a Vulnerability Management policy that includes quarterly third-party scanning, with findings remediated per policy and retests performed as needed.

Change Control

Management has implemented a formal change management policy. This policy outlines requirements for the authorization, development, configuration, documentation, testing, approval, and implementation of changes affecting infrastructure, data, and software.

System changes undergo testing, review, and approval before deployment to the production environment. To maintain control and segregation of duties, access for making source code changes and publishing to production is restricted to authorized personnel, based on their defined roles and responsibilities. The Company utilizes separate environments for development, testing, and production activities. Management receives automated alerts upon promotion of changes to the production environment, and version control software is employed to manage source code. Additionally, rollback capabilities are established to revert changes if necessary.

Data Communications

Firewall systems are in place to filter unauthorized inbound network traffic and deny connections not explicitly authorized. Network Address Translation (NAT) manages internal Internet Protocol (IP) addresses, and administrative access to firewalls is restricted to authorized Signifyd personnel.

Signifyd leverages redundant infrastructure provided by its cloud service provider to mitigate single points of failure for its services. This design helps ensure high availability, with systems configured to seamlessly transition to redundant components if a primary system encounters an issue.

Penetration testing is conducted by a qualified third-party vendor using an industry-accepted methodology agreed upon by Signifyd and the vendor. This process rigorously assesses the security posture of their systems and environments by identifying and attempting to exploit vulnerabilities through simulated attack scenarios. Testing is performed from both external and internal perspectives, covering network and application layers, and includes security controls related to access, data handling, and system configuration.

They conduct vulnerability scanning regularly using a third-party tool. Their approach is designed to efficiently test their systems while minimizing any potential risks from the scanning process itself. Identified results are reviewed and assessed using a risk-based approach and then actioned on accordingly. Any findings are addressed in line with their internal policies, and they perform retests and on-demand scans as needed.

Authorized Signifyd personnel access their fully cloud-based production environment via the internet. They secure this access with industry-leading VPN technology and mandatory MFA and Single Sign-On (SSO).

Boundaries of the System

The scope of this report includes Signifyd's Commerce Protection Platform System performed in the San Jose, California; Denver, Colorado; New York, New York; Seattle, Washington; Mexico City, Mexico; Belfast, Great Britain; and London, Great Britian facilities.

This report does not include the cloud hosting services, capacity management and backup services provided by AWS at multiple facilities.

Changes to the System Since the Last Review

No significant changes have occurred to the services provided to user entities since the organization's last review.

Incidents Since the Last Review

No significant issues, such as any reportable security incident as defined by applicable data breach laws, have occurred concerning the services offered to user entities (Subscribers/Merchants) since the organization's last review.

Criteria Not Applicable to the System

The following criteria are not applicable to Signifyd's Commerce Protection Platform System:

Criteria Not Applicable to the System		
Category	**Criteria**	**Reason**
Privacy	P3.1	Signifyd does not directly collect personal information from data subjects. Rather, such information is submitted to Signifyd by Subscribers (i.e., Merchants or Customers) to our Commerce Protection Platform. Pursuant to our contractual agreements, these Subscribers bear the sole responsibility for collecting personal information from data subjects and obtaining their explicit consent.
	P3.2	Signifyd does not directly collect personal information from data subjects. Rather, such information is submitted to Signifyd by Subscribers (i.e., Merchants or Customers) to our Commerce Protection Platform. Pursuant to our contractual agreements, these Subscribers bear the sole responsibility for collecting personal information from data subjects and obtaining their explicit consent.
	P6.1	Signifyd does not directly collect personal information from data subjects. Rather, such information is submitted to Signifyd by Subscribers (i.e., Merchants or Customers) to our Commerce Protection Platform. Pursuant to our contractual agreements, these Subscribers bear the sole responsibility for collecting personal information from data subjects and obtaining their explicit consent.

Criteria Not Applicable to the System		
Category	**Criteria**	**Reason**
	P6.2	Signifyd does not directly collect personal information from data subjects. Rather, such information is submitted to Signifyd by Subscribers (i.e., Merchants or Customers) to our Commerce Protection Platform. Pursuant to our contractual agreements, these Subscribers bear the sole responsibility for collecting personal information from data subjects and obtaining their explicit consent.
	P6.4	Signifyd does not directly collect personal information from data subjects. Rather, such information is submitted to Signifyd by Subscribers (i.e., Merchants or Customers) to our Commerce Protection Platform. Pursuant to our contractual agreements, these Subscribers bear the sole responsibility for collecting personal information from data subjects and obtaining their explicit consent.
	P6.5	Signifyd does not directly collect personal information from data subjects. Rather, such information is submitted to Signifyd by Subscribers (i.e., Merchants or Customers) to our Commerce Protection Platform. Pursuant to our contractual agreements, these Subscribers bear the sole responsibility for collecting personal information from data subjects and obtaining their explicit consent.

Subservice Organizations

This report does not include the cloud hosting services, capacity management and backup services provided by AWS at multiple facilities.

Subservice Description of Services

AWS is a public cloud service platform that supports a broad selection of operating systems, programming languages, frameworks, tools, databases, and devices. AWS provides a wide array of configurable security options and the ability to control them so that security can be customized to meet unique requirements.

Complementary Subservice Organization Controls

Signifyd's services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the Trust Services Criteria related to Signifyd's services to be solely achieved by Signifyd control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Signifyd.

The following subservice organization controls should be implemented by AWS to provide additional assurance that the Trust Services Criteria described within this report are met:

Subservice Organization - AWS		
Category	**Criteria**	**Control**
Common Criteria / Security	CC6.4	AWSCA-4.12: Key Management Service (KMS)-Specific - Recovery key materials used for disaster recovery processes by KMS are physically secured offline so that no single AWS employee can gain access to the key material.
		AWSCA-4.13: KMS-Specific - Access attempts to recovery key materials are reviewed by authorized operators on a cadence defined in team processes.
		AWSCA-5.1: Physical access to data centers is approved by an authorized individual.
		AWSCA-5.2: Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		AWSCA-5.3: Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
		AWSCA-5.4: Physical access points to server locations are recorded by closed circuit television camera (CCTV). Images are retained for 90 days, unless limited by legal or contractual obligations.
		AWSCA-5.5: Physical access points to server locations are managed by electronic access control devices.
		AWSCA-5.6: Electronic intrusion detection systems (IDSs) are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.
Availability	A1.2	AWSCA-5.7: Amazon-owned data centers are protected by fire detection and suppression systems.
		AWSCA-5.8: Amazon-owned data centers are air conditioned to maintain appropriate atmospheric conditions. Personnel and systems monitor and control air temperature and humidity at appropriate levels.
		AWSCA-5.9: Uninterruptible Power Supply (UPS) units provide backup power in the event of an electrical failure in Amazon-owned data centers.
		AWSCA-5.10: Amazon-owned data centers have generators to provide backup power in case of electrical failure.
		AWSCA-5.11: Contracts are in place with third-party colocation service providers which include provisions to provide fire suppression systems, air conditioning to maintain appropriate atmospheric conditions, UPS units, and redundant power supplies.
		AWSCA-5.12: AWS performs periodic reviews of colocation service providers to validate adherence with AWS security and operational standards.
		AWSCA-7.2: S3-Specific - S3 performs continuous integrity checks of the data at rest. Objects are continuously validated against their checksums to prevent object corruption.

Subservice Organization - AWS		
Category	**Criteria**	**Control**
		AWSCA-7.3: S3-Specific - When disk corruption or device failure is detected, the system automatically attempts to restore normal levels of object storage redundancy.
		AWSCA-7.4: S3-Specific - Objects are stored redundantly across multiple fault-isolated facilities.
		AWSCA-7.5: S3-Specific - The design of systems is sufficiently redundant to sustain the loss of a data center facility without interruption to the service.
		AWSCA-7.6: Relational Database Service (RDS)-Specific - If enabled by the customer, RDS backs up customer databases, stores backups for user-defined retention periods, and supports point-in-time recovery.
		AWSCA-8.1: Monitoring and alarming are configured by Service Owners to identify and notify operational and management personnel of incidents when early warning thresholds are crossed on key operational metrics.
		AWSCA-8.2: Incidents are logged within a ticketing system, assigned severity rating and tracked to resolution.
		AWSCA-10.1: Critical AWS system components are replicated across multiple Availability Zones and backups are maintained.
		AWSCA-10.2: Backups of critical AWS system components are monitored for successful replication across multiple Availability Zones.

Signifyd management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant Trust Services Criteria through written contracts, such as SLA.

In addition, Signifyd performs monitoring of the subservice organization controls, including the following procedures:

- Reviewing attestation reports over services provided by vendors and subservice organizations
- Monitoring external communications, such as customer complaints relevant to the services provided by the subservice organizations

COMPLEMENTARY USER ENTITY CONTROLS

Signifyd's services operate with the assumption that User Entities (our customers) will implement certain complementary controls. These are essential as not all Trust Services Criteria related to Signifyd's services can be solely achieved by Signifyd's procedures. Accordingly, User Entities should establish their own internal controls to complement those of Signifyd's.

Key complementary user entity controls include:

1. User entities are responsible for understanding and complying with their contractual obligations to Signifyd.
2. User entities are responsible for notifying Signifyd of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own systems of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of Signifyd services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Signifyd services.
6. User entities are responsible for providing Signifyd with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying Signifyd of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.