A-LIGN

Signifyd, Inc.

Type 2 SOC 3

2024

Signifyd

SOC 3 FOR SERVICE ORGANIZATIONS REPORT

July 1, 2023 to June 30, 2024

Table of Contents

SECTION 1

ASSERTION OF SIGNIFYD, INC. MANAGEMENT

ASSERTION OF SIGNIFYD, INC. MANAGEMENT

July 5, 2024

We are responsible for designing, implementing, operating, and maintaining effective controls within Signifyd, Inc.'s ('Signifyd' or 'the Company') Commerce Protection Platform System throughout the period July 1, 2023 to June 30, 2024, 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, 2023 to June 30, 2024" 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, 2023 to June 30, 2024, 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, 2023 to June 30, 2024".

Signifyd uses Amazon Web Services, Inc. ('AWS') and Google Cloud Platform ('GCP') to provide cloud hosting services, capacity management and backup services (collectively, the 'subservice organizations'). 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, 2023 to June 30, 2024 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.

Varun Kumar
SVP Product & Engineering
Signifyd, Inc.

SECTION 2

INDEPENDENT SERVICE AUDITOR’S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To Signifyd, Inc.:

Subject

We have examined Signifyd's 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, 2023 to June 30, 2024, 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 Amazon Web Services, Inc. ('AWS') and Google Cloud Platform ('GCP') to provide cloud hosting services, capacity management and backup services (collectively, the 'subservice organizations'). 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, 2023 to June 30, 2024, 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, 2023 to June 30, 2024, 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, 2024

SECTION 3

SIGNIFYD, INC.'S DESCRIPTION OF ITS SIGNIFYD'S COMMERCE PROTECTION PLATFORM SYSTEM THROUGHOUT THE PERIOD JULY 1, 2023 TO JUNE 30, 2024

OVERVIEW OF OPERATIONS

Company Background

Signifyd was founded in 2011 with the mission of protecting merchants from fraud, consumer abuse, and friction in the buying experience. The company provides guaranteed commerce protection by using big data, machine learning, and expert manual review to shift liability for fraud from merchants to Signifyd. Signifyd's 100 percent financial guarantee on approved orders means ecommerce merchants can expand into new markets and ship more orders without worrying about fraud risk or the cost associated with it.

Signifyd has formed strategic partnerships with Salesforce Commerce Cloud, Magento, Shopify, BigCommerce, FIS/Worldpay, and Accertify. The company has received numerous awards and mentions as a market and strategy leader, most recently from G2 as Leader in Fraud Protection, Momentum Leader, and Most Implementable.

Signifyd has been listed as having a Top Company Culture by Entrepreneur. The company has regularly been named to Inc. Magazine's Best Workplaces list and is repeatedly recognized by the San Francisco Business Times and Silicon Valley Business Journal as one of the Bay Area's Best Places to Work.

Signifyd counts among its customers a number of companies on the Fortune 1000 and Internet Retailer Top 500 lists. Signifyd is headquartered in San Jose, California, with locations in Denver, New York, Seattle, Mexico City, Belfast, and London.

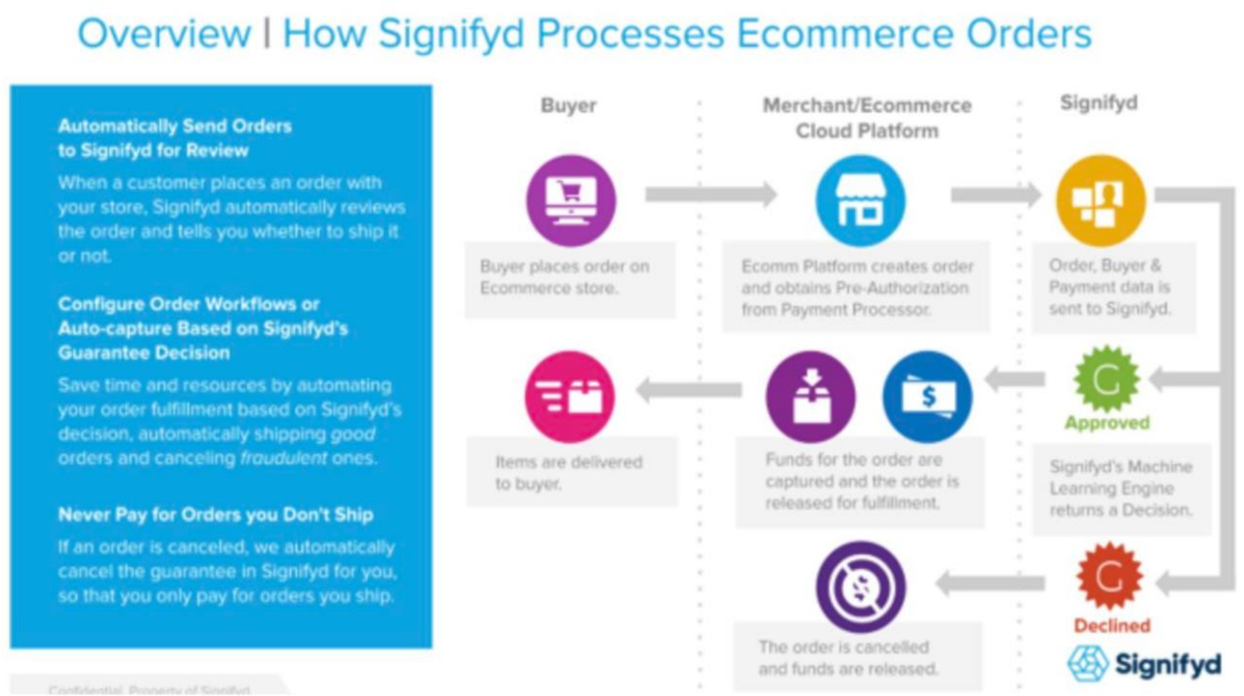
Description of Services Provided

Commerce Protection Platform

Signifyd provides an end-to-end Commerce Protection Platform that leverages its Commerce Network to maximize conversion, automate customer experience, and eliminate fraud and customer abuse for retailers. Signifyd leverages big data, machine learning, and expert manual review to provide a 100 percent financial guarantee against fraud on approved orders. This effectively shifts the liability for fraud away from ecommerce merchants, allowing them to increase sales and open new markets while reducing risk. Signifyd also protects merchants from customer abuse by providing a financial guarantee in cases of item-not-received (INR) claims and by offering a highly automated Chargeback Recovery product.

Signifyd's Commerce Protection Platform is a cloud native, nonstop, state-of-the-art processing system. It receives incoming ecommerce transactions through a Representational State Transfer (REST) Application Programming Interface (API) integration or Signifyd plugins from multiple ecommerce platforms. Using machine learning technologies, this system provides real-time analysis of transactions and issues guarantees to merchants via webhook integrations. Customers can view order status and access business reports via the Signifyd Console. Besides the online system, Signifyd Engineering has also crafted offline systems for machine learning model training, data analysis, risk management, claims management, chargebacks management, and business reporting.

Process Diagram



Overview | How Signifyd Processes Ecommerce Orders

Automatically Send Orders to Signifyd for Review

When a customer places an order with your store, Signifyd automatically reviews the order and tells you whether to ship it or not.

Configure Order Workflows or Auto-capture Based on Signifyd's Guarantee Decision

Save time and resources by automating your order fulfillment based on Signifyd's decision, automatically shipping *good* orders and canceling *fraudulent* ones.

Never Pay for Orders you Don't Ship

If an order is canceled, we automatically cancel the guarantee in Signifyd for you, so that you only pay for orders you ship.

Buyer places order on Ecommerce store.

Ecomm Platform creates order and obtains Pre-Authorization from Payment Processor.

Order, Buyer & Payment data is sent to Signifyd.

Signifyd's Machine Learning Engine returns a Decision.

Funds for the order are captured and the order is released for fulfillment.

Items are delivered to buyer.

The order is cancelled and funds are released.

Buyer
Merchant/Ecommerce Cloud Platform
Signifyd
$
Approved
Declined
Signifyd
Confidential. Property of Signifyd

Principal Service Commitments and System Requirements

Signifyd designs its processes and procedures related to its fraud protection solution for ecommerce merchants to meet its objectives for its Commerce Protection Platform. Those objectives are based on the service commitments that Signifyd makes to user entities; the laws and regulations that govern the provisioning of its services; and the financial, operational, and compliance requirements that Signifyd has established for the services.

Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs), as well as within the Privacy Policy published on its public website. Security commitments are standardized and include, but are not limited to, the following:

- Protect the Confidentiality & Integrity of Subscriber & End User Information
- Provide Uptime & Availability to the Platform & Associated Services as Stated in SLAs
- Ensure Quality, Accuracy, & Security of the Solution & Data Therein
- Ensure Security, Confidentiality, & Integrity of Data Coming in Contact with Third-parties

Signifyd establishes operational and system requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Signifyd’s system policies and procedures, system design documentation, and in contracts with its Subscribers. Signifyd’s principal system requirements include the following:

- Protect the Confidentiality & Integrity of Subscriber & End User Information.
- Access to the production environment is limited to authorized employees based on job function.
- Production infrastructure is segregated from the non-production environment and from public facing infrastructure.
- A Defense in Depth control strategy is implemented which includes multiple layers of perimeter defense around core application and database servers including network and application firewalls, load balancers, logical access restrictions, and threat monitoring and logging utilities.
- Data in transit over the public internet is encrypted using Transport Layer Security (TLS) 1.2 or greater.

- Provide Uptime & Availability to the Platform & Associated Services as Stated in SLA.
- Business Continuity and Disaster Recovery processes are in place and plans are tested annually to ensure Business Continuity Plan (BCP)/Disaster Recovery (DR) capabilities.
- Signifyd's production system is fault-tolerant, scalable, and highly available. Incoming traffic is load balanced across geographically dispersed availability zones.
- A robust backup process has been established for production databases and End User data. Ensuring Quality, Accuracy, & Security of the Platform & Data Therein.
- Changes to the solution follow an established Software Development Lifecycle (SDLC) process, which includes testing and quality assurance of changes in a testing or staging environment prior to promotion to the production environment.
- Quarterly vulnerability scanning and annual penetration testing is completed to monitor the production platform for high-risk security vulnerabilities and misconfigurations.
- Public internet facing systems are segregated from the production network through network segmentation, security groups, and logical access restrictions. End User access to the solution is governed through an Application Program Interface which controls the type and formatting of all input and output from the system.
- User access reviews are performed semi-annually. Any issues identified are documented and tracked to completion.
- Ensuring Security, Confidentiality, & Integrity of Data Coming in Contact with Third-parties.
- Authentication and data transmission to the production environment takes place over secure transmission channels (e.g., Virtual Private Network (VPN), Secure Shell (SSH), TLS).
- The Company has established a third-party risk management program and conducts pre-onboarding assessments of the vendors and annual re-assessments of its critical service providers in order to track and manage third-party risk. Any issues identified during the risk assessments are tracked through to remediation.
- Vendor MSAs specify information security and confidentiality requirements for the vendor.

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 Virtual Private Cloud (VPC)	VPC	Provides a private network for Signifyd's Commerce Protection Platform
AWS VPC GATEWAY	Virtual network gateway	Facilitates communications between components running inside the VPC and the Internet
Signifyd Microservices	Proprietary software developed by Signifyd to provide the Commerce Protection Platform	Various

Primary Infrastructure		
Hardware	**Type**	**Purpose**
AWS	Supporting infrastructure for Signifyd microservices	Elastic Load Balancers Relational Database Service DynamoDB Redshift Simple Storage Service (S3) Kinesis Others
Instaclustr	Investigation datastore	Hosted Cassandra
Elastic	Search services	Elasticsearch
Tecton	Feature store	Used for Data Science and machine learning (ML) algorithms
Databricks	Data warehouse	Used for Data Science analysis and model training

Software

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

Primary Software		
Software	**Operating System**	**Purpose**
Datadog	Platform monitoring	Monitoring
PagerDuty	On-call alerting and incident management	Incident Alerting
Loggly	Application log collection and monitoring	Log collection
Panther	Security log monitoring	Security Information and Event Management (SIEM)
Jagger	Application log collection and monitoring	Log collection

People

The Signifyd staff provides support for the above services in each of the following functional areas:

- Executive Management - Provides general oversight and strategic planning of operations.
- Development Team - Responsible for delivering a responsive system that fully complies with the functional specification.
- System Administrators - Responsible for effective provisioning, installation/configuration, operation, and maintenance of systems hardware and software relevant to the system.
- Customer Support - Serves customers by providing product and service information that includes resolving product and service issues.
- Information Security - Performs regularly scheduled audits relative to defined standards, provides continuous improvement feedback, and assesses legal and regulatory requirements.

Data

User data is captured and utilized by Signifyd’s Commerce Protection Platform to deliver its Commerce Protection Platform Services. Such data includes, but is not limited to, the following:

- Ecommerce transaction information, including information on the device used and behavior on Signifyd’s customers’ site that led to such transaction.
- Personally identifiable information, including e-mail address, physical address, first name, last name, birth date, age, company, job title, photo, website Uniform Resource Locator (URLs), social network user IDs, instant messenger handles, and Internet protocol (IP) address.
- Certain credit card information, including Address Verification Service (AVS) and Card Verification Code (CVV) response codes, billing address, Issuer Identification Number, and last 4 digits.
- Identifiers, such as: phone number, user identification (ID), first name, last name, physical address, e-mail address, zip/postal code, device ID, order ID, transaction ID, items purchased.
- Payment and bank information, such as: transaction amount, payment method, last 4 digits of a payment card number, card Bank Identification Number (BIN):
  - Signifyd does not process payments or evaluate creditworthiness.
  - Signifyd does not receive full Primary Account Number (PAN) or Payment Card Industry (PCI) sensitive information to make fulfillment decisions; however, depending on the financial institution and how a merchant receives chargebacks, Signifyd may receive PCI sensitive information as part of the claims evaluation or dispute management process.
- Internet or Network Activity, such as: login behavior, behavior transaction analysis, IP address:
  - Signifyd collect geo-location data of users when relevant to card-not-present transactions from mobile applications, e.g., wallet payments or scan and go payments.
- Inferences Drawn from other Personal Information.

Privacy Commitments

Signifyd receives a User Data License from our merchant customers to process information about transactions on their e-commerce storefronts. This is solely for the purposes of fraud identification, prevention, dispute, and monitoring purposes, and to analyze data for the purpose of building, maintaining and improving our predictive models and fraud-related services.

Collection of user data includes information such as such as personal identifiers, internet activity, inferences, and payment information (note: Signifyd does NOT receive full PAN or PCI sensitive information and will never process payments to evaluate creditworthiness). See the API documentation for a full list on the types of data collected.

Signifyd’s legal and compliance teams monitor best practices and changes within the industry, including changes to applicable laws and regulations:

1. A summary of the significant privacy and related security requirements common to most agreements between the service organization and its user entities and any requirements in a particular user entity’s agreement that the service organization meets for all or most user entities.
2. A summary of the significant privacy and related security requirements mandated by law, regulation, an industry, or a market that are not included in user entity agreements but the service organization meets for all or most user entities.
3. The purposes, uses, and disclosures of personal information as permitted by user entity agreements and beyond those permitted by such agreements but not prohibited by such agreements and the service organization’s commitments regarding the purpose, use, and disclosure of personal information that are prohibited by such agreements.
4. A statement that the information will be retained for a period no longer than necessary to fulfill the stated purposes or contractual requirements or for the period required by law or regulation, as applicable, or a statement describing other retention practices.
5. A statement that the information will be disposed of in a manner that prevents loss, theft, misuse, or unauthorized access to the information.

6. If applicable, how the service organization supports any process permitted by user entities for individuals to obtain access to their information to review, update, or correct it.
7. If applicable, a description of the process to determine that personal information is accurate and complete and how the service organization implements correction processes permitted by user entities.
8. If applicable, how inquiries, complaints, and disputes from individuals (whether directly from the individual or indirectly through user entities) regarding their personal information are handled by the service organization.
9. A statement regarding the existence of a written security program and what industry or other standards it is based on.
10. Other relevant information related to privacy practices deemed appropriate for user entities by the service organization.

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 and GCP, 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 has implemented role-based access controls that limit access to sensitive information to only those individuals who require access based on job function, active employment, and management approval.

Administrative level access to the Company's production network is limited to appropriate individuals based on job function with the Company.

Remote access to the Company's network and system infrastructure is limited to only appropriate individuals based on job function and active employment with the company. Remote access to the Company's network and system infrastructure requires multifactor authentication (MFA).

The company has logically segmented the production platform so that unrelated portions of the entity's information systems are isolated from each other.

Use of service and utility accounts are subject to biannual review and manager approval. Access to the Company's systems requires a unique username and password and MFA.

The network perimeter is controlled with security groups configured to control access based on predefined access control lists. Network and infrastructure monitoring utilities alert network administrators of issues detected by the system based on predefined alert thresholds.

Strong password complexity requirements are established and enforced in accordance with the Information Security Policy.

Sensitive authentication data such as service accounts and encryption keys are stored in a key management system. Access to sensitive authentication data is limited to only appropriate individuals based on job function and active employment with the company.

Confidentiality and Privacy

Signifyd has established confidentiality policies and procedures that define the following:

- How confidential information is protected against unauthorized access, use, and disclosure during input, processing, retention, output, and disposition
- How external access to and disclosure of confidential information is restricted to authorized parties
- The requirements for the Company to obtain written confidentiality commitments from vendors and other third-parties who have access to confidential information

The Company's Data Protection Policy outlines a data protection process, which identifies types of personal data and sensitive personal information and the related processes, systems involved in the handling of such information. Signifyd destroys data in accordance with the retention policies and as required by Service Agreements with Subscribers. The Legal team is responsible for handling privacy-related concerns (including data removal requests).

Privacy Controls Related to Choice & Consent

Signifyd provides notice of its privacy practices via its corporate website through its Terms of Service and Privacy Notice. Users have the ability to exercise their choices through the privacy portal on the website, or they can contact Signifyd at privacy@signifyd.com. Prior to utilizing the Signifyd Commerce Protection platform, Signifyd requires that subscribers enter into a service agreement and accept the organization's Privacy Notice and terms of use. This service agreement and policies communicate choices available regarding the collection, use, retention, disclosure, and disposal of personal information and the consequences, if any, of each choice. Signifyd has also recently published their Privacy Frequently Asked Questions (FAQs) for their customers, explaining their data processing practices and their legal status under various data protection laws.

Privacy Controls Related to Collection

Signifyd only collects personal information consistent with privacy commitments required for rendering services as defined in the Service Agreement, API Documentation, and Privacy Notice. Privacy Controls Related to Use, Retention, & Disposal. Signifyd retains subscriber data in accordance with applicable data protection laws, or as agreed upon through customer contracts.

Privacy Controls Related to Access

In the event that a data subject submits a data subject request directly to Signifyd, pursuant to applicable law, Signifyd reviews the data subject request and responds in accordance with its obligations under applicable data privacy laws and regulations.

Privacy Controls Related to Disclosure & Notification

Signified only enables data to be shared among third-party service providers which have been authorized for disclosure after successful completion of a third-party security and privacy assessment implemented with Security, Finance, Information Technology (IT), and Legal oversight. Signifyd limits the sharing of data with third-party service providers to only the data to which they have permission as defined in Confidentiality and Service agreements.

Formal Confidentiality and Service Agreements, which require adherence to the privacy and confidentiality requirements set forth by Signifyd, are in place for third-parties and vendors with access to personally data. Privacy related disclosures and potential disclosures identified during the incident management process are assessed by the Legal Team. Assessments are documented in accordance with the incident handling and data breach process. Unauthorized uses and disclosures that constitute a breach based on the type, sensitivity, value, and amount of personal data that is used or disclosed inappropriately are recorded and relevant parties are notified as per legal and regulatory requirements.

Privacy Criteria Related to Quality

Personal information collected by Signifyd via its API or plugins follows predefined required data fields and enforces data integrity rules. Privacy Controls Related to Monitoring & Enforcement Privacy concerns, inquiries, and complaints are reported to the privacy team. Concerns, inquiries, and complaints are captured within the ticketing system and tracked to remediation in accordance with the incident handling procedure. The Legal team monitors the continued relevance and applicability of the entity's policies and procedures related to privacy regulations, agreements, and contracts.

Computer Operations - Backups

Backups are supported by redundant AWS availability zones. The system leverages multiple data centers within these zones to ensure continued operation in the event of a failure.

Backup and restoration tests of backup data from the production system are performed at least annually.

Computer Operations - Availability

Management has implemented an Incident Response Plan (IRP) to guide timely and efficient responses to security incidents and breaches. These incidents are documented, reviewed, and tracked to final remediation, including a root cause analysis. The plan outlines internal and external communication procedures, ensuring the external communications adhere to contract and regulatory requirements. Additionally, the Company has a business continuity and disaster recovery plan, which is reviewed, tested, and updated annually.

Application-level monitoring tool sets are integrated with System and Application Insights to monitor for and respond to incidents within the application such as resource constraints, application errors, availability issues, and networking communication errors.

Monitoring tool sets are integrated with System and Application Insights to monitor for backup errors.

Any failed backups are investigated and re-run to ensure successful backups.

Change Control

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

System changes are tested, reviewed, and approved prior to implementation to the production environment. Access to make changes to source code and publish code to production is limited to only appropriate individuals based on job function and active employment with the Company. Separate environments are used for development, testing, and production. Automated alerts are in place to notify management when changes are promoted to the production environment. Version control software is in place to manage current versions of source code.

Data Communications

Firewall systems are in place to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized. Network address translation (NAT) functionality is utilized to manage internal IP addresses. Administrative access to the firewall is restricted to authorized employees.

Redundancy is built into the system infrastructure supporting the data center services to help ensure that there is no single point of failure that includes firewalls, routers, and servers. In the event that a primary system fails, the redundant hardware is configured to take its place.

Penetration testing is conducted to measure the security posture of a target system or environment. The third-party vendor uses an accepted industry standard penetration testing methodology specified by Signifyd. The third-party vendor’s approach begins with a vulnerability analysis of the target system to determine what vulnerabilities exist on the system that can be exploited via a penetration test, simulating a disgruntled/disaffected insider or an attacker that has obtained internal access to the network. Once vulnerabilities are identified, the third-party vendor attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing includes network and application layer testing as well as testing of controls and processes around the networks and applications and occurs from both outside (external testing) and inside the network.

Vulnerability scanning is performed by a third-party tool on a quarterly basis in accordance with Signifyd policy. Technologies are customized to test the organization's infrastructure and software in an efficient manner while minimizing the potential risks associated with active scanning. Findings are addressed in accordance with Signifyd’s established Vulnerability Management policy and retests and on-demand scans are performed on an as needed basis.

Authorized employees may access the system through from the Internet through the use of leading VPN technology. Employees are authenticated through the use of a token-based MFA system.

Boundaries of the System

The scope of this report includes the 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 data center hosting services, capacity management and backup services provided by AWS at multiple facilities.

This report does not include the data center hosting services, capacity management and backup services provided by GCP at multiple facilities.

Changes to the System in the Last 12 Months

No significant changes have occurred to the services provided to user entities in the 12 months preceding the end of the review period.

Incidents in the Last 12 Months

No significant incidents have occurred to the services provided to user entities in the 12 months preceding the end of the review period.

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 collect explicit consent from data subjects to collect personal information. The responsibility for collecting consent to the use of personal data lies on the end user of the Signifyd Commerce Protection Platform.

Criteria Not Applicable to the System		
Category	**Criteria**	**Reason**
	P3.2	Signifyd does not collect explicit consent from data subjects to collect personal information. The responsibility for collecting consent to the use of personal data lies on the end user of the Signifyd Commerce Protection Platform.
	P6.1	Signifyd does not collect personal information from data subjects. Instead, data subjects' personal information is provided to Signifyd by Subscribers of the platform. Subscribers of Signifyd's Commerce Protection Platform service collect personal information from data subjects and are responsible for obtaining explicit consent from data subjects.
	P6.2	Signifyd does not collect personal information from data subjects. Instead, data subjects' personal information is provided to Signifyd by Subscribers of the platform. Subscribers of Signifyd's Commerce Protection Platform service collect personal information from data subjects and are responsible for obtaining explicit consent from data subjects.
	P6.4	Signifyd does not collect personal information from data subjects. Instead, data subjects' personal information is provided to Signifyd by Subscribers of the platform. Subscribers of Signifyd's Commerce Protection Platform service collect personal information from data subjects and are responsible for obtaining explicit consent from data subjects.
	P6.5	Signifyd does not collect personal information from data subjects. Instead, data subjects' personal information is provided to Signifyd by Subscribers of the platform. Subscribers of Signifyd's Commerce Protection Platform service collect personal information from data subjects and are responsible for obtaining explicit consent from data subjects.

Subservice Organizations

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

This report does not include the data center hosting services, capacity management and backup services provided by GCP 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.

GCP provides data center hosting services, capacity management and backup services, which includes implementing physical security controls for the housed in-scope systems. Controls include but are not limited to requiring visitor sign ins, requiring badges for authorized personnel, and monitoring and logging of physical access to the facilities.

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 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.

Subservice Organization - AWS		
Category	**Criteria**	**Control**
		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.
		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.

The following subservice organization controls should be implemented by GCP to provide additional assurance that the trust services criteria described within this report are met:

Subservice Organization - GCP		
Category	**Criteria**	**Control**
Common Criteria / Security	CC6.4	Data center server floors, network rooms, and security systems are physically isolated from public spaces and/or delivery areas.
		Access to sensitive data center zones requires approval from authorized personnel and is controlled via badge readers, secondary identification mechanisms, and/or physical locks.

Subservice Organization - GCP		
Category	**Criteria**	**Control**
		Visitors to data center facilities must gain approval from authorized personnel, have their identity verified at the perimeter, and remain with an escort for the duration of their visit.
		Data center perimeters are defined and secured via physical barriers.
		Access lists to high security areas in data centers are reviewed on a periodic basis and inappropriate access is removed in a timely manner.
		Security measures utilized in data centers are assessed annually and the results are reviewed by executive management.
		Data centers are continuously staffed and monitored by security personnel through the use of real-time video surveillance and/or alerts generated by security systems.
		Visitors to corporate offices must be authenticated upon arrival and remain with an escort for the duration of their visit.
		Automated mechanisms are utilized to track inventory of production machines and inventory of all serialized server components.
Availability	A1.2	The organization's information processing resources are distributed across distinct, geographically dispersed processing facilities to support service redundancy, and availability.
		The organization conducts disaster resiliency testing which covers reliability, survivability, and recovery on an ongoing basis (and at least annually).
		The organization has implemented business continuity measures to maintain the availability of its production infrastructure and services.
		The organization maintains business continuity plans to define how personnel should respond to disruptions.
		Critical power and telecommunications equipment in data centers is physically protected from disruption and damage.
		Redundant power is utilized to support the continued operation of critical data center equipment in the event of a loss of the primary power source(s).
		Data centers are equipped with fire detection alarms and protection equipment.

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 are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity 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, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Signifyd’s.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities’ locations, user entities’ auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

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.