SOC 3 Report

System and Organization Controls Report on the Suitability of the Design and Operating Effectiveness of Controls

Description of Signifyd's Commerce Protection Platform for the period July 01, 2022, to June 30, 2023

Prepared in Accordance with the AICPA's SSAE No. 18

Table of Contents

Section I

Independent Service Auditor's Report

risk3sixty

Security | Privacy | Compliance

Section I – Independent Service Auditor's Report

risk3sixty Compliance, LLC
408 South Atlanta Street, Suite 180
Roswell, GA 30075

To: Signifyd

Scope

We have examined Signifyd's ("the Company's") accompanying assertion titled "Assertion of Signifyd Management" (assertion) that the controls within the Signifyd Commerce Protection Platform (system) were effective throughout the period July 1, 2022, to June 30, 2023, 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* (AICPA, *Trust Services Criteria*).

The accompanying assertion and the Description of the Boundaries of the Signifyd system indicate that complementary user entity controls that are suitably designed and operating effectively are necessary, along with related controls at Signifyd, to achieve Signifyd's service commitments and system requirements based on the applicable trust services criteria. The Description of the Boundaries of the Signifyd system presents the complementary user entity controls assumed in the design of Signifyd's controls. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

As indicated in the assertion, Signifyd uses subservice organizations to provide data center hosting, capacity management, platform redundancy, data storage, and backup services. The accompanying assertion and the Description of the Boundaries of the Signifyd system indicate that certain service commitments and system requirements based on the applicable trust services criteria can be met only if complementary subservice organization controls assumed in the design of the service organization's controls are suitably designed and operating effectively, along with the related controls at Signifyd. The Description of the Boundaries of the Signifyd system presents the types of complementary subservice organization controls assumed in the design of Signifyd's controls. Our examination did not include the services provided by the subservice organization, and we have not evaluated whether the controls management expects to be implemented at the subservice organizations have been implemented or whether such controls were suitably designed and operating effectively throughout the period July 1, 2022, to June 30, 2023.

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. In Section II, Signifyd has also provided the accompanying 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 and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve Signifyd's service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Signifyd's service commitments and system requirements based on the applicable trust services criteria

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Signifyd's fraud prevention system were effective throughout the period July 1, 2022, to June 30, 2023, 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.

risk3sixty compliance, LLC

Roswell, Georgia
August 17, 2023

Section II

Assertion of Signifyd's Management

Section II – Assertion of Signifyd's Management

August 17, 2023
Signifyd
99 Almaden Blvd., 4th Floor
San Jose, CA 95113

We are responsible for designing, implementing, operating, and maintaining effective controls within Signifyd's Commerce Protection Platform (system) throughout the period July 1, 2022, to June 30, 2023, to provide reasonable assurance that Signifyd's service commitments and system requirements relevant to security, availability, confidentiality, and privacy were achieved. Our description of the boundaries of the system is presented in Attachment A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period July 1, 2022, to June 30, 2023, 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* (AICPA, *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 Attachment B.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system operated effectively throughout the period July 1, 2022, to June 30, 2023, to provide reasonable assurance that Signifyd's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Signifyd's controls operated effectively throughout that period.

Attachment A

Description of the Boundaries of the Signifyd Commerce Protection Platform

risk3sixty

Security | Privacy | Compliance

Attachment A - Description of the Boundaries of the Signifyd Commerce Protection Platform

Company Background

Signifyd was founded in 2011 with the mission of empowering fearless commerce by protecting merchants from fraud, consumer abuse, and friction in the buying experience. The company has grown into a market leader in 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, CA., with locations in Denver, New York, Seattle, Mexico City, Belfast, and London.

Overview of the 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 REST 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

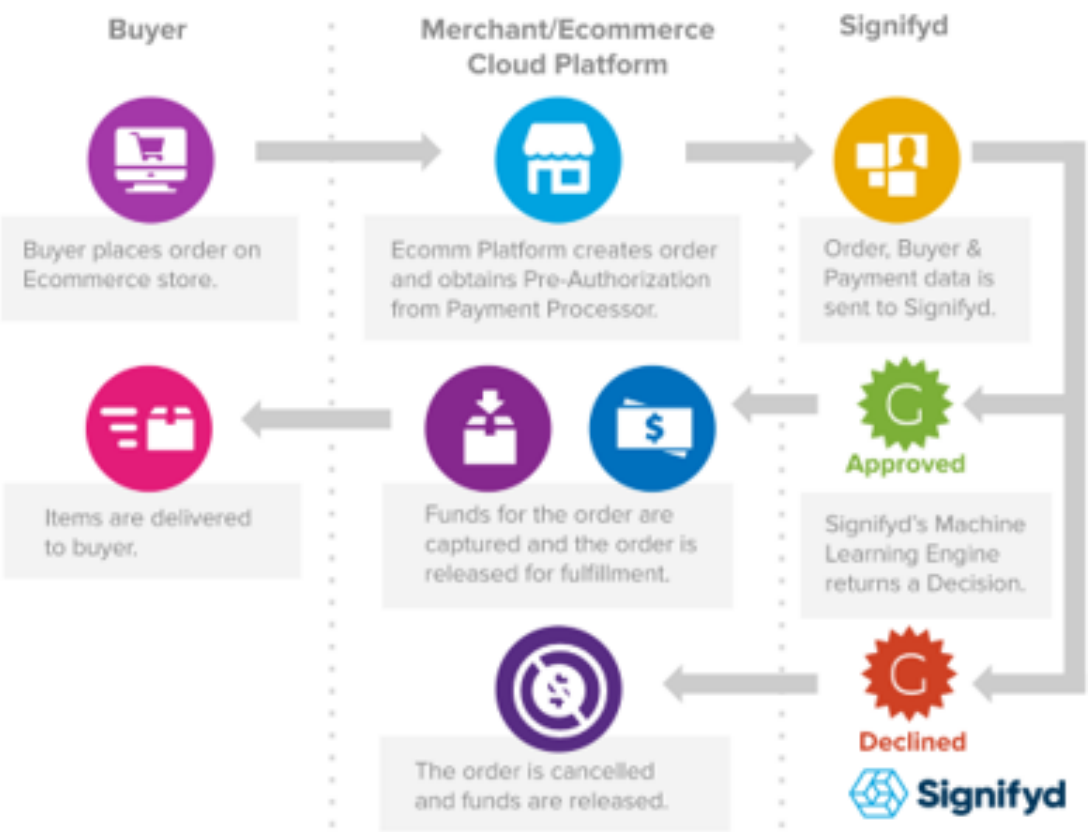
When a customer places an order with your store, Signifyd automatically reviews the order and tells you whether to ship it or not.

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.



Infrastructure

Primary hardware and software used to provide Signifyd's Commerce Protection Platform service includes the following:

Primary Hardware	
Component	**Purpose**
AWS EC2	Virtual machines running Linux Operating System – Hosts Signifyd's Commerce Protection Platform System runtime components
AWS VPC	Virtual private cloud – 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 AWS	Proprietary software developed by Signifyd to provide the Commerce Protection Platform – Various Supporting infrastructure for Signifyd microservices: • Elastic Load Balancers • Relational Database Service • DynamoDB • Redshift • S3 • Kinesis • Others
Instaclustr	Investigation datastore – Hosted Cassandra
Elastic	Search services – Elastic search
Tecton	Feature store – Used for Data Science and machine learning (ML) algorithms
Databricks	Data warehouse – Used for Data Science analysis and model training

Primary Software	
Component	**Purpose**
Datadog	Platform monitoring
PagerDuty	On-call alerting and incident management
Loggly	Application log collection and monitoring
Jagger	Log collection
Panther	SIEM and security log monitoring

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

Signifyd's production data is managed, processed, and stored in accordance with applicable laws. End 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 email address, physical address, first name, last name, birth date, age, company, job title, photo, website URLs, social network user IDs, instant messenger handles, and IP address.
- Certain credit card information, including AVS and CVV response codes, billing address, Issuer Identification Number, and last 4 digits.
- Identifiers, such as: phone number, user ID, first name, last name, physical address, email 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 BIN.
    - We do not process payments or evaluate creditworthiness.
    - We do not receive full PAN or PCI sensitive information to make fulfillment decisions; however, depending on the financial institution and how a merchant receives chargebacks, we 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
    - We 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

Processes & Procedures

Formal Signifyd IT policies and procedures describe physical security, logical access, computer operations, change control, and data communication standards. All teams are expected to adhere to the Signifyd policies and procedures that define how services should be delivered. These are located on the Company's intranet and can be accessed by any Signifyd team member.

Complementary Subservice Organization Controls

Signifyd utilizes subservice organizations to perform certain functions to improve operating and administrative effectiveness. The accompanying description includes only policies, procedures, and control activities at Signifyd, and does not include policies, procedures, and control activities at the third-party service organizations described below. The examination by the Independent Service Auditors did

not extend to policies and procedures at these subservice organizations. The most significant subservicing organizations used by the Company are shown below:

Service Provider	Description of Services	Relevant Criteria
Amazon Web Services (AWS)	Data center hosting services, capacity management, and backup services.	CC6.4;* CC7.2;* A1.2;*A1.3*
Elastic	Data storage and backup services	CC7.2*
Google Cloud Platform (GCP)	Data center hosting services, capacity management, and backup services.	CC6.4;* CC7.2;* A1.2;* A1.3*
Instaclustr	Data storage and backup services	CC7.2*

**Subservice organization is complementary to the criteria*

Complementary subservice organization controls (CSOCs) are controls that Signifyd's management assumed, in the design of the system, would be implemented by their subservice organizations and are necessary, in combination with controls at Signifyd, to provide reasonable assurance that Signifyd's service commitments and system requirements were achieved. The following subservice organizations are responsible for the respective CSOCs and Signifyd's related service commitments and system requirements can be achieved only if the CSOCs are suitably designed and operating effectively during the period addressed by the description.

Complementary Subservice Organization Controls (CSOCs) – Amazon Web Services (AWS)		
Category	Criteria	Applicable Controls
Security	CC6.4	Physical access to facilities housing the production servers is restricted to authorized personnel.
	CC7.2	Critical system components are replicated across multiple Availability Zones and backups are maintained.
Availability	A1.2 A1.3	AWS is responsible for maintaining physical systems architecture across redundant availability zones to provide high availability to the Signifyd platform.

Complementary Subservice Organization Controls (CSOCs) – Elastic		
Category	Criteria	Applicable Controls
Security	CC7.2	Critical system components are replicated across multiple Availability Zones and backups are maintained.

Complementary Subservice Organization Controls (CSOCs) – Google Cloud Platform (GCP)		
Category	Criteria	Applicable Controls
Security	CC6.4	Physical access to facilities housing the production servers is restricted to authorized personnel.
	CC7.2	Critical system components are replicated across multiple Availability Zones and backups are maintained.

Complementary Subservice Organization Controls (CSOCs) – Google Cloud Platform (GCP)		
Category	Criteria	Applicable Controls
Availability	A1.2 A1.3	GCP is responsible for maintaining physical systems architecture across redundant availability zones to provide high availability to the Signifyd platform.

Complementary Subservice Organization Controls (CSOCs) – Instaclustr		
Category	Criteria	Applicable Controls
Security	CC7.2	Critical system components are replicated across multiple Availability Zones and backups are maintained.

Complementary User Entity Control Considerations

Signifyd's services are designed with the assumption that certain controls would be implemented by user organizations. In certain situations, the application of specific controls at user organizations is necessary to achieve Signifyd's service commitments and system requirements based on the applicable trust services criteria.

This section highlights those internal control responsibilities that Signifyd believes should be present for each user organization and has considered in developing its control policies and procedures described in this report. In order for users to rely on the control structure's policies and procedures reported on herein, each user must evaluate its own internal control structure to determine if the following procedures are in place.

Furthermore, the following list of control policies and procedures is intended to address only those policies and procedures surrounding the interface and communication between Signifyd and each user. Accordingly, this list does not allege to be, and is not, a complete listing of the control policies and procedures that provide a basis for management's assertions related to the applicable trust services criteria.

Complementary User Entity Controls		
Category	Criteria	Applicable Controls
Security	CC2.3 CC9.2	User entities are responsible for understanding and complying with their contractual obligations to Signifyd.
	CC2.3 CC6.1	User entities are responsible for notifying Signifyd of changes made to technical or administrative contact information.
	CC6.1	User entities are responsible for providing Signifyd with a list of approvers for security and system configuration changes for data transmission.
	CC6.1	User entities are responsible for ensuring the supervision, management, and control of the use of Signifyd services by their personnel.
	CC7.5	User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Signifyd services

Complementary User Entity Controls		
Category	Criteria	Applicable Controls
Security & Privacy	CC2.1 CC2.3 CC7.3 CC7.4 P6.5	User entities are responsible for immediately notifying Signifyd of any actual or suspected information security breaches, including compromised user accounts, including those used for API integrations, customer console access, and secure file transfers.
Privacy	P2.1 P3.2 P6.1	User entities are responsible for implementing a mechanism for obtaining explicit consent for the collection, use, retention, disclosure, and disposal of personal information for all end users of user entity solutions utilizing the Signifyd Commerce Protection Platform.
	P5.1 P5.2 P6.7 P7.1 P8.1	User entities are responsible for correcting, amending, or appending the personal information of data subjects whose information they use on Signifyd's Commerce Protection Platform.
Availability	A1.2	User entities are responsible for maintaining their own systems of record.

Attachment B

Principal Service Commitments & System Requirements

risk3sixty

Security | Privacy | Compliance

Attachment B – Principal Service Commitments & System Requirements

Principal Service Commitments

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 Service Level Agreements
- Ensuring Quality, Accuracy, & Security of the Solution & Data Therein
- Ensuring Security, Confidentiality, & Integrity of Data Coming in Contact with Third Parties

Principal System Requirements

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.
- All data in transit over the public internet is encrypted using TLS.

Provide Uptime & Availability to the Platform & Associated Services as Stated in Service Level Agreements

- Business Continuity and Disaster Recovery processes are in place and plans are tested annually to ensure BCP/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 Solution & Data Therein

- All changes to the solution must follow a strict 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 web application penetration testing is completed to monitor the production platform for high-risk security vulnerabilities and misconfigurations.
- All public internet facing systems are segregated from the production network through network segmentation, firewalling, 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

- All authentication and data transmission to the production environment takes place over secure transmission channels (e.g., VPN, SSH, TLS).
- The Company has established a third-party risk management program and conducts pre-onboarding assessments of all vendors and annual re-assessments of its 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.