SOC 3 Report

System and Organization Controls (SOC 3) Report on the Suitability of the Design and Operating Effectiveness of Controls

Description of Signifyd’s Commerce Protection Platform for the period July 01, 2020, to June 30, 2021

Prepared in Accordance with AICPA Standard SSAE No. 18
Table of Contents

I.  Assertion of Signifyd Management ....................................................................................................................... 3
II.  Independent Service Auditor’s Report .................................................................................................................. 6
III. Signifyd’s Description of Its Commerce Protection Platform .................................................................................. 10
   a.  Overview of Company ........................................................................................................................................ 10
   b.  Overview of Solution .......................................................................................................................................... 10
   c.  Components of the System Used to Provide the Services .................................................................................. 11
   d.  Overview of Relevant Aspects of the Overall Control Environment ................................................................. 13
   e.  Complementary Subservice Organization Controls .......................................................................................... 23
   f.  Complementary User Entity Control Considerations ......................................................................................... 24
   g.  Principal Service Commitments and System Requirements ............................................................................. 27
Section I

Assertion of Signifyd Management
I. Assertion of Signifyd Management

July 28, 2021
Signifyd
2540 N 1st St 3rd Floor
San Jose, CA 95131

We have prepared the accompanying description in Section III titled “Signifyd’s Description of Its Commerce Protection Platform” throughout the period July 01, 2020, to June 30, 2021, based on the criteria for a description of a service organization’s system in DC section 200, 2018 Description Criteria for a Description of a Service Organization’s System in a SOC 2® Report, (AICPA, Description Criteria), (description criteria). The description is intended to provide report users with information about the Commerce Protection Platform that may be useful when assessing the risks arising from interactions with Signifyd’s system, particularly information about system controls that Signifyd has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, confidentiality, privacy, and availability set forth in TSP section 100, 2017 Trust Services Principles and Criteria for Security, Availability, Processing integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

Signifyd uses a subservice organization to provide data center hosting, data storage, and backup services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary along with the controls at Signifyd, to achieve Signifyd’s service commitments and system requirements based on the applicable trust services criteria. 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 organization.

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. 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.

We confirm, to the best of our knowledge and belief, that:

1. the description presents Signifyd’s Commerce Protection Platform that was designed and implemented throughout the period July 01, 2020, to June 30, 2021, in accordance with the description criteria.
2. the controls stated in the description were suitably designed throughout the period July 01, 2020, to June 30, 2021, to provide reasonable assurance that Signifyd’s service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of Signifyd’s controls throughout that period.

We, therefore, confirm the accuracy of the information provided in the accompanying description.
3. the controls stated in the description operated effectively throughout the period July 01, 2020, to June 30, 2021, 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.
Section II
Report of Independent Accountants
II. Independent Service Auditor’s Report

risk3sixty Compliance LLC
555 South Atlanta Street
Suite B500
Roswell, GA 30075

To: Signifyd

Scope

We have examined Signifyd’s accompanying assertion titled “Assertion of Signifyd Management” (Assertion) to determine that the controls within “Signifyd’s (“the Company” or “Signifyd”) Signifyd Commerce Protection Platform (System) were effective throughout the period July 01, 2020, to June 30, 2021, 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).

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 I, Signifyd has provided its assertion titled “Assertion of Signifyd Management” (Assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. Signifyd is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization’s service commitments and system requirements.

Service Auditor’s Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. 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, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the
service organization’s service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization’s system and the suitability of the design and operating effectiveness of controls involves the following:

- 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 the controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- 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
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Evaluating the overall presentation of the description

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

**Inherent Limitations**

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that each individual user may consider important to meet their informational needs.

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 of 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 policies or procedures may deteriorate.
Opinion

In our opinion, in all material respects:

- the description presents Signifyd’s Commerce Protection Platform that was designed and implemented throughout the period July 01, 2020, to June 30, 2021, in accordance with the description criteria.
- the controls stated in the description were suitably designed throughout the period July 01, 2020, to June 30, 2021, to provide reasonable assurance that Signifyd’s service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of Signifyd’s controls throughout that period.
- the controls stated in the description operated effectively throughout the period July 01, 2020, to June 30, 2021, 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.

Roswell, Georgia
July 28, 2021
Attachment A
Description of the Commerce Protection Platform
III. Signifyd’s Description of Its Commerce Protection Platform

a. Overview of Company

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 the 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, Netsuite, Miva, Accertify and ThreatMetrix. 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 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, Mexico City, Belfast and London.

b. Overview of Solution

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.

### System 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.

---

#### c. Components of the System Used to Provide the Services

**Infrastructure** – Primary infrastructure used to provide Signifyd's Commerce Protection Platform Service includes the following:

<table>
<thead>
<tr>
<th>Primary Infrastructure</th>
<th>Item</th>
<th>Detail</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS EC2</td>
<td>Virtual machines</td>
<td>running Linux Operating System</td>
<td>Hosts Signifyd’s Guaranteed Fraud Protection</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>System runtime components</td>
</tr>
<tr>
<td>AWS VPC</td>
<td>Virtual private cloud</td>
<td></td>
<td>Provides a private network for Signifyd’s</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Commerce Protection Platform</td>
</tr>
<tr>
<td>AWS VPC Gateway</td>
<td>Virtual network</td>
<td>gateway</td>
<td>Facilitates communications between components</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>running inside the VPC and the Internet</td>
</tr>
</tbody>
</table>
Software - Primary software used to provide Signifyd’s Commerce Protection Platform Services includes the following:

<table>
<thead>
<tr>
<th>Software</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signifyd microservices</td>
<td>various Proprietary software developed by Signifyd to provide the Commerce Protection Platform</td>
</tr>
<tr>
<td>AWS</td>
<td>Elastic Load Balancers Supporting infrastructure for</td>
</tr>
<tr>
<td>Instaclustr</td>
<td>Hosted Cassandra Investigation datastore</td>
</tr>
<tr>
<td>Elastic</td>
<td>Elasticsearch Search services</td>
</tr>
<tr>
<td>Datadog</td>
<td>Monitoring Platform monitoring</td>
</tr>
<tr>
<td>PagerDuty</td>
<td>Incident alerting On-call alerting and incident management</td>
</tr>
<tr>
<td>Loggly</td>
<td>Log collection Application log collection and</td>
</tr>
<tr>
<td>Panther</td>
<td>SIEM Security log monitoring</td>
</tr>
</tbody>
</table>

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
- Quality assurance team - verifies that the system complies with the functional specification through functional testing procedures
- 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
- Security and Compliance - 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 the relevant data and financial compliance requirements and other regulations. End User data is captured and utilized by Signifyd’s Commerce Protection Platform to deliver its Guaranteed Fraud Protection
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 URL’s, 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

Processes and 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.

d. Overview of Relevant Aspects of the Overall Control Environment

The Company’s internal control environment reflects the overall attitude, awareness and actions of management, the board of directors, and others concerning controls and the emphasis given to controls, as expressed by the Company’s policies, procedures, methods and organizational structure. The following is a description of the components of internal control pertaining to Signifyd’s systems.

Corporate Governance

Signifyd has a defined process to govern aspects of the business including:

Corporate Governance and Management of Employees

The Company has established standards and guidelines for management, employees, and contractor’s ethical behavior, as outlined in the company’s Employee Handbook. The handbook includes a termination policy for personnel who violate the Company's policies and procedures, which may include disciplinary action up to and including involuntary termination.

The Company maintains an organizational and management reporting structure that aligns with business objectives. The organizational chart is updated by management upon changes to the company's organizational structure.

Roles and responsibilities are defined by written job descriptions and communicated to the Company's employees upon hire, as well as to their managers and supervisors.

Management monitors personnel compliance with the code of conduct and security policies
through monitoring of customer and workforce member complaints that can be submitted to Management via email. Any deviations to the code of conduct are addressed immediately in accordance with the employee handbook.

The Company screens personnel through pre-employment background checks prior to hiring. All employees and contractors are required to sign Employee Agreements, that require employees to adhere to the Company's code of conduct, security and confidentiality policies, and procedures as part of their initial terms and conditions of employment.

Employees complete security and privacy awareness training upon hire and annually thereafter to help ensure personnel understand the entity's security and privacy commitments, policies, and requirements as defined by company policies and procedures.

Management and employee's complete performance reviews at least annually. Performance reviews are evaluated by each individual's supervisor to ensure that individual's goals and performance is in alignment with business objectives.

**Communication and Information**

Signifyd has implemented processes to communicate management’s expectations internally as well as communicate agreements, updates and pertinent information related to security and privacy to external users of the system.

**Communications within the Organization**

The company maintains security policies and procedures, which communicate objectives and responsibilities for information security, necessary to support the function of internal control. Policies and procedures are made available to employees via the Company's policy document repository.

Top level management meets at least quarterly to review the company strategy, goals, and performance objectives.

The Company has designated the Information Security Group as responsible for monitoring controls and commitments related to company security practices. Management reviews the results of internal and external security assessments on a quarterly basis. Results of these reviews are integrated into management strategy and business objectives and tracked to final remediation.

**Communications with Subscribers and End Users**

Customer responsibilities are outlined and communicated through service level agreements (SLAs).

The Company communicates relevant security and privacy commitments, which are made available on the corporate website and by written request.
System descriptions, that delineate the boundaries of the system and describe relevant system components as well as the purpose and design of the system, are made available to authorized external users via the company website.

When major changes to security and privacy commitments are made, the Company communicates these changes to impacted stakeholders via updates to the Signifyd.com website.

Security incidents and unauthorized disclosures of customer data are communicated to customers, relevant legal and regulatory authorities, and others as required by law, contract, or at the advisement of legal counsel, per the incident management policy.

**Risk Management**

Signifyd has implemented multiple processes and procedures to identify, monitor, and control for risk to the organization and its ability to meet its strategic objectives, including potential for fraud.

**Enterprise Risk Management**

The company has defined and implemented a risk management process, overseen by top level management, that includes identification of risks, the process for evaluating risks based upon identified threats, likelihood, impact, and the company's specified risk treatment plans. A formal risk assessment is completed at least annually.

Top level management formally reviews potential changes to the business, technology, and regulatory environment, including meeting with legal counsel as needed, at least annually.

The Company has designated the Information Security Group as responsible for monitoring controls and commitments related to company security practices. Management reviews the results of internal and external security assessments on a quarterly basis. Results of these reviews are integrated into management strategy and business objectives and tracked to final remediation.

The Company maintains select insurance policies to transfer risk as part of its company risk management strategy.

**Third Party Risk Management**

The Company has implemented a vendor risk management policy to govern the company's risk management program.

The Company has established a third-party risk management program and conducts annual assessments of its service providers in order to track and manage third party risk. Any issues identified during the annual assessment are tracked through to remediation.

Corporate Master Services Agreements (MSA) are established to help define third party
requirements for maintaining security and related regulatory and policy commitments.

**Monitoring Activities**

Signifyd has implemented multiple layers of monitoring activities consisting of both management activities and automated utilities.

**Management Monitoring Activities**

Management level monitoring activities include quarterly leadership meetings to review the company strategy, goals, and performance objectives, as well as review the results of internal and external security assessments which are integrated into management strategy and business objectives.

Top level management has implemented a system of internal control based on AICPA COSO 2013 and PCI DSS. The internal control environment is reviewed and updated at least annually. Management also includes annual risk assessment, external penetration tests, and internal and external vulnerability scans. Issues and risks identified as part of these assessments are tracked to remediation. Top level management also performs a review of potential changes to the business, technology, and regulatory environment, including reviews with legal counsel, as needed, at least annually.

The Company performs internal and external vulnerability scans of the system at least quarterly. The Information Security Group assesses and prioritizes the results of the scans and tracks identified issues to final remediation.

The Company engages a third party to perform an annual external penetration test of the system. Management assesses and prioritizes the results of the penetration test and tracks identified issues to final remediation.

Issues submitted by internal and external users of the system are reviewed and prioritized by Management. Prioritized issues are tracked to final remediation.

**Systematic Monitoring Activities**

The Company leverages system monitoring tools to review and report on the production platform's performance in order to support the functioning of internal control.

Anti-virus/Anti-malware software is installed on all workstations and. Antivirus/Antimalware software is configured to receive an updated virus signature at least daily. Signifyd IT receives a report of devices that have not been updated in more than 24 hours and follows up on those devices.
Access Control

The Signifyd Commerce Protection Platform solution is hosted on AWS infrastructure. Signifyd controls access to the production environments and assets through a defense in depth approach.

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 and current employment 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 multi-factor authentication.

Administrative level access to critical system components, including (databases, system infrastructure components, operating systems, and front-end application level), are restricted to appropriate individuals based on job function and current employment with the company.

The company has logically segmented the production platform so that unrelated portions of the entities information system are isolated from each other.

Use of generic or shared user accounts is prohibited. 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 multifactor authentication.

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

Password complexity standards are established to enforce include the following:

- Minimum length of 8 characters
- Complexity required
- Account lockout after 6 invalid attempts
- Last four passwords are retained and cannot be reused

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.
Governing Access to Data

All data classified as potentially sensitive is encrypted at the database level while at rest. When data cannot be encrypted at rest due to business reasons, compensating controls including VPC isolation and additional access controls are established. All data in transit over the public internet is encrypted using TLS.

Management approves and provisions new user access based upon the user’s job function and business need prior to being granted access to the system. Management removes terminated users’ access upon termination.

The Company maintains an up-to-date and complete inventory of information technology assets.

Management performs a periodic user access review of all systems at least semi-annually. Any accounts noted as inappropriate are noted and tracked to final remediation.

All media containing sensitive data including electronic, hardcopy, photocopy, etc. shall be destroyed when it is no longer needed for business or legal reasons as defined in the company’s Data Destruction Policy.

The Company has implemented mobile device management (MDM) tools that enforce mobile device hardening on company laptops, including the ability to remotely wipe devices, if needed.

Governing Physical Access

All production infrastructure is managed within AWS’ SOC 2 Type II compliant cloud computing platforms. Physical access to the corporate office is restricted to only appropriate individuals with electronic key fob access. Visitors to corporate offices must be signed in by authorized personnel before gaining access to the facility.

System Operations

Signifyd has implemented detection and monitoring utilities and procedures to identify and respond to potential vulnerabilities, malicious activities and operational anomalies.

Production Infrastructure Configuration Management

The Company has implemented detection and monitoring tools within the production environment to identify anomalies including potentially malicious activity or out of patch systems. Engineering receives alerts based on pre-defined thresholds which are logged and tracked to final remediation.

Established entity standards exist for infrastructure and software hardening and configurations of key system components and infrastructure.
The Company has implemented a configuration management policy that documents the process required for making changes to the Company's systems.

**Incident Response**

Management has implemented an incident management and response policy that outlines the requirements for responding to anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives.

Security events are documented, reviewed, and tracked to final remediation by the Signifyd Information Security team. A root cause analysis is conducted to determine the cause and mitigate the risk of such an incident occurring in the future.

Security events that may impact internal or external users, including breaches of sensitive information or loss of service, are communicated to the impacted parties in line with contract and regulatory requirements.

The Company has established a business continuity and disaster recovery plan, both of which are reviewed, tested, and updated on an annual basis.

**Change Management**

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.

All 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.

**Confidentiality**

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 confidentiality commitments from vendors and other third parties who have access to confidential information;

• the protocols for assessing the compliance with confidentiality commitments and requirements by vendors and others third parties and the corrective actions required, if necessary; and

• the protocols for the communication of changes to confidentiality commitments and requirements to internal and external users, vendors, and other third parties.

The Company’s Data Security Policy outlines a data protection process, which identifies types of personal information and sensitive personal information and the related processes, systems, and third parties involved in the handling of such information.

Signifyd erases or destroys records in accordance with the retention policies and as required by Service Agreements with Subscribers. Subscribers may inform the organization of privacy related concerns (including record removal requests) via a member of the customer service team. Requests for data removal are logged in the ticketing system and tracked to final resolution.

Privacy

Privacy Controls Related to Choice and Consent

Prior to utilizing the Signifyd Guaranteed Fraud Protection platform, Signifyd requires that subscribers enter into a service agreement and accept the organization’s privacy policy and terms of use.

Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from the end user (i.e. data subject) on behalf of the Subscriber, if required, and such consent is obtained only for the purpose for which the information is intended consistent with the entity’s privacy commitments and system requirements as defined within the Service Agreement.

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 within its Privacy policy.

Privacy Controls Related to Use, Retention, and Disposal

Signifyd retains Subscriber data in accordance with the requirements of Service Agreements with Subscribers and applicable legal and regulatory requirements.

Signifyd erases or destroys records in accordance with the retention policies and as required by Service Agreements with Subscribers. Subscribers may inform the organization of privacy related
concerns (including record removal requests) via a member of the customer service team or emailing privacy@signifyd.com. Requests for data removal are logged in the ticketing system and tracked to final resolution.

Privacy Controls Related to Access

Subscribers may access copies of end user stored personal information and other transaction data within the data management portal, where they have the ability to access end user’s stored personal information for review and, upon request, provide physical or electronic copies of that information to the data subject consistent with the entity’s privacy commitments and system requirements.

Privacy Controls Related to Disclosure and 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, IT and Legal oversight.

Third party service providers may only access the data to which they have permission as defined in Confidentiality and Service agreements.

All internal and external Signifyd web console access to data subject information is logged.

In the instance of a breach or incident related to the security or privacy of the system or end users, incidents are documented within the ticketing system and tracked to remediation, in accordance with the incident handling and data breach process.

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 identifiable information.

The Company has established a third-party risk management program and conducts annual assessments of its service providers in order to collect, track, and manage third party security controls based upon the risk presented to the business. Any issues identified during the assessment are tracked through to remediation.

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 information 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 Application Programming Interface (API) or
plugins predefines required data fields and enforces data integrity rules.

Privacy Controls Related to Monitoring and Enforcement

Subscribers and End Users may perform a "Resubmission" within the Signifyd solution to provide additional information for reconsideration in the event that an automated transaction fails or is declined.

Privacy concerns, inquiries and complaints can be reported to privacy@signifyd.com. All concerns, inquiries and complaints are captured within the ticketing system and tracked to remediation in accordance with the incident handling procedure.

The in-house Legal Team monitors the continued relevance and applicability of the entity’s policies and procedures related to privacy regulations, agreements, and contracts.

Availability

Signifyd maintains application and system level monitoring integrated across the Commerce Protection Platform environment to monitor for and respond to incidents. Incident monitoring includes those such as application errors, backup errors, availability, resource constraints, and networking communications errors.

Applications and databases that support the production environment have been strategically designed to utilize multiple availability zones of the subservice organizations.

Signifyd conducts routine backup and restoration tests of production database and the supporting infrastructure to verify the integrity and availability of critical assets.

Changes to the System During the Period

There were no changes that are likely to affect report users’ understanding of how the Commerce Protection Platform is used to provide the service during the examination period from July 01, 2020, to June 30, 2021.

Information Security Incidents

There were no system incidents during the examination period from July 01, 2020, to June 30, 2021 that were the result of controls that were not suitably designed or operating effectively, to management’s knowledge. There were also not any incidents during the specified period that resulted in a significant failure in the achievement of one or more of the Company’s service commitments or system requirements.

Criteria Not Applicable to the System

P1.1 - This criterion is not applicable to Signifyd because the company does not interact directly
with data subjects or collect information directly from data subjects. Signifyd provides its Guaranteed Fraud Protection services to businesses (Subscribers), and those businesses have the responsibility to interact and communicate with data subjects as needed.

**P5.2** – This criterion is not applicable to Signifyd because the company does not correct, amend, or append personal information provided by data subjects. The responsibility for correcting, amending, or appending personal information is the responsibility of Subscribers who collect the personal information from data subjects.

**P6.1** – This criterion is not applicable to Signifyd because the company 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 Guaranteed Fraud Protection service collect personal information from data subjects and are responsible for obtaining explicit consent from data subjects.

e. **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:

<table>
<thead>
<tr>
<th>Service Provider</th>
<th>Description of Services</th>
<th>Relevant Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon Web Services (AWS)</td>
<td>Data center hosting services, capacity management and backup services.</td>
<td>CC6.4* CC7.2*</td>
</tr>
<tr>
<td>Instaclustr</td>
<td>Data Storage and Data Backup Services</td>
<td>CC7.2*</td>
</tr>
<tr>
<td>Elastic</td>
<td>Data Storage and Data Backup Services</td>
<td>CC7.2*</td>
</tr>
</tbody>
</table>

*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

<table>
<thead>
<tr>
<th>Principle</th>
<th>Criteria</th>
<th>Applicable Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>CC6.4</td>
<td>Physical access to facilities housing the production servers is restricted to authorized personnel.</td>
</tr>
<tr>
<td></td>
<td>CC7.2</td>
<td>Critical system components are replicated across multiple Availability Zones and backups are maintained</td>
</tr>
</tbody>
</table>

### Complementary Subservice Organization Controls (CSOCs) – Instaclustr

<table>
<thead>
<tr>
<th>Principle</th>
<th>Criteria</th>
<th>Applicable Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>CC7.2</td>
<td>Critical system components are replicated across multiple Availability Zones and backups are maintained</td>
</tr>
</tbody>
</table>

### Complementary Subservice Organization Controls (CSOCs) – Elastic

<table>
<thead>
<tr>
<th>Principle</th>
<th>Criteria</th>
<th>Applicable Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>CC7.2</td>
<td>Critical system components are replicated across multiple Availability Zones and backups are maintained</td>
</tr>
</tbody>
</table>

f. **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 the Applicable Trust Services Criteria included in this report.

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.
Complimentary User Entity Control Considerations

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 API integrations, customer console access, and secure file transfers.
8. 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.
9. 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.
Attachment B
Principal Service Commitments and System Requirements
g. **Principal Service Commitments and 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 provision 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 and Integrity of Subscriber and 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 (including both structured and unstructured data) is encrypted at rest and when in transit over the public internet. In the event that data cannot be encrypted at rest due to business purposes, compensating controls including VPC isolation and additional access controls are established.

**Provide Uptime and Availability to the Platform, and 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.

**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:
Ensuring Quality, Accuracy and Security of the Solution and Data Therein

- All changes to the solution must follow a strict SDLC 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, logical access restrictions. End User access with 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.
- All authentication and data transmission to the production environment take place over secure transmission channels (i.e. VPN, SSH, TLS).

Ensuring Security, Confidentiality, and Integrity of Data Coming in Contact with Third Parties

- Vendor MSAs specify information security and confidentiality requirements for the vendor.