



OPTIMIZED
PAYMENTS

SYSTEM AND ORGANIZATION CONTROLS (SOC) 3 REPORT ON
MANAGEMENT'S ASSERTION RELATED TO ITS

Harmonize - Payment Analytics

Relevant to Security

For the period December 1, 2025 to February 28, 2026

TOGETHER WITH INDEPENDENT AUDITORS' REPORT

Prepared by:



Table of Contents

1. Independent Service Auditors' Report.....	1
Scope	1
Service Organization's Responsibilities	1
Service Auditors' Responsibilities.....	1
Inherent Limitations	2
Opinion	2
2. Assertion of Optimized Payments Management.....	3
3. Description of Optimized Payments' Harmonize - Payment Analytics.....	4
Company Background	4
Services Provided.....	4
Principal Service Commitments and System Requirements.....	4
Components of the System	5

1. Independent Service Auditors' Report

To the Management of Optimized Payments LLC (Optimized Payments)

Scope

We have examined Optimized Payments' accompanying assertion titled "Assertion of Optimized Payments Management" (assertion) that the controls within Optimized Payments' Harmonize - Payment Analytics (system) were effective throughout the period December 1, 2025, to February 28, 2026, to provide reasonable assurance that Optimized Payments' service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)* in AICPA, *Trust Services Criteria*.

Service Organization's Responsibilities

Optimized Payments 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 Optimized Payments' service commitments and system requirements were achieved. Optimized Payments has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Optimized Payments is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditors' Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether 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 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 controls were not effective to achieve Optimized Payments' 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 Optimized Payments' 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.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the 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 organizations service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Optimized Payments Harmonize - Payment Analytics were effective throughout the period December 1, 2025, to February 28, 2026, to provide reasonable assurance that Optimized Payments' service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.



San Jose, California
April 6, 2026

2. Assertion of Optimized Payments Management

We are responsible for designing, implementing, operating, and maintaining effective controls within the Optimized Payments LLC (Optimized Payments) Harmonize - Payment Analytics (system) throughout the period December 1, 2025, to February 28, 2026, to provide reasonable assurance that Optimized Payments' service commitments and system requirements relevant to Security were achieved. Our description of the boundaries of the system is presented in the section of this report titled, "Description of Optimized Payments Harmonize - Payment Analytics," (description) 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 December 1, 2025, to February 28, 2026, to provide reasonable assurance that Optimized Payments' service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus - 2022)* in AICPA, *Trust Services Criteria*.

Optimized Payments' 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 the accompanying system description.

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 December 1, 2025, to February 28, 2026, to provide reasonable assurance that Optimized Payments' service commitments and system requirements were achieved based on the applicable trust services criteria.

Signed by Optimized Payments LLC Management

April 6, 2026

3. Description of Optimized Payments' Harmonize - Payment Analytics

Company Background

Optimized Payments was founded in 2007 with the objective of simplifying payments for businesses that accept electronic payments. These solutions are delivered via strategic consulting and a proprietary cloud-based analytics platform. The organization is based in Atlanta, Georgia.

Industries served includes Retail, e-commerce, hospitality, subscriptions, insurance, B2B, healthcare, and any other large organization that is accepting electronic payments.

Services Provided

Optimized Payments provides consulting services throughout the United States and across the globe, while the entire team is based in the US. The Company was founded in 2007 to simplify payments for large organizations that accept cards.

Optimized Payments also provides cloud-hosted analytics in the United States to provide large organizations insight into their payments data and streamlines back-office processes. This enables organizations to understand insights into:

- Authorization performance and KPIs to help businesses recover more revenue
- Sales and fee data, helping business reduce costs of payments
- Streamline reconciliation of payments, to reduce manual, tedious processes
- Assisting with the management, and representment of consumer disputes for payment charges
- Support ad-hoc payments requests and analyses for our clients
- Provide custom dashboards for enterprise clients

Data is tracked through the entire lifecycle of processing, from ingestion to normalization to visualization to the clients. Various checks, balances and alerts are set up to ensure consistent processing of data.

Principal Service Commitments and System Requirements

Optimized Payments design its processes and procedures related to Payment Analytics to meet its objective for its Harmonize services

Security Commitments to customer entities are documented and communicated in the SLA and other customer agreement as well as in the description of the service offering provided online.

Security commitments are standardized and include but are not limited to the following:

- Security Principles within the fundamental designs of the optimized payments systems that are designed to permit the systems user to access the information they needed based on their role in the system while restricting them from accessing information not needed for their role use of encryption technologies to protect the customer data both at the rest and in transit
- Optimized payments establish operational requirements that support the achievement if security commitments relevant laws and regulations, and other systems requirements. Such requirements are communicated in the Optimized payments systems policies and procedures, system design documentation and contract with customers.
- Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the Harmonize systems.

Components of the System

Infrastructure

Primary Infrastructure		
Type	Hardware	Purpose
Firewall	FortiGate Firewall 200F	Filters traffic into and out of the private network supporting the corporate and VPN services.
Switches	Forti Switch S148	Connects devices on the corporate network by sending message to the specific device(s) that need to receive it
Access Points	Forti Ap PU431	Connects wireless networks and forward packets within the network or other networks.
Firewall	Azure Firewall	Filters traffic into and out of the private network supporting the cloud services
WAF	Azure Web Application Firewall	Hosts files to support the corporate web application
Azure	AKS, Key vault, Blob Storage	ETL Infrastructure Access Key security & Storage services

Software

Primary Software	
Software	Purpose
Sigma	Business Intelligence Tool
PagerDuty	Schedules and routes alerts to operations personnel

Primary Software	
Software	Purpose
Elk Stack	Log Ingestion
Microsoft Azure Entra	Provides device administration including access control policies for authentication of administrators, commands, and audit logging of managed devices
Azure DevOps	Pipeline, Code Repository, IaC code, Configurations management
Snowflake	Cloud-based dataware house used for larger data sets.

People

- Corporate - Executives, senior operations staff, and company administrative support staff, such as legal, compliance, internal audit, training, contracting, accounting, finance, human resources, and transportation provider relations. These individuals use the Engagedly primarily as a tool to measure performance at an overall corporate level. This includes reporting done for internal metrics as well as for optimized payments user entities.
- Operations - Staff that administers the scheduling and administration of Facilities and Maintenance support and reporting
- IT - Service desk, IT infrastructure, IT networking, IT system administration, software systems development and application support, information security, and IT operations personnel manage electronic interfaces and business implementation support.
 - The service desk group provides technical assistance to the optimized payments users.
 - The infrastructure, networking, and systems administration staff typically has no direct use of the Harmonize systems. Rather, it supports Optimized Payments IT infrastructure, which is used by the software. A Component systems administrator and owners will deploy the releases of the Harmonize and other software into the production environment.
 - The information security staff supports the Harmonize indirectly by monitoring internal and external security threats and maintaining current antivirus software.
 - The information security staff maintains the inventory of IT assets.
 - Data Analytics support operations to manage the user interfaces for the Harmonize systems. This includes processing user entity supplied membership and eligibility files, producing encounter claims files, and other user-oriented data.

Data

Optimized Payments categorizes data into the following key types:

- Authorization Data
- Settlement Data
- Deposit Data
- Chargeback Data
- Other Dimensional Data



This data is collected from a variety of vendors and acquirers through SFTP, API, Webhook, or other technologies. Upon acquisition, it undergoes an Extract, Transform, Load (ETL) process to ensure it is normalized and securely stored in our Snowflake data warehouse. This preparation is crucial for comprehensive analysis and reporting.

Once normalized, the data is leveraged for detailed analysis and visualization. Harmonize is used to generate a series of interactive dashboards, providing valuable insights. These dashboards are centrally managed by an administrator to ensure consistency and control over the visualized data.

Users are granted access to the dashboards through the online Auth0 Single Sign-On. Access is tightly regulated, with permissions granted exclusively to authorized personnel based on their role and client association. All data exchanges and outputs are protected with industry-standard encryption, ensuring the highest levels of security and confidentiality throughout the entire data lifecycle.

Processes, Policies, and Procedures

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

Physical Security

All data is hosted on Azure. Azure data centers do not permit physical access to Optimized Payments employees, and all operations are conducted remotely.

Logical Access

Optimized Payments uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. Resources are protected through the use of native system security and add-on software products that identify and authenticate users and validate access requests against the users' authorized roles in access control lists. In the event incompatible responsibilities cannot be segregated, Optimized Payments implements monitoring of one or more of the responsibilities. Monitoring must be performed by a superior without responsibility for performing the conflicting activities or by personnel from a separate department.

All resources are managed in the asset inventory system, and each asset is assigned an owner. Owners are responsible for approving access to the resource and for performing periodic reviews of access by role.

Employees and approved vendor personnel sign on to the Optimized Payments network using a Microsoft Entra user ID and password. Users are also required to separately sign on to any systems or applications that do not use the shared sign-on functionality of MS Entra. Passwords must conform to defined password standards and are enforced through parameter settings in the systems. These settings are part of the configuration standards and force users to change passwords at a defined interval, disable the user ID's ability to access the system and components after a specified number of unsuccessful access attempts, and mask workstation screens, requiring reentry of the user ID and password after a period of inactivity.

Employees accessing the system from outside the Optimized Payments network are required to use a token-based two-factor authentication system. Employees are issued tokens upon employment and must return the token during their exit interview. Vendor personnel are not permitted to access the system from outside the Optimized Payments network.

Customer access unique username services through the Internet using the SSL functionality of their web-browser. These customer employees must supply a valid user ID and password to gain access to customer cloud resources. Passwords must conform to password configuration requirements configured on the virtual devices using the virtual server administration account. Virtual devices are initially configured in accordance with optimized payments configuration standards, but these configuration parameters may be changed by the virtual server administration account.

Upon hire, employees are assigned to a position in the HR management system. Two days prior to the employees' start date, the HR management system creates a report of employee user IDs to be created and access to be granted. The report is used by the security service desk to create user IDs and access rules. Access rules have been pre-defined based on the defined roles. The system lists also include employees with position changes and the associated roles to be changed within the access rules.

On an annual basis, access rules for each role are reviewed by a working group composed of security Team, Operation Team, and HR personnel. In evaluating role access, group members consider job description, duties requiring segregation, and risks associated with access. Completed rules are reviewed and approved by the ISO. As part of this process, the ISO reviews access by privileged roles and requests modifications based on this review.

The HR system generates a list of terminated employees as on needed basis. This report is used by the services desk to delete employee access. On an annual basis, HR runs a list of active employees. The security service desk uses this list to suspend user IDs and delete all access roles from IDs belonging to terminated employees.

On a quarterly basis, managers review roles assigned to their direct reports. Role lists are generated by security and distributed to the managers via the event management system. Managers review the lists and indicate the required changes in the event management record. The record is routed back to the security help desk for processing. The operation or HR team identifies any records not returned within two weeks and follows up with the manager. As part of this process, the ISO reviews employees with access to privileged roles and requests modifications through the event management system.

Computer Operations – Backups

Customer data is backed up and monitored by operations personnel for completion and exceptions. In the event of an exception, operations personnel perform troubleshooting to identify the root cause and then re-run the backup job immediately or as part of the next scheduled backup job depending on customer indicated preference within the documented work instructions.

Backup infrastructure and cloud backup virtual machines and data infrastructure resides on private networks, logically secured from other networks within the Azure Data Centers.

Computer Operations – Availability

Incident response policies and procedures are in place to guide personnel in reporting and responding to information technology incidents. Procedures exist to identify, report, and act upon system security breaches and other incidents. Incident response procedures are in place to identify and respond to incidents on the network.

Optimized Payments monitors the capacity utilization of physical and computing infrastructure both internally and for customers to ensure that service delivery matches service level agreements. Optimized Payments evaluates the need for additional infrastructure capacity in response to growth of existing customers and/or the addition of new customers. Infrastructure capacity monitoring includes, but is not limited to, the following infrastructure:

- Resizing the computing resources.
- Disk Storage
- I/O operations.
- Auto Scaling & Provisioning

Optimized Payments has implemented a patch management process to ensure contracted customer and infrastructure systems are patched in accordance with vendor recommended operating system patches. Optimized Payments system owners review proposed operating system patches to determine whether the patches are applied. System Owners are responsible for determining the risk of applying or not applying patches based upon the security and availability impact of those systems and any critical applications hosted on them. Optimized Payments staff validate that all patches have been installed and if applicable that reboots have been completed.

Change Control

Optimized Payments maintains documented Systems Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality assurance testing and User Acceptance Testing (UAT) results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

Optimized Payments has implemented a patch management process to ensure contracted customer and infrastructure systems are patched in accordance with vendor recommended operating system patches. Optimized payments system owners review proposed operating system patches to determine whether the patches are applied. Optimized payments systems are responsible for determining the risk of applying or owners not applying patches based upon the security and availability impact of those systems and any critical applications hosted on them. Optimized payments staff validate that all patches have been installed and if applicable that reboots have been completed.

Data Communications

Azure 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.

Vulnerability scanning is performed by an internal security team on a scheduled basis in accordance with vulnerability and patch management program policy. The internal security team uses industry standard scanning technologies and a formal methodology specified by Optimized Payments. These technologies are customized to test the organization's infrastructure and software in an efficient manner while minimizing the potential risks associated with active scanning. Retests and on-demand scans are performed on an as needed basis. Scans are performed during non-peak windows. Tools requiring installation in the Optimized Payments internal system are implemented through the Change Management process. Scanning is performed with approved scanning templates and with bandwidth-throttling options enabled.

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 two-factor authentication system.

Boundaries of the System

The scope of this report includes the Services performed by Optimized Payments. This report does not include the data center hosting services provided by Azure.

The applicable trust services criteria and the related controls:

The Trust Services Categories that are in scope for the purposes of this report are as follows:

- **Security:** Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability or confidentiality of information or systems and affect the entity's ability to meet its objectives.

Control Environment

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of Optimized Payments control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Optimized Payments ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

Specific control activities that the service organization has implemented in this area are described below:

- Formally, documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel.
- Policies and procedures require employees sign an acknowledgment form indicating they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual.
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employee handbook.
- Background checks are performed for employees as a component of the hiring process.

Commitment to Competence

Optimized Payments management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into the requisite skills and knowledge.

Specific control activities that the service organization has implemented in this area are described below:

- Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements.
- Training is provided to maintain the skill level of personnel in certain positions.

Management's Philosophy and Operating Style

Operating style encompass a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks, and management's attitudes toward information processing, accounting functions, and personnel.

Specific control activities that the service organization has implemented in this area are described below:

- Management is periodically briefed on regulatory and industry changes affecting the services provided.
- Executive management meetings are being held to discuss major initiatives and issues that affect the business as a whole.

Organizational Structure and Assignment of Authority and Responsibility

Optimized Payments organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

Optimized Payments assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

Specific control activities that the service organization has implemented in this area are described below:

- Organizational charts are in place to communicate key areas of authority and responsibility.
- Organizational charts are communicated to employees and updated as needed.

Human Resource Policies and Practices

Optimized Payments success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top quality personnel who ensures the service organization is operating at maximum efficiency. Optimized Payments human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

Specific control activities that the service organization has implemented in this area are described below:

- New employees are required to sign acknowledgement forms for the employee handbook and a confidentiality agreement following new hire orientation on their first 7 days of employment.

Risk Assessment Process

Optimized Payments risk assessment process identifies and manages risks that could potentially affect Optimized Payments ability to provide reliable services to user organizations. This ongoing process requires that management identify significant risks inherent in products or services as they oversee their areas of responsibility. Optimized Payments identifies the underlying sources of risk, measures the impact to organization, establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks.

This process has identified risks resulting from the nature of the services provided by Optimized Payments, and management has implemented various measures designed to manage these risks. Risks identified in this process include the following:

- Operational risk – changes in the environment, staff, or management personnel.
- Strategic risk - new technologies, changing business models, and shifts within the industry.
- Compliance – legal and regulatory changes.

Optimized Payments has established an independent organizational business unit that is responsible for identifying risks to the entity and monitoring the operation of the firm's internal controls. The approach is intended to align the entity's strategy more closely with its key stakeholders, assist the organizational units with managing uncertainty more effectively, minimize threats to the business, and maximize its opportunities in the rapidly changing market environment. Optimized Payments attempts to actively identify and mitigate significant risks through the implementation of various initiatives and continuous communication with other leadership committees and senior management.

Integration with Risk Assessment

The environment in which the system operates the commitments, agreements, and responsibilities of Optimized Payments Harmonize system as well as the nature of the components of the system result in risks that the criteria will not be met. Optimized Payments addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meeting the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, Optimized Payments management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

Information and Communications Systems

Information and communication is an integral component of Optimized Payments internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations. This process encompasses the primary classes of transactions of the organization, including the dependence on, and complexity of, information technology. At optimized payments, information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, regulators, and employees.

Various weekly calls are held to discuss operational efficiencies within the applicable functional areas and to disseminate new policies, procedures, controls, and other strategic initiatives within the organization. Additionally, Annual meetings are held bi-annually in each geographic location to provide staff with updates on the firm and key issues affecting the organization and its employees. Senior executives lead the Company meetings with information gathered from formal automated information systems and informal databases, as well as conversations with various internal and external colleagues. General updates to entity-wide security policies and procedures are usually communicated to the appropriate Optimized Payments personnel via e-mail messages.

Monitoring Controls

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. Optimized Payments management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

On-Going Monitoring

Optimized Payments management conducts quality assurance monitoring on a regular basis and additional training is provided based upon results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Management's close involvement in optimized payments operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of optimized payments personnel.

Changes to the System in the Last 3 Months

No significant changes have occurred to the services provided to user entities in the 3 months preceding the end of the review date.

Incidents in the Last 3 Months

No significant incidents have occurred to the services provided to user entities in the 3 months preceding the end of the review date.

Criteria Not Applicable to the System

All relevant trust services criteria were applicable to Optimized Payments' Harmonize - Payment Analytics.

Subservice Organizations

Optimized Payments' 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 Optimized Payments' services to be solely achieved by Optimized Payments' control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Optimized Payments.

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

Security Category	
Criteria	Controls expected to be in place
CC6.1 - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Azure is responsible for implementing controls for the transmission, movement, and removal of the underlying storage devices for its cloud hosting services where the entity's system resides.
CC6.2 - Prior to issuing system credentials and granting system access, the entity registers and	

Security Category	
Criteria	Controls expected to be in place
authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	
CC6.3 - The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	
CC6.5 - The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	
CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	
CC6.7 - The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	
CC6.4 - The entity restricts physical access to facilities and protected information assets (e.g., datacenter facilities, backup media storage and other sensitive locations) to authorized personnel to meet the entity's objectives.	Azure is responsible for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers where the entity's system resides.

Optimized Payments management, along with the subservice organization, defines the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, Optimized Payments performs monitoring of the subservice organization controls, including the following procedures:

- Holding periodic discussions with vendors and subservice organization
- Reviewing attestation reports over services provided by vendors and subservice organization
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization.

Complementary User Entity Controls

Optimized Payments' 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 the SOC 2 Criteria related to Optimized Payments' services to be solely achieved by Optimized Payments' control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Optimized Payments'.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the SOC 2 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 Optimized Payments.
2. User entities are responsible for notifying Optimized Payments of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of Optimized Payments 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 Optimized Payments services.
6. User entities are responsible for providing Optimized Payments with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying Optimized Payments of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.