Global Payments US Merchant Payment Processing

System and Organization Controls for Service Organizations: Relevant to User Entities' Internal Control Over Financial Reporting (SOC 1)

For the period of November 1, 2023 through
October 31, 2024

globalpayments

Global Payments US Merchant Payment Processing

System and organization Controls for Service Organizations: Relevant to User Entities' Internal Control over Financial Reporting (SOC 1)

TABLE OF CONTENTS

Independent Service Auditors' Report **1**

Management of Global Payments' Assertion **5**

Management of Global Payments' Description of its US Merchant Payment Processing System **8**

- Scope of Report 9
- Overview of Operations 10
- Relevant Aspects of the Control Environment, Risk Assessment, Monitoring, and Communication 13
- Description of Transaction Processing 18
- Information Systems Overview 20
- Relevant Changes to Information Systems 23
- Business Process Control Activities 24
- General Information Technology Control Activities 26
- Complementary Subservice Organization Controls & Monitoring of Subservice Organizations 29
- Complementary User Entity Controls 31

Global Payments' Control Objectives and Related Controls and KPMG's Tests of Controls and Results of Tests **32**

- KPMG Overview 33
- Business Process Control Activities 34
- General Information Technology Control Activities 40

Other Information Provided by Management of Global Payments **56**

globalpayments

Section 1

Independent Service Auditors’ Report

KPMG LLP
Suite 2000
303 Peachtree Street, N.E.
Atlanta, GA 30308-3210

Independent Service Auditors’ Report

Board of Directors of Global Payments Inc.:

Scope

We have examined management of Global Payments’, doing business as “Global Payments Inc.”, “Heartland, A Global Payments Company”, and “Total System Services LLC (TSYS)” (collectively “Global Payments” or “the Company”), accompanying description of its US Merchant Payment Processing system (the System) for processing user entities’ transactions throughout the period November 1, 2023 to October 31, 2024 titled “Management of Global Payments’ Description of its US Merchant Payment Processing System” (the Description) and the suitability of the design and operating effectiveness of the controls included in the Description to achieve the related control objectives stated in the Description, based on the criteria identified in “Management of Global Payments’ Assertion” (the Assertion). The controls and control objectives included in the Description are those that management of Global Payments believes are likely to be relevant to user entities’ internal control over financial reporting, and the Description does not include those aspects of the System that are not likely to be relevant to user entities’ internal control over financial reporting.

The information included in Section 5, “Other Information Provided by Management of Global Payments” is presented by management of Global Payments to provide additional information and is not a part of the Description. Information about Management Responses to Control Testing Exceptions, Global Payments’ Business Continuity, and Disaster Recovery, and Privacy Practices has not been subjected to the procedures applied in the examination of the Description and of the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the Description and, accordingly, we express no opinion on it.

Global Payments uses the subservice organizations identified in Section 3 to perform some of the services provided to user entities that are likely to be relevant to those user entities’ internal control over financial reporting. The Description includes only the control objectives and related controls of Global Payments and excludes the control objectives and related controls of the subservice organizations. The Description also indicates that certain control objectives specified by Global Payments can be achieved only if complementary subservice organization controls assumed in the design of Global Payments’ controls are suitably designed and operating effectively, along with the related controls at Global Payments. Our examination did not extend to controls of the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The Description indicates that certain control objectives specified in the Description can be achieved only if complementary user entity controls assumed in the design of Global Payments’ controls are suitably designed and operating effectively, along with related controls at Global Payments. Our examination did not extend to such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service Organization’s Responsibilities

In Section 2, management of Global Payments has provided the Assertion about the fairness of the presentation of the Description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the Description. Global Payments is 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, specifying the control objectives and stating them in the Description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria stated in the Assertion, and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the Description.

Service Auditors' Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the Description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives 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 the examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in the Assertion, the Description is fairly presented and the controls were suitably designed and operated effectively to achieve the related control objectives stated in the Description throughout the period November 1, 2023 to October 31, 2024. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

- performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on the criteria in management's assertion
- assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description
- testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the description were achieved
- evaluating the overall presentation of the description, suitability of the control objectives stated in the description, and suitability of the criteria specified by the service organization in its assertion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

Inherent Limitations

The Description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the System that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all misstatements in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the Description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives stated in the Description, is subject to the risk that controls at a service organization may become ineffective.

Description of Tests of Controls

The specific controls tested and the nature, timing, and results of those tests are listed in Section 4.

Opinion

In our opinion, in all material respects, based on the criteria described in the Assertion:

- the Description fairly presents the System that was designed and implemented throughout the period November 1, 2023 to October 31, 2024

- the controls related to the control objectives stated in the Description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period November 1, 2023 to October 31, 2024, and subservice organizations and user entities applied the complementary controls assumed in the design of Global Payments' controls throughout the period November 1, 2023 to October 31, 2024
- the controls operated effectively to provide reasonable assurance that the control objectives stated in the Description were achieved throughout the period November 1, 2023 to October 31, 2024 if complementary subservice organization controls and complementary user entity controls, assumed in the design of Global Payments' controls, operated effectively throughout the period November 1, 2023 to October 31, 2024.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of management of Global Payments, user entities of Global Payments' System during some or all of the period November 1, 2023 to October 31, 2024, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information including information about controls implemented by user entities themselves, when assessing the risks of material misstatement of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

KPMG LLP

Atlanta, Georgia
December 11, 2024

Section 2

Management of Global Payments' Assertion

Management of Global Payments' Assertion

We have prepared the accompanying description of Global Payments Inc. doing business as "Global Payments Inc.", "Heartland, A Global Payments Company", and "Total System Services LLC ("TSYS")" (collectively "Global Payments" or "the Company") US Merchant Payment Processing system (the System) for processing user entities' transactions throughout the period November 1, 2023 to October 31, 2024 titled "Management of Global Payments' Description of its US Merchant Payment Processing System" (the Description) for user entities of the System during some or all of the period November 1, 2023 to October 31, 2024, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by subservice organizations and user entities of the System themselves, when assessing the risks of material misstatement of user entities' financial statements.

Global Payments uses subservice organizations to perform some of the services provided to user entities that are likely to be relevant to those user entities' internal control over financial reporting. The Description includes only the control objectives and related controls of Global Payments and excludes the control objectives and related controls of the subservice organizations. The Description also indicates that certain control objectives specified in the Description can be achieved only if complementary subservice organization controls assumed in the design of our controls are suitably designed and operating effectively along with the related controls at Global Payments. The Description does not extend to controls of the subservice organizations.

The Description indicates that certain control objectives specified in the Description can be achieved only if complementary user entity controls assumed in the design of Global Payments' controls are suitably designed and operating effectively, along with related controls at Global Payments. The Description does not extend to controls of the user entities. We confirm, to the best of our knowledge and belief, that:

a) The Description fairly presents the System made available to user entities of the System during some or all of the period November 1, 2023 to October 31, 2024 for processing their transactions as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the Description

   i. presents how the System made available to user entities of the System was designed and implemented to process relevant user entity transactions, including, if applicable,

      (1) the types of services provided, including, as appropriate, the classes of transactions processed;

      (2) the procedures, within both automated and manual systems, by which those services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities of the System;

      (3) the information used in the performance of the procedures, including, if applicable, related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities;

      (4) how the System captures and addresses significant events and conditions other than transactions;

      (5) the process used to prepare reports and other information for user entities;

      (6) services performed by a subservice organization, if any, including whether the carve-out method or the inclusive method has been used in relation to them;

      (7) the specified control objectives and controls designed to achieve those objectives, including, as applicable, complementary user entity controls and complementary subservice organization controls assumed in the design of the service organization's controls;

      (8) other aspects of our control environment, risk assessment process, information and communication (including the related business processes), control activities, and monitoring activities that are relevant to the services provided.

ii. includes relevant details of changes to Global Payments’ System during the period covered by the Description.

iii. does not omit or distort information relevant to Global Payments’ System, while acknowledging that the Description is prepared to meet the common needs of a broad range of user entities of the System and their auditors, and may not, therefore, include every aspect of the System that each individual user entity of the System and its auditor may consider important in its own particular environment.

b) The controls related to the control objectives stated in the Description were suitably designed and operated effectively throughout the period November 1, 2023 to October 31, 2024 to achieve those control objectives if subservice organizations and user entities applied the complementary controls assumed in the design of Global Payments' controls throughout the period November 1, 2023 to October 31, 2024. The criteria we used in making this assertion were that:

i. the risks that threaten the achievement of the control objectives stated in the Description have been identified by management of Global Payments;

ii. the controls identified in the Description would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives stated in the Description from being achieved; and

iii. the controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

Global Payments Inc.

December 11, 2024

Section 3

Management of Global Payments' Description of its US Merchant Payment Processing System

Scope of Report

As part of its overall internal controls reporting program, Global Payments Inc., doing business as “Global Payments Inc.”, “Heartland, A Global Payments Company” and “Total System Services LLC (“TSYS”)” (collectively “Global Payments” or “the Company”), management defines and determines the scope and timing of this SOC 1 report. This report addresses the Global Payments’ US Merchant Payments System, which includes the legacy TSYS (Broomfield and Omaha portfolio) merchant business (“TSYS”), the legacy Heartland merchant business (“HPY”), and legacy Global Payments merchant business (“GP”).

The scope of this report is limited to the Global Payments US Merchant Payment Processing system used to perform merchant transaction processing for US merchants, and the general computer controls that support these services which are the responsibility of Global Payments. The scope of this report also includes mass merchant pricing maintenance, funding and settlement processing, and merchant reporting.

Global Payments management recognizes that the Global Payments US Merchant Payment Processing system can be a relevant component of a customer’s information systems. Accordingly, Global Payments management has selected a twelve-month scope period (November 1, 2023 through October 31, 2024) for this Report on Controls at a Service Organization Relevant to User Entities’ Internal Control Over Financial Reporting (referred to as a SOC 1® Report).

Card transaction data exchange occurs through Visa, Inc., MasterCard International Incorporated, Discover Network, and American Express–Global Network Services. Throughout this document, these organizations are referred to as Payment Card Networks, Payment Cards, Card Associations, or Payment Brands. Additionally, data exchange with these organizations occurs through designated networks, dedicated telecommunication lines, and Internet Service Providers. Services provided by Payment Card Networks and data exchange that occurs through designated networks, dedicated telecommunication lines, and Internet Service Providers are not within the scope of this report.

Global Payments management recognizes that the purpose of this report is to communicate to user organizations and their auditors, who have a sufficient understanding of how the scope of this report is relevant to user organizations to consider the description, information on the design and operating effectiveness of controls, and any significant changes in business processes or controls during the period of November 1, 2023 to October 31, 2024. As part of ongoing operations, Global Payments makes changes to its operations and various support group roles and responsibilities to better align the business to service customers. This report reflects changes that have occurred since the last report.

Payment Card Industry Data Security Standards (PCI DSS) compliance is not included in this report; however, PCI DSS assessments are conducted at Global Payments annually.

Overview of Operations

Overview of US Merchant Payment Business

Global Payments provides payment technology solutions directly to US merchants through its US Merchant Payments business. Global Payments' has its own proprietary technology, which enables it to provide a broad suite of payment products and end-to-end processing services, including customer support. Through development of a diversified product line, Global Payments has become one of the leaders in the merchant processing industry. Not all customers subscribe to all the services offered and some services and controls described in the report may not apply to specific customers.

Specific service options include the following:

- end-to-end processing for a range of payment types;
- physical Point-Of-Sale (POS) solutions;
- online, mobile, and tablet-based payment solutions;
- e-commerce gateway services;
- security and risk management solutions;
- reporting and analytical tools; and
- other value-added services.

Payment technology services are offered under the Global Payments and Heartland brands directly to merchants, primarily through a relationship-led direct sales force, as well as referral partnerships with financial and other institutions, Independent Sales Organizations (ISOs), and integrated technology partners.

Credit and debit card transaction processing includes the processing of the world's major international Payment Brands, including American Express, Discover Card, JCB, Mastercard, UnionPay International, and Visa, as well as certain domestic debit networks. Global Payments facilitates transaction processing services, including authorization, electronic draft capture, file transfers to facilitate funds settlement, and certain exception-based, back office support services such as chargeback resolution.

As part of the funds settlement process, Global Payments uses financial institutions to facilitate funds transfers between the Payment Brands and the merchants. Depending on the nature and risk of the merchant's business, Global Payments may utilize a sponsorship model where the financial institution used to settle funds between the Payment Brand and the merchant acts as a settlement bank and maintains control of all settlement funds.

Overview of Global Payments

Global Payments Inc. (NYSE: GPN) is a leading payments technology company delivering innovative software and services to customers globally. Global Payments technologies, services, and team member expertise allow the company to provide a broad range of solutions that enable customers to operate their businesses more efficiently across a variety of channels around the world. Headquartered in Georgia with approximately 27,000 team members worldwide, Global Payments is a Fortune 500® company and a member of the S&P 500 with worldwide reach spanning North America, Europe, Asia-Pacific, and Latin America.

Global Payments aligns its business functions into two distinct operating segments to better facilitate the delivery of services to customers:

- **Merchant Solutions:** Through the Merchant Solutions segment, which includes the US Merchant Payment business, Global Payments provides payment technology and software solutions to customers globally. Global Payments technology solutions are similar around the world enabling customers to accept card, check, and digital-based payments. Global Payments offerings include, but are not limited to, authorization, settlement and funding services, customer support, chargeback resolution, terminal rental, sales and deployment, payment security services, consolidated billing, and reporting. In addition, Global Payments offers a wide array of enterprise software solutions that streamline business operations to customers in numerous vertical markets. Global Payments also provides a variety of commerce-enablement solutions and services, including specialty point-of-sale software, analytics and customer engagement, human capital management and payroll, and reporting that assist customers with driving demand and operating their businesses more efficiently.

- **Issuer Solutions:** Through the Issuer Solutions segment, Global Payments provides solutions that enable financial institutions and other financial service providers to manage their card portfolios, reduce technical complexity and overhead, and offer a seamless experience for cardholders on a single platform. In addition, Global Payments provides flexible commercial payments, accounts payable, and electronic payment solutions that support B2B payment processes for businesses and governments. Global Payments also offers complementary services including account management and servicing, fraud solution services, analytics and business intelligence, cards, statements and correspondence, customer contact solutions, and risk management solutions. Additionally, the Issuer Solutions segment provides B2B payment services and other financial service solutions marketed to businesses, including software-as-a-service ("SaaS") offerings that automate key procurement processes, provide invoice capture, coding and approval, and enable virtual cards and integrated payment options across a variety of key vertical markets.

Certain corporate support functions, including Legal, Enterprise Risk Management, Information Security, Corporate Security, Finance and Accounting, Audit Services, Technology Solutions, and Human Resources, support all operating segments. Management and oversight of each segment and the corporate functions are performed by Executive Leadership, which reports directly to the Chief Executive Officer.

Oversight by Board of Directors

Global Payments is governed by a Board of Directors elected by the shareholders. The Board of Directors is responsible for governance, oversight, and risk management of the Company's activities. The Board of Directors is composed of external business executives and meets regularly to review and approve strategic initiatives, review operating and financial results, and exercise oversight and monitoring of Global Payments' risks and internal control programs.

Leadership Oversight

Leadership oversees the operations of each Global Payments business and is responsible for strategy, product management, technology delivery and operations, business operations, customer relationship management, and all supporting corporate operations. The US Merchant business leadership team reports to Merchant Solutions leadership, which is highly experienced in the payments and financial services industry, and meets regularly to verify alignment with overall business strategy. The US Merchant business executive and senior management team play a significant role in monitoring that the control environment within the Merchant Solutions Segment is functioning properly by providing oversight for the various functional groups within the organization. Controls have been established by management and are documented in policies and procedures, which are updated and disseminated to personnel.

Global Payments Corporate Functions

Global Payments has implemented defined organizational structures for the entire enterprise, including the US Merchant business. The following corporate functions support the enablement of business operations and delivery of customer services of US Merchant business:

- **Legal:** The Legal function oversees all legal activity, including reviewing and executing contracts, managing regulatory compliance and data privacy programs, overseeing intellectual property licensing and portfolio management, and managing litigation and other dispute resolution.

- **Enterprise Risk Management:** The Enterprise Risk Management (ERM) function uses a systematic approach to evaluating and improving the effectiveness of risk management and controls to support the Company's strategic objectives. ERM assists the Company in identifying and managing enterprise risks in support of its vision, mission, and goals.

- **Information Security:** The Information Security function is responsible for creating, implementing, and maintaining a comprehensive information security program to protect the Company's information systems and data assets. The Information Security team monitors relevant regulatory industry trends and changes that may affect Global Payments and its customers. The Security Incident Response Team is part of the Information Security function.

- **Corporate Security:** Corporate Security is responsible for creating and maintaining a corporate safety and physical security policy and environment for all Global Payments facilities and team members. The Physical Security Team also ensures that access to Global Payments facilities is appropriately controlled and monitored.

- **Finance and Accounting:** The Finance and Accounting functions record, process, control, manage, and report Global Payments' financial information. Responsibilities include, but are not limited to, governance, establishment and monitoring of accounting policies and processes, oversight and monitoring of the design and effectiveness of internal controls over financial reporting, the performance of monthly accounting and forecasting activities, internal and external financial reporting, financial planning and budgeting, and the preparation, billing, and collection of customer invoices, and accounts receivable.
- **Audit Services:** The Audit Services Group (ASG) performs financial, information technology, compliance, and operational audits. The audit activities are aimed at identifying risk and compliance issues that pose challenges and concerns to the organization. ASG regularly communicates the results to the Audit and Technology Committees of the Board of Directors, executive leadership, and management. Additionally, ASG provides advisory services and staff augmentation support for external audit projects.
- **Technology Solutions:** Global Payments' Technology Solutions is responsible for the definition and execution of technology strategies for the entire company worldwide. Technology Solutions (TS) creates and deploys platforms and systems to drive success and deliver high-quality software, products, projects, and solutions.
- **Human Resources:** The Human Resources (HR) department maintains personnel policies and standards. Human resources policies and standards have been established for hiring, onboarding, employee conduct and compliance, and termination activities. The HR department communicates the policies and standards to the organization through internal communications and the intranet.

US Merchant Payments Business Operations

The following functions support the business operations of the US Merchant Payment Processing business:

- **Settlement Accounting:** The US Merchant business management system securely and accurately validates, transmits, and delivers payments on behalf of merchants. The Settlement team monitors all incoming files and applies accuracy checks for data and content validity, interchange qualification, and balancing errors and rejects.
- **Global Network Operations Center**: The Network Operations Center (GNOC) within the US Merchant segment actively monitors the US Merchant production processing environment and computer operations. The Data Transmission group is notified of failures and deviations of processing jobs and file transfers. The Data Transmission group actively works with appropriate production support personnel to resolve failures and deviations.
- **Pricing Operations:** The pricing groups within the US Merchant business update merchant pricing as necessary based on internal initiatives led by Finance or as a result of Card Association pricing changes. Pricing Operations groups review the requested pricing changes for appropriateness and perform quality control reviews over the changes once they have been entered into the system to confirm that changes were implemented completely and accurately.

Relevant Aspects of the Control Environment, Risk Assessment, Monitoring, and Communication

Control Environment

Global Payments has defined internal controls based on various industry frameworks (e.g., COSO, NIST), which are used in the design and analysis of the internal controls included in this report.

Global Payments' and the US Merchant business control environments reflect the position taken by management and the Board of Directors concerning the importance of controls and the emphasis given to controls within the Company's policies, procedures, methods, and organizational structure. The following is a description of the key elements of the control environments related to the services provided by the US Merchant business.

Segregation of Duties

Global Payments' organizational structure provides for the proper segregation of functional areas. Responsibilities are further segregated among the appropriate operating groups to prevent individuals from performing incompatible functions.

Policies and Standards

Global Payments has developed various policies and standards that cover topics such as technology operations, information security, system configuration, software and systems development, business continuity, data privacy, business conduct and ethics, and physical security. Policies and standards are updated periodically and published on the Company's intranet where all team members can access them. Global Payments has established enterprise-wide goals and objectives designed to satisfy all the information security requirements mandated by applicable laws, regulations, and industry standards. Achievement of the goals is supported by defined policies and standards for maintaining information technology and security controls.

IT specific policies and standards cover a wide variety of topics, including required security practices, data classification and handling, security awareness and training, and system capacity and performance and are reviewed and updated, as appropriate, at least annually by management. The Information Security Policy and related Information Security Standards align with the NIST Information Security Framework (CSF) and incorporate other relevant regulatory requirements. The Chief Information Security Officer (CISO) and General Counsel are responsible for reviewing the policy and standards, and the Technology Committee provides final approval.

Human Resources Policies and Practices

Global Payments adheres to the written policies and standards that govern hiring. Background checks and drug testing is performed for all employees prior to establishing employment, unless otherwise prohibited by law. A contingency clause exists in all new employment offer letters that explains that the offer is valid only upon completion of a successful background check and drug test. Employees are required to enter into a confidentiality agreement upon commencement of employment with Global Payments. These agreements explain employee duties and responsibilities to guard confidential information and trade secrets. At the inception of employment, employees also review and acknowledge the Code of Conduct and Ethics, which explains how employees should follow carefully prescribed practices to avoid conflicts of interest and practice honesty and integrity in all business dealings.

New hire orientation sessions are conducted for new employees. Additionally, all employees are required to attend annual information security training to reinforce company policies and information security responsibilities. Code of Conduct and Ethics training is also required annually for all employees, to reaffirm Global Payments' commitment to best business practices. Formal technical, business, and management leadership training programs and classes are also provided as appropriate based on role. Contingent workers granted physical and/or logical access must acknowledge the Global Payments Inc. Contingent Worker Attestation and a related behavior, security, and acceptable use policy (the GPN Requirements and Expectations Policy (Non-employee workers)), upon engagement and receive annual training on Code of Conduct and Ethics.

Employees undergo regular performance reviews by their reporting manager. Performance reviews are completed at least annually and are retained within the employees' personnel file or retained in the performance rating system records.

Upon termination of employment, notices are provided to Information Security via the Company's HR Information System (HRIS), or through a medium best suited to meet the needs of the specific function. Such mediums include direct notifications, including email, reporting, or integration with specific applications. Reports of terminated employees are provided to Identity and Access Management and system owners on a regular basis for revocation or confirmation that access has been removed. Facilities Management will revoke physical access by disabling and obtaining the terminated employee's assigned access badge.

Integrity and Ethical Values

Global Payments is committed to upholding the highest standards of ethical conduct. These standards are an integral part of Global Payments and why customers and partners choose to do business with Global Payments. The Code of Conduct and Ethics is intended to give all team members the tools to respond to situations that might violate the Company's standards and expectations. It upholds Global Payments' focus on personal accountability and Global Payments responsibility to doing the right thing as key parts of Global Payments mission and values. Global Payments' commitment to excellence is fundamental to its corporate philosophy both at Global Payments and at its affiliated companies. Global Payments team members and executive leadership share a common set of objectives and benefit from the achievement of those objectives through ethical decisions and behavior. Global Payments regularly reviews the Code of Conduct and Ethics and related policies to ensure they provide the very best guidance.

The Company's intranet site contains an EthicsPoint link and phone number where employees and third parties can raise any concerns confidently and anonymously, if preferred (except where prohibited by law). The EthicsPoint contact points are also communicated to employees in the Code of Conduct and Ethics, the GP Team Member Handbook, and referenced in the annual online compliance training. EthicsPoint reports and results are monitored and communicated to the Audit Committee of the Board of Directors on a quarterly basis.

Risk Assessment

Global Payments has implemented an Enterprise Risk Management (ERM) program that identifies and manages risks throughout the Company. The program allows management to align strategies and resources necessary to address identified risks and opportunities. In addition, the ERM team is responsible for corporate risk monitoring and reporting, information and IT risk, business continuity and disaster recovery governance, vendor risk management, client / customer assurance engagement, regional risk and compliance, and federal examiner relations.

The Client Assurance and Customer Assurance functions within ERM support customer / client reviews and distribution of Global Payments' System and Organization Controls (SOC) reports and other assurance, assertion, and attestation reports.

The Chief Risk Officer oversees ERM and is responsible for the development and implementation of risk management policies, processes and methodologies. The Chief Risk Officer provides regular reporting to the Audit and Technology Committees of the Board of Directors.

Global Payments protects the organization by integrating the principles of ERM through:

- embedding risk management into the culture and strategic decision-making of its business functions, which can lead to improved business performance;
- creating a risk-aware culture, enabling Global Payments to identify and make plans to avoid material impact on finances and operations, while encouraging the acceptance of manageable risk; and
- proactive management and monitoring of risks that may hinder the accomplishment of strategic objectives.

ERM assists in the achievement of strategic objectives by bringing a systematic approach to evaluating and continually improving the effectiveness of risk management and control, which is designed to support the continued growth and success of the Company. In addition, ERM acts as a shared service providing resources to support the business with risk monitoring / oversight, risk management program development, and where appropriate deep dives into top risks.

ERM facilitates a two-level governance committee structure which provides a risk management focus at both the operational and strategic levels.

- The first level of ERM governance is the Operational Management Risk Committee (OMRC). This committee is composed of selected members of senior management who represent all areas of the Company and collectively provide operational risk oversight and have the authority to develop and commit to risk mitigation strategies and to apply resources necessary to support agreed-upon strategies. The OMRC meets monthly and is chaired by the Chief Risk Officer. This committee receives updates from the corporate segments, key enterprise oversight departments (e.g., ERM, Information Security, Privacy, Government Relations), and other areas of interest or significance as identified by the Chief Risk Officer or committee members for cross-functional discussion.

- The second level of ERM governance is the executive Management Risk Committee (MRC). The MRC is composed of the executive leadership team: Chief Executive Officer, Chief Strategy and Transformation Officer, Chief Financial Officer, Chief Information Officer, Chief Legal and Administrative Officer, Chief Operating Officer, Segment Presidents, General Counsel, and Chief Risk Officer, which meets monthly and is focused on reviewing key existing and emerging risks and managements' strategy to mitigate those risks. The committee meetings are facilitated and organized by the Chief Risk Officer, during which reports containing summary-level information and recommendations are reviewed and, as necessary, decisions are made to further risk mitigation strategies.

In addition to management's risk assessment activities, a separate risk assessment is performed by ASG. The ASG risk assessment is designed to identify and prioritize the specific audit activities required to be performed to evaluate the design and effectiveness of financial, operational, technology, and compliance internal controls. The ASG risk assessment and audit plan are updated at least annually to reflect potential changes in the organization's risk profile, which could result from changes in structure, business strategies and operations, compliance requirements, emerging technologies, and / or new products and services.

Monitoring

Activities Conducted by the Board of Directors

The Board of Directors is bound by a charter and bylaws, and each of its committees is bound by a committee charter, which aids in ensuring appropriate governance activities. The Board of Directors is responsible for the overall governance of Global Payments and has defined its desired qualifications and skills for nomination and membership, including a requirement that the majority of the members be independent of the Company.

As part of its activities, the Board of Directors and its committees conduct an annual self-evaluation of its performance and obtain ongoing training and / or outside counsel and consultation as needed. Further, the Board of Directors meets regularly in executive sessions as well as with executive management. The Board of Directors also oversees and is responsible for approving executive succession plans to ensure continuity of management.

The Global Payments Board of Directors and Audit Committee are responsible for the oversight of ASG's activities, while Global Payments management is responsible for the risk management process. The Audit Committee is independent of Global Payments' management and holds quarterly private meetings with the Chief Audit Executive and external auditors to discuss and challenge the reasonableness of the financial reporting and internal control processes and systems.

The Technology Committee reports to the Board of Directors on matters related to IT and security, and reviews the practices and key initiatives of the Company related to IT and information security. Information Security leadership meets with the Technology Committee each quarter to present and discuss information security risks that are relevant to the organization. Information Security programs and initiatives are a standing agenda item for Committee meetings and provide an opportunity for evaluating key risks for further action. The Technology Committee holds a quarterly private meeting with the Chief Information Security Officer to further discuss matters that may be confidential in nature.

Activities Conducted by Management

Global Payments has established several groups that are charged with designing, assessing, and monitoring the Company's systems and internal control processes in addition to the aforementioned ERM processes.

- ASG conducts regular internal control assessments aimed at identifying risk and compliance issues that pose challenges and concerns to the organization and communicates these observations to the Board of Director Committees, executive leadership, and senior management.
- ERM conducts an annual assessment of the Company's risk exposure and maintains a risk inventory for distribution to management with risk ratings updated and discussed with leadership monthly.
- The IT Risk team works with the Company's information technology teams and other business groups on a proactive basis to support compliance programs and improve internal controls.
- The Legal, ERM, and Information Security groups monitor regulatory and relevant industry trends, issues, and new or changes to existing regulations and standards that may affect Global Payments and its customers. This monitoring includes, but is not limited to, issues of data security, privacy, and financial services business practices and industry regulation.

- As part of ERM Governance, ERM identifies processes, systems, environmental conditions, etc., which pose current and emerging risks to the achievement of Company objectives, as documented in the ERM risk register. Based on the register, ERM works with senior management to determine top tier (prioritized) risks, which are presented to the Board of Directors or an assigned subcommittee for additional input. On an annual rotation, ERM performs a risk analysis / deep dive evaluation on top tier risks. ERM works with senior management to establish specific risk appetites (aligning with the board-level risk appetite) and risk tolerances for objectives that relate to the top tier risks. The statements are presented to the Board of Directors or an assigned sub-committee.

Vendor Risk Management

A vendor risk management process is established by the Vendor Risk Management Program Office (VMPO) within ERM to determine the risk exposure of a vendor relationship to Global Payments. Each vendor is evaluated based on set criteria and assigned a risk ranking of Tier 1 - 4 which defines the levels of risk exposure. Tier 1 vendors are the most critical to the Company, and their risk assessments include more frequent and in-depth evaluations as well as more visibility to executive leadership. For Tier 1 vendor relationships, Quarterly Business Reviews (QBRs) are conducted by the vendor relationship manager to evaluate pertinent risk and compliance considerations, including contractual obligations such as Service Level Agreements (SLAs), business resiliency metrics, security and confidentiality, 4th-party management, and relevant reporting requirements. The VMPO conducts comprehensive vendor assessments on triennial basis and performs a review of the vendor's Report on Controls at a Service Organization (SOC) annually or as a new report becomes available to assess the vendor's internal control environment and whether controls are in place and operating effectively. Vendors not ranked as Tier 1 are assessed on a periodic basis depending on risk. For all vendors, the employee responsible for the vendor relationship monitors the competence of the third parties based on the deliverables / services provided and their interactions with the third party.

Audit Services Group

ASG provides independent, objective assurance and advisory services designed to add value and improve the operations of Global Payments. The mission of ASG is to enhance and protect organizational value by providing risk-based and objective assurance, advice, and insight. ASG helps Global Payments accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of governance, risk management, and control processes.

ASG is chartered by the Board of Directors and managed and directed by the Chief Audit Executive. The Chief Audit Executive reports functionally to the Audit Committee of the Board of Directors and administratively to the Chief Financial Officer. ASG consists of professionals with many years of audit experience in information technology, financial, operational, and compliance processes for the payments industry. Most of the Company’s internal auditors hold professional certifications. ASG operates in conformance with the Institute of Internal Auditors (IIA) professional standards when performing audits.

ASG is responsible for providing comprehensive audit coverage to all segments and businesses within Global Payments. ASG reports on a quarterly basis to senior management and the Audit and Technology Committees regarding the status of the audit plan, results of audit engagements and applicable regulatory examinations, significant risk exposures and control issues, including fraud risks and governance issues and other matters requiring the attention of, or requested by, the Audit or Technology Committees. The Global Payments Board of Directors and Audit Committee are responsible for the oversight of Internal Audit activities. Global Payments management is responsible for the risk management process.

The scope of internal audit activities encompasses, but is not limited to, objective examinations of evidence for the purpose of providing independent assessments to the Audit and Technology Committees, management, and outside parties on the adequacy and effectiveness of governance, risk management, and control processes for Global Payments. Internal audit assessments include evaluating whether:

- risks relating to the achievement of Global Payments strategic objectives are appropriately identified and managed;
- the actions of Global Payments officers, directors, employees, and contract employees are in compliance with Global Payments policies, standards, procedures, and applicable laws, regulations, and governance standards;
- the results of operations or programs are consistent with established goals and objectives;
- operations or programs are being carried out effectively and efficiently;
- established processes and systems to enable compliance with the policies, procedures, laws, and regulations that could significantly impact Global Payments;
- information and the means used to identify, measure, analyze, classify, and report such information are reliable and have integrity; and

- resources and assets are protected adequately.

ASG employs a comprehensive approach to develop the annual Internal Audit Plan, which includes areas such as evaluating the Company's key risks, considering the Company's strategic plan, evaluating planned changes to business processes and technology, and regulatory and compliance requirements. ASG conducts an annual risk assessment, which considers internal and external factors as well as fraud risk considerations. The risk assessment results are a key input for developing the annual Internal Audit Plan. Risk assessments and audit plans are updated, as necessary, throughout the year. The Audit Committee annually approves the Internal Audit Plan. ASG has policies and procedures that include the audit charter, administrative policies and standards, as well as methodology procedures.

Regulatory Review

As a financial data management and processing service provider, Global Payments is subject to regulation by federal, state, national and international regulatory agencies. Depending on the geography and segment, regulatory agencies periodically examine (via onsite and offsite processes) Global Payments' management, IT, information security, compliance, operational, risk management, and financial controls. Additionally, national and international Payment Brands perform regular onsite inspections and audits.

Contract Management

Services provided to Global Payments US Merchant customers are governed by written agreements between the parties. Such contracts include, among other things, a description of in-scope products and services, intellectual property rights, regulatory compliance obligations, Service Level Agreements (SLAs), and the parties' rights and obligations with respect to Security. Customer commitments, including committed service levels, are generally documented and managed in customer contracts. Any changes to such customer commitments would be documented in amendments or addenda to customer contracts.

Communication

Global Payments and the US Merchant business have implemented various methods of communication so employees understand their individual roles and responsibilities for transaction processing, customer servicing, control responsibilities, and to communicate significant events in a timely manner. These methods include orientation and training, team member guides (including policies and procedures), Global Payments website and intranet sites, training programs, internal newsletters and knowledge sharing, and periodic management and team member meetings. Information is identified, captured, and communicated to management to assist with maintaining the internal control program; including reports and information displays provided by finance and accounting systems, regulatory and operational compliance systems, and production systems. Relevant information includes service quality, service level compliance, and other relevant control information required to monitor and control the Company.

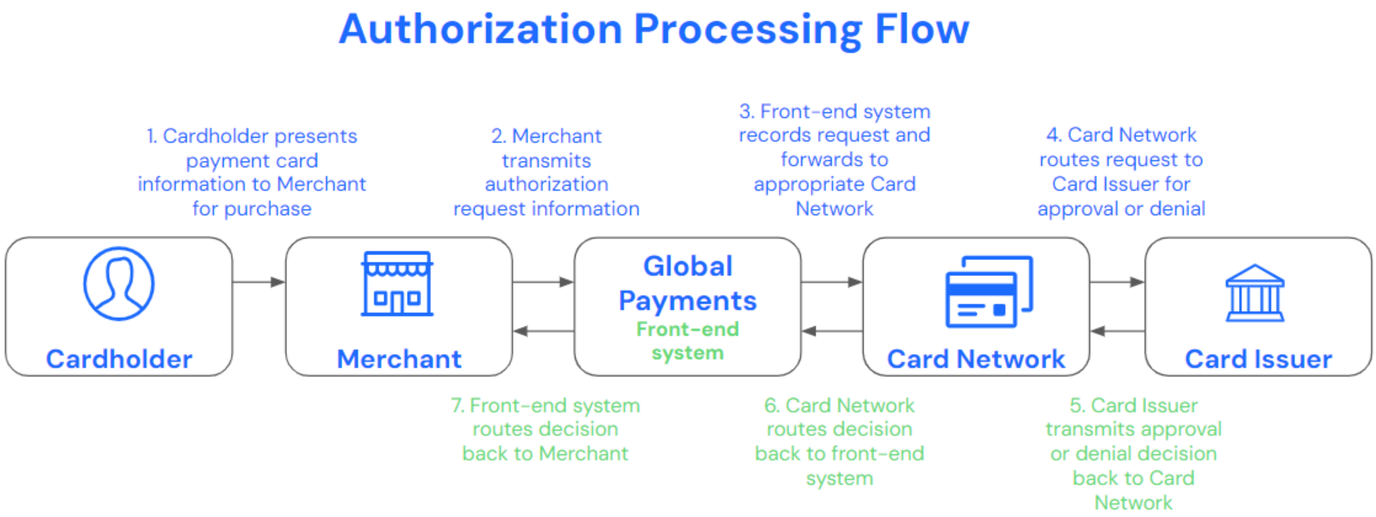
Customer communications are generally provided directly to customers through Customer Relationship Managers. These communications are provided either via email, mailer, or via a customer portal. These communications can include service and product offerings, outages, pricing changes, and regular business updates. In instances where an incident occurs or the Company needs to communicate with a broader group of customers, the Corporate Communications team, working closely with other key stakeholders, drafts the message, which is then disseminated to account and relationship managers in order to communicate to customers through the aforementioned methods.

Description of Transaction Processing

Authorization

When a cardholder initiates a payment card transaction, the payment card information is captured at the merchant Point-of-Sale (POS), terminal, or other device. The authorization request is routed to the front-end system, which then routes the transaction to the appropriate Payment Card Network. The Payment Card Network communicates with the cardholder's issuing bank (Card Issuer), which either approves or declines the transaction based on the cardholder's available balance or credit line. Once the Card Issuer has made the approval or denial, the decision is routed back to the appropriate Payment Card Network. The Payment Card Network will receive and record the approval or denial and then route the information to Global Payments' front-end system, which then communicates the approval or denial to the merchant POS or terminal device.

The diagram below provides an overview of the authorization process for US Merchant customers that utilize Global Payments for authorization processing services. The risks associated with the authorization process are addressed through the Clearing and Settlement controls, and as such, controls specific to authorization are not included in the scope of this report. This description of the authorization processing flow has been included for informational purposes.


Authorization Processing Flow
1. Cardholder presents payment card information to Merchant for purchase
2. Merchant transmits authorization request information
3. Front-end system records request and forwards to appropriate Card Network
4. Card Network routes request to Card Issuer for approval or denial
Cardholder
Merchant
Global Payments
Front-end system
Card Network
Card Issuer
7. Front-end system routes decision back to Merchant
6. Card Network routes decision back to front-end system
5. Card Issuer transmits approval or denial decision back to Card Network

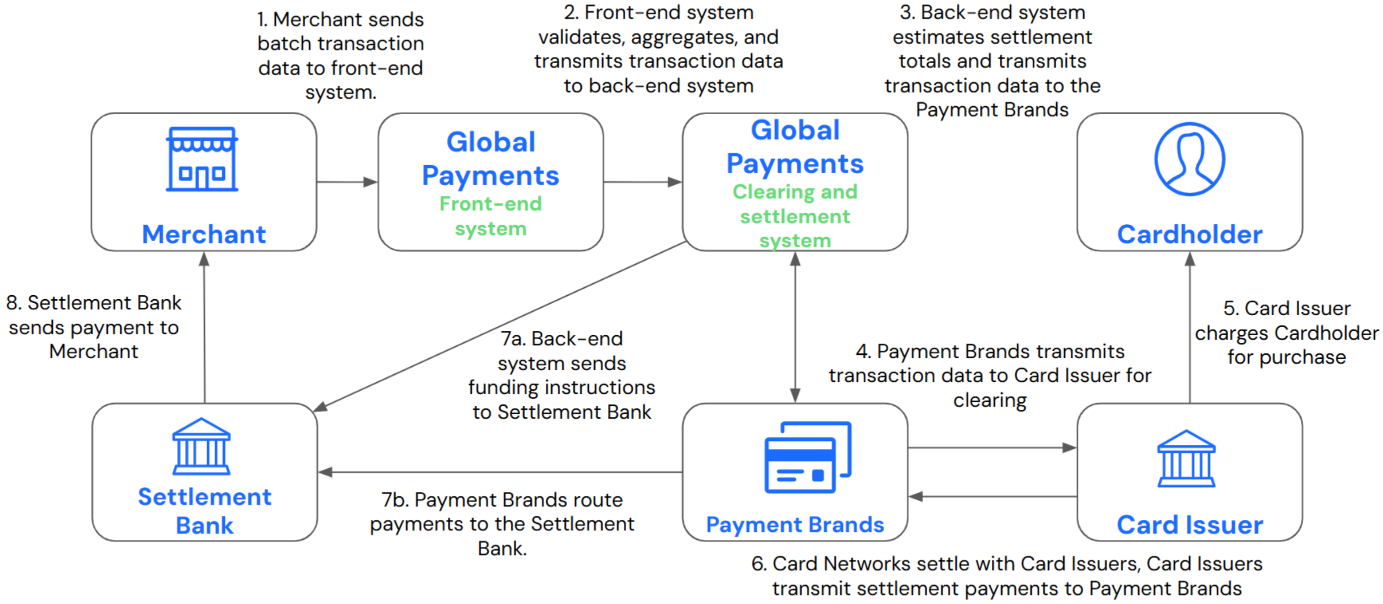
Clearing and Settlement

Upon initiation by the merchant, once or multiple times a day, a merchant will initiate a process to close the batch of transactions on the POS device. A successful batch close will trigger the front-end system to include the relevant transaction details in the next batch transaction file, also referred to as capture files, files transmitted to the clearing and settlement and funding system. Batch files are subject to a number of validations on both front-end and clearing and settlement systems to reduce errors and help ensure completeness and accuracy of processed transactions. For validated transactions, the clearing and settlement system calculates fees, estimates adjustments, and transmits the transaction data in regular settlement files sent to the Card Networks for interchange processing and clearing with the Card Issuers.

The Payment Brands settle with the Card Issuers, transmit processed settlement and funding files to the clearing and settlement system, and send monetary deposits to the Settlement bank. The clearing and settlement system processes the settlement and funding files and creates the ACH files, which includes funding instructions, to fund merchants. Once the ACH files are processed, funds are deposited by the settlement bank to merchant bank accounts.

The diagram below provides an overview of the clearing and settlement process. Applicability of the processing steps below may vary depending on the Global Payments clearing and settlement services and systems utilized for individual US Merchant customers.

Clearing and Settlement Processing Flow


1. Merchant sends batch transaction data to front-end system.
2. Front-end system validates, aggregates, and transmits transaction data to back-end system
3. Back-end system estimates settlement totals and transmits transaction data to the Payment Brands
Merchant
Global Payments Front-end system
Global Payments Clearing and settlement system
Cardholder
8. Settlement Bank sends payment to Merchant
7a. Back-end system sends funding instructions to Settlement Bank
4. Payment Brands transmits transaction data to Card Issuer for clearing
5. Card Issuer charges Cardholder for purchase
Settlement Bank
Payment Brands
Card Issuer
7b. Payment Brands route payments to the Settlement Bank.
6. Card Networks settle with Card Issuers, Card Issuers transmit settlement payments to Payment Brands

Information Systems Overview

Clearing and Settlement Systems Overview Table and Description

Clearing and Settlement System	Operating System	Database	Data Center Hosting
Global Payments Merchant Accounting System (GMAS) **Global Payments*	z-Series	IBM/DB2	QTS Suwanee (Third Party)
TSYS Merchant Accounting System (TMAS) **TSYS*	z-Series	IBM/DB2	QTS Suwanee (Third Party)
Financial Control Services (FCS) **TSYS*	z-Series	IBM/DB2	QTS Suwanee (Third Party)
Passport **Heartland*	Windows	SQL Server	Evoque through March 15, 2024 (Third Party) QTS Atlanta Metro effective March 16, 2024 (Third Party)
OnTrak **TSYS*	Windows	SQL Server	Google Cloud Platform (Third Party)
i.Balance! **Global Payments*	Linux VM	SQL Server	Google Cloud Platform (Third Party)
Frontier **Global Payments*	Windows	SQL Server	QTS Atlanta Metro and QTS Richmond (Third Party)

**Technology's legacy legal entity ownership*

Global Payments clearing and settlement systems provide merchant accounting processes for clearing and settlement. The front-end authorization systems transmit authorization and capture files to these systems where data validation routines are executed and transactions are recorded. Additionally, these systems perform analyses to estimate fees and adjustments, and submit transaction data to the Payment Brands for interchange processing. After processing, the final, adjusted transaction data is received from the Payment Brands and recorded in these systems.

The Global Payments clearing and settlement systems are used by the Settlement Accounting team to facilitate the merchant settlement process by preparing daily merchant reconciliation reports that are reviewed by the team to help ensure settlement activities between merchants and the Payment Brands are being performed completely and accurately. Additionally, the TMAS and GMAS systems aggregate merchant activity to generate merchant statements on a monthly basis for customer monitoring and reporting via scheduled jobs and initiate Automated Clearing House (ACH) funding transactions to merchants. Passport aggregates transaction data to be sent to the Third Party for statement generation.

TMAS, GMAS, and FCS execute on mainframe systems developed by Global Payments and managed by Technology Solutions. As TMAS, GMAS, and FCS are mainframe applications, they share databases and therefore have no data transfer jobs. Access to mainframe operating systems and GMAS application is controlled by CA-ACF2, an access control software package, and access to TMAS and FCS, the mainframe application systems, are controlled by the Sign-On Initiator (SONI) security system, an internally developed system that controls and monitors access by user and authenticates via a unique user ID and password.

Global Payments employee access to i.Balance! is controlled by a unique username and password. Global Payments employee access to Passport, OnTrak, and Frontier are SSO controlled at the Network or Operating System layer.

Merchant Pricing Systems Overview Table and Description

Merchant Pricing System	Operating System	Database	Data Center Hosting
Global Payments Merchant Accounting System (GMAS) **Global Payments*	z-Series	IBM/DB2	QTS Suwanee (Third Party)
HPS Enterprise (Fee Rule Manager) **Heartland*	Windows	SQL Server	Global Payments (Indiana)
OnTrak (MassTrak) **TSYS*	Windows	SQL Server	Google Cloud Platform (Third Party)
eConnections (PPM) **TSYS*	IBM AIX/Linux	Informix/DB2	Global Payments (Arizona)
MAP (WIM) **TSYS*	Windows/Linux	Oracle	QTS Suwanee (Third Party)

**Technology's legacy legal entity ownership*

The Global Payments pricing systems consist of multiple modules and applications that support the merchant boarding, credit, and pricing processes. Fee Rule Manager, MassTrak, PPM, and WIM are modules within these systems that are used to perform mass pricing updates and house merchant pricing data after initial onboarding. Additionally, for applicable, merchants pricing data is inputted and housed within the GMAS application.

Global Payments employee access to HPS Enterprise, OnTrak, and MAP are SSO controlled at the Network or Operating System layer. Global Payments employee access to eConnections is controlled via a unique user ID and password. Access to the GMAS application is controlled by CA-ACF2, an access control software package.

Relevant Changes to Information Systems

As of March 15, 2024, technology components of the in-scope application, Passport, were migrated from a third party on-prem model hosted by Evoque data center to the third party on-prem model hosted by QTS. ASG performed an audit review of the relevant IT controls relevant to the migration of Passport from Evoque data center to QTS and determined that the migration did not change the design or the functionality of the US Merchant Payment Processing system and the migration followed Global Payments change management controls.

Business Process Control Activities

Merchant Pricing

Pricing and interchange maintenance activities may be initiated for various reasons, typically either by the Global Payments Finance department or as a result of Payment Brands adjusting processing fees.

The Finance team actively reviews the pricing change requests to determine the exact mass merchant pricing changes needed. Once it is determined that a mass pricing change needs to occur, the Finance team shares the necessary updates with Pricing Operations for implementation. Appropriate personnel within the Pricing Operations team review the proposed changes prior to being imported into the system.

Following the import process, a member of the pricing operations team will perform a validation of the changes that were imported to validate that all pricing changes were implemented successfully. Any discrepancies as a result of the upload are identified and reviewed by a different member of the pricing operations team and communicated to appropriate personnel for resolution as necessary.

Funding and Settlement Processing

Global Payments uses multiple clearing and settlement systems to validate and process funding and settlement for merchant transactions. Transactions are originated by the merchant and are captured by various front-end systems as they are authorized by the Payment Brands. These systems compile the transactional information for each merchant into data files that are transmitted to Global Payments' clearing and settlement systems for processing.

Activities that support Global Payments' funding and settlement processing are performed dependent on the functionality of each legal entity's technology.

GMAS, Passport, Frontier, and i.Balance!

Once merchant transactions and batches are received from the front-end systems and transmitted to the clearing and settlement systems, a series of data validation controls are performed to help ensure the completeness and accuracy of the authorization data loaded to the clearing and settlement systems for processing. Specifically, system validation checks identify and suspend potential duplicate settlement files, which are then investigated and resolved.

Settlement systems and processes support the performance of reconciliations between pre-processing (expected to be funded) and post-processing (actual totals) at various stages of the system. Additionally, the clearing and settlement systems reconcile the incoming sales files to the outgoing files, and as part of the month end process, Settlement account reconciliations prepared monthly by the Settlement Accounting team are independently reviewed and approved by a senior Settlement Accounting team member. Unexplained items are researched, documented, resolved, and reviewed timely.

TMAS and FCS

Merchant transactions and batches are received from the front-end systems and transmitted to the clearing and settlement systems processing. Clearing and settlement systems account for adjusting transactions (e.g., rejects, reversals) and various funding and settlement requirements, calculate fees, and project the expected settlement amount as calculated by the Payment Card Networks. Any errors in processing merchant funding would be detected through this settlement process.

On a daily basis, Settlement Accounting personnel perform a Proof and Verification (P&V) balancing reconciliation to help ensure that the incoming merchant batch files received by the clearing and settlement systems (via the front-end networks) reconcile to the outgoing data file sent to the Payment Brands (by the clearing and settlement systems). This reconciliation helps ensure the accuracy of the outgoing data sent to the Payment Brands and predicts what the Payment Brands are going to send to the settlement banks after settlement. Any discrepancies are investigated and resolved as appropriate. The reconciliation is independently reviewed as evidenced by the reviewer sign off on the reconciliation.

On a daily basis, Settlement Accounting personnel prepare a Card Balancing reconciliation that compares the outgoing data file sent to the Payment Brands by the clearing and settlement systems to the return file received from the Payment Brands the next day, which identifies any adjustments and fees not initially estimated by the clearing and settlement systems. The reconciliation is independently reviewed as evidenced by the reviewer sign off on the reconciliation.

Once the expected settlement amounts are calculated by the clearing and settlement systems, ACH files are generated and sent to the settlement banks for merchant funding. Concurrently, the clearing and settlement systems send data files with the merchant transactions to the Payment Brands for processing.

After the Payment Brands process the transactions and finalize the fees and adjustments, the Payment Brands submit the settlement payment to the settlement banks to fund the merchants and transmit data files with the final adjustments and fees back to Global Payments via the clearing and settlement systems.

For the ACH files generated by the clearing and settlement systems, Settlement personnel prepare an ACH Balancing reconciliation on a daily basis that compares the sales files received to the ACH file generated by the clearing and settlement system to help ensure the completeness and accuracy of payments sent to merchants. The reconciliation is independently reviewed as evidenced by the reviewer's sign off on the reconciliation.

Merchant Reporting

Global Payments clearing and settlement systems automatically apply merchant pricing information to incoming transactions to calculate transaction processing fees, which are reflected on the merchants' monthly statement and processed during the monthly settlement process. Refer to Funding and Settlement Processing control objective for further detail.

GMAS and TMAS

The merchant monthly Statement is generated in GMAS or TMAS via automated jobs and provides merchants with transaction, rate, and billing details. Access to modify data within GMAS or TMAS is restricted to authorized personnel based on job responsibilities to help ensure merchant statements are complete and accurate.

Changes to the configuration of merchant statements are submitted as a new request through a change tracking tool, where the request is assigned to the appropriate change management team. Changes to merchant statements follow the enterprise change management process, refer to the Change Management control objective below.

Passport

The merchant monthly statement provides merchants with transaction, rate, and billing details. Transaction data from Passport is aggregated via scheduled jobs on a daily and monthly basis. Monitoring of jobs is performed and job failures are investigated and resolved.

On the first business day of the following month, the aggregated data is sent to a third-party vendor, Output Services Group (OSG), which was formerly named EverView. The third-party vendor then processes these files and generates statements for merchants.

Changes to the configuration of merchant statements are submitted to OSG for development and implementation; therefore, changes to Passport merchant statements are out of scope for this report.

General Information Technology Control Activities

Change Management

Global Payments maintains formal Software Development Life Cycle (SDLC) and change management policies that govern the intake, development, testing, and deployment of application and infrastructure changes utilizing both Agile delivery and modified Waterfall approaches. These policies govern all IT-related changes, including new or existing (modified) applications and emergency changes/fixes.

All application and infrastructure change requests are logged and tracked in the Global Payments ticketing tool. Once change requests are added to the ticketing tool, development and Quality Assurance (QA) testing activities are performed in separate environments that are logically and physically separated from the production environment. Successful completion of the QA process is required before changes are approved and deployed into production. Application testing includes functional, regression, integration, user and mock production testing, and uses the application change control release timetable. Test scripts/decks have been established and are frequently included in formal application testing.

After development activities are completed, an independent technical peer review is required and documented on the change request. The Change Advisory Board (CAB) holds regularly scheduled change control meetings with responsible stakeholders where changes are reviewed and receive final approval prior to the release into the production environment. Certain “standard” changes are pre-approved and do not require independent peer review or CAB approval. Emergency changes are defined in the Global Payments policies and must be approved by GNOC prior to the release into the production environment. Emergency changes are also subject to CAB review and approval in accordance with policies and procedures.

Where technology permits, Global Payments employs segregation of duties to protect the production environments from unauthorized changes. Users with development access are restricted from migrating source code to production environments.

Where applicable, Global Payments utilizes a code repository tool that is configured to require a code review by an independent person prior to the release to the production environment. Access to the code repository tool is restricted to appropriate individuals based on job function.

Changes promoted to production via the code repository tool are reviewed by authorized individuals to confirm the appropriateness of the change and that it followed the change management process, or to confirm changes were not developed by users with access to migrate changes.

In instances where technology does not support system-enforced segregation of duties nor system enforced peer code review, Global Payments utilizes file integrity monitoring (FIM) tools to detect unauthorized changes. FIM tools are configured to generate email alerts when completed changes are made to the production environment. The Release Deployment team, a division of Technology Solutions, reviews the changes to determine whether they were authorized and followed the change control process.

Access to change management tools (to include FIM, code repository, and deployment tools) is restricted to authorized personnel and controlled via Windows Active Directory Single Sign On. Access to the tools is reviewed periodically by management and follows the enterprise wide User Access Review process (see the Logical Access section below).

Changes to the Frontier application are managed by the software provider. No Global Payments employees have access to make changes to the production environment.

Logical Access

Global Payments has defined policies and standards for administering, maintaining, and monitoring access to the corporate Local Area Network (LAN) and in-scope systems. Documented policies and procedures exist so that standards are clearly defined, consistently applied, and appropriately communicated. Management reviews and updates the policies and standards at least annually.

Valid usernames and passwords are required as part of login credentials to authenticate users accessing Global Payments network, in-scope applications, and related databases. Access to TMAS, FCS, GMAS, Passport, MAP, OnTrak, iBalance!, Frontier, HPS Enterprise, and the supporting infrastructure is restricted via LAN access. Users have the ability to access eConnections outside of the LAN. The eConnections application follows the Global Payments password requirements as described in this section. Password configurations follow corporate standards on password rules; logical access conforms to established account and password configuration standards and comply with corporate security requirements. Management reviews and updates the policies and standards at least annually.

The Information Security, Identity and Access Management (ISIAM) group manages the administration of user access, including remote access, user additions, deletions, changes, and profile builds for the LAN, in-scope systems, and related infrastructure. Access to privileged functionality within applications and supporting infrastructure is based on the principle of least privileged access. Access to administrative or privileged functions is restricted to appropriate personnel based on job responsibilities. All access to Global Payments systems is initiated with an access request ticket, which must be approved by an authorized manager, and is processed by the ISIAM group. Remote access is managed by Global Platform Engineering, a subdivision of Technology Solutions, and requires two-factor authentication using a SecurID token device, PIN, and valid Global Payments Logon ID.

Entitlement reviews are performed quarterly to assess the appropriateness of user access to in-scope applications, operating systems, and databases. Entitlement reviews are also performed for firewalls, IPS, utilities, routers, and switches. User accounts (assigned to a person) are reviewed quarterly and service accounts (assigned to a system process) are reviewed annually.

Global Payments is in a multi-year project to convert manual entitlement reviews to an identity governance lifecycle management tool managed by Information Security. Whether the data extraction for the entitlement review is manual or automated, the system owner is responsible for documenting the completeness and accuracy of the extraction. Information Security verifies that the completeness and accuracy validation is evidenced and that the number of records extracted from the source system matches the number of records input into the identity governance lifecycle management tool or the number of records used for a manual review. Information Security is then responsible for sending the review to the appropriate parties and for following up on any reviews not completed in a timely manner. Managers review the current list of users and their entitlements to confirm that access rights comply with the policy of minimum access commensurate with an individual's job responsibilities. Required modifications to users and corresponding access rights are communicated to the appropriate groups for processing.

Information Security receives notification on a regular basis of changes to a user’s employment status, including terminations and transfers. Employee access, including administrator access, is based upon job responsibilities and access is removed or disabled upon notification of termination. Upon team member or contractor termination, managers are responsible for obtaining company hardware (e.g., laptop, badge, mobile phone). For team members, managers are responsible for initiating a termination workflow in Workday for processing by Human Resource Business Partners (HRBP) within 2 business days of the termination (or otherwise as required by local laws). For contractors, managers are responsible for initiating the termination process with local HR within 10 business days of the termination (or once all contractor agreements have been resolved) by obtaining company hardware and/or initiating the workflow in Workday. HR reviews and approves the workflow request. Upon receipt of the termination notification from HR, access is disabled within 3 business days. For transfers, access is modified to reflect the change in responsibilities as noted by the affected managers. Network access for the GP, HPY, and TSYS - Omaha portfolios are automatically disabled upon entering the termination date in the HR system, while network access for TSYS - Broomfield portfolio is manually disabled.

System Architecture

Due to system architecture, several of the in-scope applications do not allow users to modify data or affect system processing via the application-level user interface. As such, application-level logical access controls are outside the scope of this report. The specific applications that are excluded include:

- **Passport** application does not utilize a front-end user interface. All data processing occurs programmatically.
- **i.Balance!** Is a read-only system where users are not able to modify data or processing through the front-end user interface.

Data Center Physical Access

Physical security at Global Payments’ facilities is managed by Corporate Security personnel who set minimum security standards as defined within the Global Payments Physical Security Policy. The Physical Security Policy identifies physical security standards for all Global Payments facilities, including high security work areas (i.e., Data Centers).

The Corporate Security team uses the Physical Security Management System (PSMS) to manage access to Global Payments facilities. PSMS is the badging system used to restrict access to Global Payments facilities to authorized employees and visitors. Visitors to Global Payments facilities are required to present identification and sign in on a visitor log prior to access being granted to the facility. PSMS also logs badge access activities and manages badge access areas. Corporate Security personnel process access requests, monitor alarm hardware, and record physical security related events for Global Payments facilities within PSMS. Physical Security personnel monitor access 24x7 from multiple locations. The video data is retained for 90 days.

On a limited basis, visitors are permitted to access high security areas. Visitors are required to present identification and register with reception at the high security areas. The identification is used to generate a visitor badge, which contains the visitor's picture and dates(s) of their visit. The badge must be visible, and visitors but be escorted by Global Payments personnel at all times.

Global Payments data centers are equipped with intrusion alarms, surveillance cameras and related monitoring screens, zoned access card entry systems, and biometric recognition devices (multi-factor authentication), which are monitored by Corporate Security personnel. The zoned access card entry system and/or biometric recognition devices provide additional access controls in sensitive areas within the facility.

PSMS administrative access is limited to authorized Corporate Security personnel, who require physical access to log into a workstation on which PSMS software has been installed using an individual Logon ID and password for both the LAN and the PSMS system. Only a limited number of Global Payments Corporate Security personnel have administrative access to functions such as creating or modifying access privileges to include establishing clearance codes and door groups.

Badges are provisioned as part of the normal onboarding process for Global Payments team members and vendors and require management approval. Access is removed through the normal de-provisioning process based on termination notification processes (See the Logical Access section for additional information on provisioning and deprovisioning processes).

Access to the data centers is additionally restricted through other multifactor authentication, which is also managed through PSMS. Access to high security work areas is reviewed at least quarterly by area managers as facilitated by Corporate Security.

For the Kyndryl and QTS Suwanee data centers, access to and monitoring of the Global Payments cage is controlled by Global Payments and these controls are included in the scope of this report. The external physical security and environmental controls are owned and administered by Kyndryl and QTS Suwanee and are not included in the scope of this report.

For the Evoque, QTS Richmond, and QTS Atlanta Metro data centers, physical access and monitoring of sensitive areas is controlled by Evoque and QTS. The external physical security and environmental controls are owned and administered by Evoque and QTS and are not included in the scope of this report.

Global Payments does not have physical access to the Google Cloud Platform data center and physical access controls for the data center is outside the scope of this report.

Computer Operations

Global Platform Engineering utilizes job scheduling and file transfer tools to schedule and manage production jobs and file transfers. Requests for new jobs or file transfers, or modifications to existing jobs or transfers, follow the change management process and are submitted to Global Platform Engineering through the Global Payments ticketing tool. Access to the tools is restricted to authorized personnel based on job function. For TMAS, GMAS, and FCS, access to the job scheduling tools is managed through CA-ACF2. Access to the job scheduling and file transfer tools is reviewed periodically by management and follows the enterprise wide User Access Review process (See the Logical Access section above).

The Global Network Operations Center (GNOC) monitors the production processing environment and computer operations, including completion of processing jobs and file transfers, for all Global Payments systems on a 24x7 basis. GNOC personnel oversee batch job performance, downloads, data feeds (in/out), and general computer operating processes. They also respond to potential production processing incidents following established procedures. This group is supported by hardware, operating system, network engineering, and application development staff (on-call 24x7), as required to support Global Payments processing. Incidents are recorded in a ticketing tool to track and manage resolution activities.

Data is backed up at least weekly through database backup jobs. Backup jobs are scheduled and monitored through a different set of tools by Global Platform Engineering. An automated email notification is generated for any backup jobs that failed the previous day. Management verifies that failed backups are resolved per system backup procedures. Additionally, in some instances, production systems are set up and configured to support data redundancy to help prevent the loss of data.

Complementary Subservice Organization Controls & Monitoring of Subservice Organizations

Global Payments utilizes subservice organizations to support complete, accurate, and timely processing of customer transactions. Global Payments' management assesses the risks associated with these subservice organizations and has implemented various management oversight and monitoring processes to confirm that the subservice organizations that present critical risk to the Company continue to provide services in a controlled manner. These include, but are not limited to, reviewing third-party service auditor reports, holding discussions with subservice organization management, and performing periodic assessments of subservice organizations' facilities, processes, and controls.

Global Payments' controls related to the US Merchant Payment Processing system cover only a portion of overall internal controls for each user entity of Global Payments. The subservice organizations related to the US Merchant Payment Processing system are identified in the table below. These subservice organizations are not in scope for this report. A brief description of the external subservice organizations and the services they provide is listed in the table below. It is not feasible for the control objectives (CO) related to the US Merchant Payment Processing system to be achieved solely by Global Payments. Therefore, each user entity's internal control over financial reporting must be evaluated in conjunction with Global Payments' controls, the related tests and results described in Section 4 of this Report, and the related controls expected to be implemented at the subservice organizations as described below.

For the control objectives listed below, the subservice organization supports the achievement of the control objectives. The complementary subservice organization controls presented below should not be regarded as a comprehensive list of all of the controls that should be employed by the subservice organization.

Subservice Organization	Services Provided	Complementary Subservice Organization Control(s)	Control Objective Reference(s)
Output Services Group, Inc. (OSG)	Provides merchant statement generation, printing, and mailing services for merchant processing performed by the Passport application.	OSG should have relevant controls in place to produce statements in a timely manner that are complete and accurate based on the input file received by Global Payments.	CO 3: Merchant Reporting
Google Cloud Platform	Provides Infrastructure as a Service for the Ontrak and i.Balance! applications.	Google Cloud Platform should have relevant controls in place for logical access to limit access to properly authorized individuals.	CO 5: Logical Access
		Google Cloud Platform should have relevant controls in place for physical access to limit access to properly authorized individuals.	CO 6: Physical Security
Evoque Data Center Solutions (Evoque)	Provides physical space within their Data Center for the technology infrastructure supporting the Passport application from 11/1/2023 - 3/15/2024. The physical access, environmental, and external physical security controls to the Global Payments cage at the Evoque site are owned and administered by Evoque and are not included in the scope of this report.	Evoque should have relevant controls in place for physical access to limit access to properly authorized individuals.	CO 6: Physical Security

Subservice Organization	Services Provided	Complementary Subservice Organization Control(s)	Control Objective Reference(s)
Quality Technology Services (QTS)	**QTS Suwanee** Provides physical space for MAP, TMAS, and GMAS applications. The physical access controls to the Global Payments cage at the QTS site are owned and administered by Global Payments are included in this report. The environmental controls, as well as external physical security, at the QTS facilities are owned and administered by QTS and are not included in the scope of this report. **QTS Atlanta Metro and Richmond** Provides physical space within their Atlanta Metro and/or Richmond Data Center for the Frontier application. The physical access controls to the QTS sites are owned and administered by QTS and are not included in this report. The environmental controls, as well as external physical security, at the QTS facilities are owned and administered by QTS and are not included in the scope of this report.	QTS should have relevant controls in place for physical access to limit access to properly authorized individuals.	CO 6: Physical Security
Kyndryl	Provides physical space for system data back-up for the U.S. data centers. The physical access controls to the Global Payments cage at the Kyndryl site are owned and administered by Global Payments and are included in this report. The environmental controls, as well as external physical security at the Kyndryl facility are owned and administered by Kyndryl and are not included in the scope of this report.	Kyndryl should have relevant controls in place for physical access to limit access to properly authorized individuals. Kyndryl should have relevant controls in place for backing up the data for the databases for in scope applications.	CO 6: Physical Security CO 7: Computer Operations

Complementary User Entity Controls

Global Payments' controls were designed with the assumption that certain controls would be implemented by customer organizations for those control objectives and related controls specified in this report . The application of such controls by customer organizations is necessary for the achievement of certain control objectives identified in this report. Complementary user entity controls are provided for the control objectives listed below. The complementary user entity controls provided for the control objectives identified should not be regarded as a comprehensive list of controls of customer organizations.

#	Complementary User Entity Control	Relevant Control Objective(s)
1	User entities should have controls in place to notify Global Payments of inaccurate or incomplete settlement amounts.	CO 2: Funding & Settlement Processing
2	User entities should have controls in place to help ensure that transactions submitted to Global Payments are appropriately authorized, complete and accurate, and are provided to Global Payments in accordance with established schedules.	CO 1: Merchant Pricing Maintenance CO 2: Funding & Settlement Processing
3	User entities should have controls in place to help ensure that erroneous data submitted for processing is corrected and resubmitted.	CO 1: Merchant Pricing Maintenance CO 2: Funding & Settlement Processing
4	User entities should have controls in place to help ensure changes in pricing, statements, and reports are reviewed for completeness and accuracy, and reconciling output and settlement files received from Global Payments to relevant user entity control totals. User entities should contact Global Payments in a timely manner to resolve any discrepancies.	CO 1: Merchant Pricing Maintenance CO 2: Funding & Settlement Processing CO 3: Merchant Reporting
5	User entities should have controls in place to help ensure merchant funding received from Global Payments reconcile to batch-out POS transactions.	CO 2: Funding & Settlement Processing
6	User entities should have controls in place to help ensure any modifications to user-owned or managed applications and platforms that interface with Global Payments applications and platforms are appropriately tested, approved, and monitored prior to implementation.	CO 4: Change Management
7	User entities should have controls in place to help ensure that customer user accounts with access to Global Payments systems and applications (e.g., eConnections) are appropriately managed, including approval of new accounts, timely removal of access for terminated users, periodic review of user access rights, and restricting access to users with a legitimate business need.	CO 5: Logical Access
8	User entities should have controls in place to help ensure that transmissions sent from the user entities to Global Payments comply with information security requirements.	CO 7: Computer Operations
9	User entities should have controls in place to notify Global Payments of issues or problems with data file transmissions on a timely basis.	CO 7: Computer Operations

Other Information about Management's Description

Global Payments' control objectives and related controls are included in Section 4 of this report, Global Payments' Control Objectives and Related Controls and KPMG's Tests of Controls and Results of Tests. Although Global Payments' control objectives and related controls are included in Section 4, they are an integral part of Global Payments' description of the system.

Section 4

Global Payments' Control Objectives and Related Controls and KPMG's Tests of Controls and Results of Tests

KPMG Overview

This examination was performed in accordance with AICPA attest standard AT-C Section 320, which establishes the requirements and application guidance for reporting on controls at a service organization that are likely to be relevant to user entities' internal control over financial reporting.

The following table clarifies certain terms used in Section 4 to describe the nature of testing performed.

Type of Test	Description
Inquiry	Inquired of the appropriate personnel. Inquiries seeking relevant information or representation from personnel were performed to obtain among other things: • Knowledge and additional information regarding the policy or procedure. • Corroborating evidence of the policy or procedure. Note: Because inquiries were conducted on all controls, the test was not listed individually for every control shown in the accompanying matrices.
Inspection	Inspected documents and records indicating performance of the control policy or procedures. This includes among other things: • Inspection of documents or records for evidence of performance, such as the existence of initials or signatures. • Inspection of source documents and authorizations to verify propriety of transactions processed. • Inspection of reports pertaining to exceptions for assessing and determining that exceptions are properly monitored, controlled, and resolved on a timely basis. • Inspection of output control procedures and related documents and reports relative to specific transactions to ensure accurate and timely updates of records are achieved. • Inspection of all other service provider organization documentation deemed vital and pertinent.
Observation	• Observation of application of specific control policies and procedures as performed by personnel as represented. • Review input and other related controls in place for ensuring accuracy, completeness, validity, and integrity of transaction processing.
Re-performance	• Re-performed the control, or processing application of the controls, to ensure the accuracy of its operation. This includes among other things the obtaining of evidence of the accuracy and correct processing of transactions by performing independent procedures within the service provider organization.

In addition, as required by paragraph .36 of AT-C Section 205, Assertion-Based Examination Engagements (AICPA, Professional Standards), and paragraph .30 of AT-C Section 320, when using information produced (or provided) by the service organization, KPMG evaluated whether the information was sufficiently reliable for their purposes by obtaining evidence about the accuracy and completeness of such information and evaluating whether the information was sufficiently precise and detailed for their purposes.

Within the following section, controls and testing are summarized across three portfolios of the merchant business (i.e., legacy Global Payments "GP", legacy Heartland "HPY", and legacy TSYS "TSYS") and their related in-scope technology. Controls and testing have been summarized within section 4. The controls do not operate consistently across the merchant business unless noted in the tables below. Detail has been provided within the Control Activities field to demonstrate how each summarized control operates amongst the segments.

Business Process Control Activities

Control Objective 1 - Merchant Pricing Maintenance:

Controls provide reasonable assurance that mass merchant pricing maintenance activities are authorized and processed completely and accurately.

#	Global Payments' Control Activities	KPMG LLP's Tests of Controls	Results of Tests
1.01	**Pricing Change Review** Mass pricing changes are authorized by appropriate Global Payments personnel prior to uploading into the system. (*GP, HPY, TSYS*)	Inspected evidence of review for a selection of mass merchant pricing changes to determine whether changes were authorized by a member of the Pricing Operations group.	No exceptions noted.
1.02	**Pricing Change Validation** Validation checks are performed after mass pricing changes are uploaded to determine the completeness and accuracy of the change. (*GP, HPY, TSYS*)	Inspected evidence of validation activities performed for a selection of mass merchant pricing changes to determine whether each pricing change was independently reviewed after implementation and errors, if any, were resolved.	No exceptions noted.

Control Objective 2 - Funding & Settlement Processing:

Controls provide reasonable assurance that settlement files are validated for completeness and accuracy, and funding activities are processed completely and accurately.

#	Global Payments' Control Activities	KPMG LLP's Tests of Controls	Results of Tests
2.01	**Duplicate Settlement File Checks** System validation checks identify and suspend settlement files that contain potentially duplicate information. *(GP, HPY)*	**GMAS, Passport:** Inspected the configurations for identifying duplicate settlement files to determine whether the system is configured to suspend duplicate files. Observed sample settlement files that were duplicated to determine whether the files submitted were evaluated by application logic and the appropriate error messages were generated.	No exceptions noted.
2.02	**Pre-Funding Balancing** Settlement systems automatically perform reconciliation between pre-processing (expected totals) and post-processing (actual totals). Variances identified by the system are investigated and resolved. *(GP, HPY)*	**i.Balance!, Passport:** Inspected the configurations for the automatic reconciliation between pre-processing and post-processing to determine whether the systems are configured to compare expected and actual monthly totals and identify variances, if any. Inspected evidence of completed reconciliations to determine whether the settlement systems automatically perform a reconciliation between pre-processing and post-processing activities, and for variances identified by the systems, if any, inspected evidence to determine whether the variances were investigated and resolved in a timely manner.	No exceptions noted.
2.03	**Post-Funding Balancing** Settlement account reconciliations are prepared monthly by the Settlement Accounting team and independently reviewed and approved by a senior Settlement Accounting team member. Unexplained items are researched and resolved timely, and documented and reviewed. *(GP, HPY)*	**Frontier:** Inspected the Settlement account reconciliations for a selection of months to determine whether the reconciliations were performed by the Settlement Accounting team and independently reviewed and approved by a senior Settlement Accounting team member. Inspected evidence for a selection of reconciling items to determine whether the items were researched and resolved timely, documented, and reviewed.	No exceptions noted.

#	Global Payments' Control Activities	KPMG LLP's Tests of Controls	Results of Tests
2.04	**Proof & Verification Balancing** On a daily basis, Global Payments Settlement personnel perform the Proof & Verification (P&V) balancing using the clearing and settlement systems data to reconcile the sales data received from the front-end networks to the outgoing cardholder data sent to the Payment Brands. Any discrepancies are investigated and resolved by Settlement personnel. The preparer and approver initial the corresponding Proof & Verification Worksheet as evidence of review and approval. (*TSYS*)	**TMAS, FCS:** For a selection of days and systems, inspected the reconciliation performed by management and • reperformed the Proof & Verification reconciliation to determine whether balances agreed to source data (supporting screens from the clearing and settlement systems), • reperformed the variance calculation to determine whether the reconciliation was performed completely and accurately, • inspected support for any discrepancies to determine whether they were investigated and resolved by Settlement personnel, and • inspected the Proof & Verification Worksheet to determine whether the reconciliation was reviewed by a separate individual.	No exceptions noted.
2.05	**Payment Brand Balancing** On a daily basis, Global Payments Settlement personnel perform the Card Balancing reconciliation processes for each of the card types using the clearing and settlement systems data. Outgoing file totals are compared to the next day's incoming file reports for each card type. If the reports do not balance, Settlement personnel research and resolve as appropriate. The preparer and approver initial the corresponding worksheet as evidence of review and approval. (*TSYS*)	**TMAS, FCS:** For a selection of days and Payment Brands, inspected the reconciliation performed by management and • reperformed the Card Balancing reconciliation to determine whether balances agreed to source data (supporting screens from the clearing and settlement systems), • reperformed the variance calculation to determine whether the reconciliation was performed completely and accurately, • inspected support for any discrepancies to determine whether they were investigated and resolved by Settlement personnel, and • inspected the Card Balancing worksheet to determine whether the reconciliation was reviewed by a separate individual.	No exceptions noted.

#	Global Payments' Control Activities	KPMG LLP's Tests of Controls	Results of Tests
2.06	**ACH Balancing** On a daily basis, the Global Payments Settlement personnel balances payments to merchants by reconciling the sales files against the ACH payments generated by the clearing and settlement systems as evidenced in the ACH Balancing Worksheet. The preparer initials the corresponding ACH Balancing Worksheet as evidence of review and approval. (*TSYS*)	**TMAS, FCS:** For a selection of days, inspected the reconciliation performed by management and • reperformed the ACH reconciliation by agreeing balances to source data (supporting sales files against the ACH payments generated by the clearing and settlement systems), • reperformed the variance calculation to determine whether the reconciliation was performed completely and accurately, • inspected support for any discrepancies to determine whether they were investigated and resolved by Settlement personnel, and • inspected the ACH Balancing worksheet to determine whether the reconciliation was reviewed by a separate individual.	No exceptions noted.

Control Objective 3 - Merchant Reporting:

Controls provide reasonable assurance that merchant statements are complete, accurate, and generated on a timely basis.

#	Global Payments' Control Activities	KPMG LLP's Tests of Controls	Results of Tests
3.01	**Transaction Pricing Calculations** Systems automatically apply merchant pricing information to transactions to calculate transaction processing fees. *(GP, HPY, TSYS)*	**GMAS, TMAS, Passport:** For selected merchants, recalculated a selection of transaction processing fees to determine whether the system calculated the transaction processing fees accurately.	No exceptions noted.
3.02	**Merchant Statements** On a monthly basis, merchant statements are generated completely, accurately, and timely. *(GP, TSYS)*	**GMAS, TMAS:** Inspected the scheduling configuration to determine whether the statements are generated timely on a monthly basis. Inspected an example merchant's monthly statement and source systems to determine whether the data displayed within the source system of record matched the data displayed within the merchant statement.	No exceptions noted.
3.03	**Merchant Statement Changes** Changes to statements are documented, tested for completeness and accuracy, and approved by management prior to migration to production. *(GP, TSYS)*	**GMAS, TMAS:** Inspected supporting documentation for a selection of changes to merchant statements to determine whether changes were documented, tested for completeness and accuracy, and approved by management before the changes were implemented in the production environment.	No exceptions noted.

#	Global Payments' Control Activities	KPMG LLP's Tests of Controls	Results of Tests
3.04	**Reporting Configuration Access** Access to modify reporting configurations is restricted to authorized personnel based on job responsibilities. *(GP, TSYS)*	**GMAS, TMAS:** Inspected system generated listings for users with the ability to modify reporting configurations to determine whether access was restricted to authorized individuals based on inquiry with the system owner and inspection of job titles and responsibilities.	No exceptions noted.
3.05	**Data Aggregation** Transaction data for monthly merchant statements is aggregated via scheduled jobs. Jobs are monitored and failures are resolved. *(HPY)*	**Passport:** Inspected the configuration for aggregating transaction data for monthly merchant statements to determine whether transaction data for monthly merchant statements is aggregated via scheduled jobs. Inspected an example merchant's monthly statement to determine whether the data displayed within the source system of record matched the data displayed within the merchant statement. Inspected evidence for a selection of job failures to determine whether job failures were monitored and resolved.	No exceptions noted.

General Information Technology Control Activities

Control Objective 4 - Change Management:

Controls provide reasonable assurance that development of new systems and changes to existing systems are documented, tested, and approved.

#	Global Payments' Control Activities	KPMG LLP's Tests of Controls	Results of Tests
4.01	**Change Tracking Tools** Change tracking tools are used to track and document requested changes to the production processing environment. (*GP, HPY, TSYS*)	Inspected the last modification date of the systems and agreed to the corresponding change ticket to determine whether the changes were tracked using a change tracking tool.	No exceptions noted.
4.02	**Change Testing and Approval** Production systems and application changes (including emergency changes) must be tested and approved in accordance with policy requirements prior to being deployed in the production processing environment. (*GP, HPY, TSYS*)	Inspected the SDLC and Change Management Policy to determine whether the policy outlines the process for documenting the testing and approval of changes prior to implementation to production. Inspected supporting documentation, including change tickets, for a selection of changes to determine whether changes were tested and approved before the changes were implemented in the production processing environment. Inspected documentation supporting Global Payments ASG's review of the IT controls relevant to the migration of Passport from Evoque data center to QTS to determine whether the migration of the Passport application from Evoque to QTS hosting did not change the design or the functionality of the US Merchant Payment Processing system, and the migration followed Global Payments change management controls.	No exceptions noted.

#	Global Payments' Control Activities	KPMG LLP's Tests of Controls	Results of Tests
4.03	**Segregation of Duties** Global Payments employs segregation of duties so that accounts with development access are restricted from migrating source code to production. *(GP, TSYS)*	**TMAS, GMAS, FCS, Passport, eConnections:** Inspected a system generated listing of accounts with access to development and code migration functions to determine whether accounts with development access were restricted from migrating source code to production.	**Exception noted:** For the Passport application, four out of nine accounts with development access have the ability to migrate source code to production. **Management's response:** See Section 5.
4.04	**Peer Review Configuration** Production systems are configured to restrict developers from deploying their own changes to the production environment without secondary approval. *(GP, HPY)*	**i.Balance!:** Inspected approval configurations for in-scope repositories to determine whether approvals by someone other than the developer were systematically enforced. Inspected system generated listings for users with the ability to modify configurations to determine whether access was restricted to authorized individuals based on inquiry with the system owner and inspection of job titles and responsibilities. **HPS Enterprise (Fee Rule Manager):** Inspected approval configurations for in-scope repositories to determine whether approvals were systematically enforced. Inspected system generated listings for users with the ability to modify configurations to determine whether access was restricted to authorized individuals based on inquiry with the system owner and inspection of job titles and responsibilities.	No exceptions noted.

#	Global Payments' Control Activities	KPMG LLP's Tests of Controls	Results of Tests
4.05a	**Review of Changes Promoted to Production** At least twice annually, management performs a review of changes promoted to production to confirm the appropriateness of the change and that it followed the change management process. *(GP, HPY)*	**i.Balance!, HPS Enterprise (Fee Rule Manager):** Inspected documentation of management's reviews to determine whether management reviewed all changes promoted to production to confirm the appropriateness of the change and that it followed the change management process.	No exceptions noted.
4.05b	**Review of Changes Promoted to Production** Beginning in August 2024, management performs a monthly review of changes promoted to production to confirm changes were not developed by users with access to migrate changes. *(HPY)*	**Passport:** For a selection of months beginning in August 2024, inspected documentation of management's reviews to determine whether management reviewed all changes promoted to production to confirm changes were not developed by users with access to migrate changes. Additionally, determined that the first monthly review performed in August included a review of all changes since the beginning of the examination period.	No exceptions noted.

#	Global Payments’ Control Activities	KPMG LLP’s Tests of Controls	Results of Tests
4.06	**File Integrity Monitoring** File Integrity Monitoring tools are configured in accordance with policies and procedures to detect changes to production systems and applications. Changes are reviewed to determine if they were authorized and followed the change control process. *(TSYS)*	**OnTrak:** For a selection of alerts, reperformed management’s review to determine whether changes to production systems and applications were logged, monitored, and resolved as appropriate. Inspected the File Integrity Monitoring tools configurations to determine whether the tool was utilized to monitor the integrity of the operating system and applications on production platforms. Further inspected the configuration within File Integrity Monitoring tools to determine whether the tool was configured to generate automated email alerts to application teams when changes were made to monitored production platforms.	**Exception noted:** For the OnTrak application, alerts were configured to send to an employee who was no longer with the company. **Management’s response:** See Section 5.
		Inspected management’s review of changes for the period of November 1, 2023 to May 22, 2024 and determined the changes pushed to the OnTrak application were authorized and followed the change management process.	No exceptions noted.
		MAP: For a selection of alerts, inspected results of management’s log review and corresponding change ticket(s) as applicable to determine whether changes to production systems and applications were logged, monitored, and resolved as appropriate. Inspected the File Integrity Monitoring tools configurations to determine whether the tool was utilized to monitor the integrity of the operating system and applications on production platforms. Further inspected the configuration within File Integrity Monitoring tools to determine whether the tool was configured to generate automated email alerts when changes were made to monitored production platforms.	No exceptions noted.

#	Global Payments’ Control Activities	KPMG LLP’s Tests of Controls	Results of Tests
4.07	**Change Management Tool Access** Access to change management tools is restricted by authentication requirements and user accounts are reviewed at least annually. (*GP, HPY, TSYS*)	Inspected password settings to determine whether the password and account lockout parameters were configured in accordance with the policy. For a selection of reviews, inspected the review of users with access to file integrity tools to determine whether access was reviewed for appropriateness and any inappropriate access identified was removed as requested.	No exceptions noted.

Control Objective 5 - Logical Access:

Controls provide reasonable assurance that logical access to production operating systems, applications, and databases is limited to authorized individuals.

#	Global Payments' Control Activities	KPMG LLP's Tests of Controls	Results of Tests
5.01	**Application Passwords** Password and account lockout parameters for application systems are configured, where technology permits, according to documented policies. (*GP, HPY, TSYS*)	**MAP, OnTrak, eConnections, HPS Enterprise (Fee Rule Manager), Frontier:** Inspected the Information Security Policy and the Information Security Standards to determine whether password standards were defined. Inspected system security settings to determine whether the password and account lockout parameters were configured in accordance with the Corporate Security Policy. **TMAS, FCS:** Inspected a selection of SONI system settings to determine whether passwords were configured in accordance with the Information Security Policy. Observed a user sign-on to production systems via SONI system software to determine whether passwords were masked at user sign-on.	No exceptions noted.
5.02	**Infrastructure Passwords** Password and account lockout parameters for production platforms (i.e., network, operating systems, and databases) are configured, where technology permits, according to documented policies. (*GP, HPY, TSYS*)	**MAP, OnTrak, eConnections, Passport, HPS Enterprise (Fee Rule Manager), i.Balance!, Frontier:** Inspected the Information Security Policy and the Information Security Standards to determine whether password standards were defined. For the in-scope network, operating systems, and databases, inspected system security settings to determine whether the password and account lockout parameters were configured in accordance with the Corporate Security Policy. **GMAS, TMAS, FCS:** Inspected a selection of CA-ACF2 Global System Options to determine whether passwords were configured in accordance with the Information Security Policy. Observed a user sign-on to production systems via CA-ACF2 system software and to determine whether passwords were masked at user sign-on.	No exceptions noted.

#	Global Payments' Control Activities	KPMG LLP's Tests of Controls	Results of Tests
5.03	**User Access Provisioning** New and modified user accounts, including administrator accounts, for in-scope systems are created as requested based on approval provided by required management. (*GP, HPY, TSYS*)	**MAP, OnTrak, eConnections, GMAS, Passport, HPS Enterprise (Fee Rule Manager), i.Balance!, Frontier:** Inspected completed access requests for a selection of new and modified users for in-scope systems to determine whether requested access was approved prior to access being granted and to determine whether access granted agreed to the access requested. **TMAS, FCS:** Inspected the on-line request forms for a selection of users added, including SONI access requests, to determine whether the procedures were followed as designed, and access was authorized in accordance with the Information Security Policy. For a selection of users provisioned, inspected the access profiles, job position, and employee department and inquired of management to determine whether the access profiles assigned to the users were based on their job function.	No exceptions noted.
5.04	**Access Removal** Application, operating system, and database access is restricted by termination of network access within 3 business days upon notification of employee termination. (*GP, HPY, TSYS*)	**GP, HPY, TSYS - Omaha Portfolio Only:** Inspected system configuration settings to determine whether employee network access was automatically disabled once HR updates employee records. For a selection of terminated employees, compared the users' network disable dates to their termination dates to determine whether user accounts were disabled in a timely manner. **TSYS - Broomfield Portfolio Only:** For a selection of terminated employees, compared the users' network disable dates to their termination dates to determine whether user accounts were disabled in a timely manner.	**Exception noted:** For 11 of 15 terminated users selected, access to the eConnections application was not removed within 3 business days of termination. **Management's response:** See Section 5.

#	Global Payments’ Control Activities	KPMG LLP’s Tests of Controls	Results of Tests
5.05	**Centralized Entitlement Reviews** On a quarterly basis, management utilizes an identity governance lifecycle management tool to perform a review of users and corresponding access permissions to in-scope production systems (i.e., applications, operating systems, and databases). Required modifications to users and corresponding access permissions are documented within the tool and access is modified as requested. Note: The user account reviews and corresponding access permissions to in-scope systems follow either the centralized or manual review process. (*GP, HPY, TSYS*)	For a selection of systems and/or quarters, inspected management’s documentation over the manual uploads and automated feeds into the identity governance lifecycle management tool to determine whether the users and entitlements were transferred completely and accurately from the systems to the identity governance lifecycle management tool. For a selection of systems and/or quarters, inspected evidence of the quarterly user entitlement reviews to determine whether management performed the review and whether required modifications arising from the review were communicated and processed.	**Exception noted:** For 1 of 2 selected quarterly user access reviews for GMAS, the user access review was not performed timely. For one of two quarters' user access reviews for one of 25 systems selected for testing within that quarter, three of the 35 access modifications selected for testing were not processed timely. In addition, see exception identified in control 7.01. **Management’s response:** See Section 5.
5.06	**Manual Entitlement Reviews** On a quarterly basis, management performs a review of users and corresponding access permissions to in-scope applications, operating systems, and databases. Required modifications to users and corresponding access permissions are documented and access is modified as requested. Note: The user account reviews and corresponding access permissions to in-scope systems follow either the centralized or manual review process. (*GP, HPY, TSYS*)	For a selection of systems and quarters, inspected management’s documentation to determine whether the users and their entitlements were generated completely and accurately. For a selection of systems and quarters, inspected evidence of the quarterly manual user entitlement reviews to determine whether management performed the review and whether required modifications arising from the review were communicated and processed.	No exceptions noted.

#	Global Payments' Control Activities	KPMG LLP's Tests of Controls	Results of Tests
5.07	**Annual Service Account Reviews** On an annual basis, service accounts are reviewed, confirmed for on-going need, and modified as requested. Note: The service account reviews follow either the centralized or manual review process. *(TSYS)*	Inspected evidence of the service accounts review to determine whether management performed the reviews and whether required modifications arising from the reviews were communicated and processed.	No exceptions noted.

Control Objective 6 - Physical Security:

Controls provide reasonable assurance that physical access to Global Payments high security areas (i.e., data centers) is limited to properly authorized individuals.

#	Global Payments' Control Activities	KPMG LLP's Tests of Controls	Results of Tests
6.01	**Policy and Procedures** The Physical Security Policy establishes the minimum security standards, policies and procedures relating to physical security for Global Payments facilities and activities. The standards cover the controls for physical access authorization to high security areas. The standard also describes the roles and responsibilities of key personnel responsible for implementation of the standards, policies and procedures. (*GP, HPY, TSYS*)	Inspected the Physical Security Policy to determine whether policies and procedures relating to physical access were documented and maintained and whether roles and responsibilities of key personnel responsible for implementation of the policies were defined.	No exceptions noted.

#	Global Payments' Control Activities	KPMG LLP's Tests of Controls	Results of Tests
6.02	**Access Control** Access to high security Global Payments facilities and data centers requires an authorized electronic cardkey and is monitored by surveillance cameras. Certain additional high security work areas such as Data Center computer operations and network equipment rooms are further restricted through the use of multifactor authentication to access. Physical Security personnel provide continuous 24x7 access monitoring and personnel security from multiple locations. (*GP, HPY, TSYS*)	Toured the Global Payments facilities to determine whether access to the data center and computer room was restricted using an electronic cardkey system and biometric devices for high security work areas. Toured the Global Payments facilities, data centers, and co-located data centers to determine whether physical access controls, including: the PSMS badge reading devices, surveillance cameras, on-site security personnel and use of single entry doors. During the tours, observed an attempt to gain access through a selection of card access devices to determine whether access was granted or denied appropriately.	No exceptions noted.
6.03	**Visitor Access** Visitor logs are used to maintain a record of visitor activity to data centers. (*GP, HPY, TSYS*)	Inspected visitor logs for a selection of days and data centers to determine whether visitor logs were used to maintain a record of visitor activity.	No exceptions noted.
6.04	**Physical Access Logging and Monitoring** Data centers are equipped with intrusion alarms, surveillance cameras and related monitoring screens. All facility access attempts are logged. (*GP, HPY, TSYS*)	Observed archived surveillance videos at the Global Payments data centers to determine whether monitoring was in place. Inspected physical access log files generated during the data center tours to determine whether the PSMS system recorded the granting or denial of access. Observed a user attempt to access a restricted area to determine whether access was denied and to determine whether an on-line alarm was triggered in the PSMS system which was monitored by Physical Security personnel.	No exceptions noted.

#	Global Payments' Control Activities	KPMG LLP's Tests of Controls	Results of Tests
6.05	**Physical Access Administration** Access to the physical access administration software is limited to authorized Physical Security personnel. The application is used to monitor access to secure locations and privileged application access is required to create or modify physical access privileges. (*GP, HPY, TSYS*)	Inspected a list of users with PSMS administrative functions to determine whether PSMS administrative functions were limited to Corporate Security personnel.	No exceptions noted.
6.06	**Physical Access Provisioning** Data center access requires a properly approved access request. Access is based on job responsibilities. (*GP, HPY, TSYS*)	Inspected the procedures for granting physical access to Global Payments employees to determine whether the procedures included requirements for granting access based upon job responsibilities. Inspected the physical access requests for a selection of employees provided access to Global Payments-owned data centers, Global Payments cages at third-party data centers during the period, PSMS records and job descriptions in the Human Resource system to determine whether access requested was consistent with job functions, whether access provided agreed with the request, and whether access forms were completed, authorized and signed according to procedures.	No exceptions noted.
6.07	**Physical Access Termination** On a daily basis, Human Resources sends Corporate Security a list of terminations and/or transfers for employees and contractors. Physical access is removed upon notification of termination. (*GP, HPY, TSYS*)	From a list of terminated Global Payments employees and contractors from the Human Resources system, inspected the physical access privileges for a selection of individuals to determine whether their physical access to high security areas had been removed on a timely basis.	No exceptions noted.

#	Global Payments' Control Activities	KPMG LLP's Tests of Controls	Results of Tests
6.08	**Physical Access Entitlement Review** A review of physical access rights to Global Payments data centers is performed at least quarterly. Access changes identified in the review are processed. (*GP, HPY, TSYS*)	For a selection of quarters, inspected Global Payments data center access report reviews to determine whether a review of access was performed and whether changes in access identified for a selection of individuals during the review were resolved.	No exceptions noted.

Control Objective 7 - Computer Operations:

Controls provide reasonable assurance that application and system processing is scheduled and monitored, and backups are available for restoration when necessary.

#	Global Payments' Control Activities	KPMG LLP's Tests of Controls	Results of Tests
7.01	**Access to Job Processing Tools** Access to job scheduling and file transfer tools is restricted to authorized individuals based on job function. (*GP, HPY, TSYS*)	**MAP, OnTrak, eConnections, Passport, HPS Enterprise (Fee Rule Manager), i.Balance!, Frontier:** Inspected a list of users who have access to job scheduling and file transfer tools, inspected job titles, and inquired of relevant management personnel to determine whether the users' access was appropriate based on job function. **GMAS, TMAS, FCS:** Inspected CA-ACF2 rules over the job scheduling software and Human Resource records to determine whether access to modify the schedule was based on job responsibilities.	**Exception noted:** Access was not disabled timely for two terminated user accounts out of the population of 295 privileged users. The two terminated user accounts were also not detected during the subsequent quarterly access review (see 5.05). **Management's response:** See Section 5.

#	Global Payments' Control Activities	KPMG LLP's Tests of Controls	Results of Tests
7.02	**GNOC Monitoring** The Global Network Operations Center (GNOC) monitors the production processing environment, including jobs and file transfers, on a continuous basis. Production issues, including incidents and file transfer failures, are documented through resolution. (*GP, HPY, TSYS*)	**MAP, OnTrak, eConnections, Passport, HPS Enterprise (Fee Rule Manager):** Inspected the IT Service Management Standard Operating Procedure to determine whether the document included procedures for identifying and responding to production processing incidents. Observed tools used by the GNOC for monitoring production processing systems to determine whether jobs and file transfers are monitored on a continuous basis. Inquired of management and inspected the tool dashboards used to monitor the production environments to determine whether the tools were actively monitored by the GNOC personnel or the tools were configured to generate alert notifications for incidents requiring investigation. Inspected tickets for a selection of production issues to determine whether the resolution of the issue was documented. **TMAS, GMAS, FCS:** Inspected the Incident and Problem Management Standards to determine whether procedures were in place for identifying and responding to production processing incidents. For a selection of alerts from a selection of the monitoring tools, inspected ticket documentation to determine whether the GNOC created a ticket, and for alerts without a ticket, inquired of the GNOC and inspected supporting documentation to determine whether a valid reason existed for not creating a ticket, in accordance with policies and procedures. For a selection of tickets created by the GNOC, inspected the ticket to determine whether the GNOC actioned and resolved alerts according to policy and procedures.	No exceptions noted.

#	Global Payments' Control Activities	KPMG LLP's Tests of Controls	Results of Tests
7.03	**Data Backups** Programs and data are backed up at least weekly. Backup failures are recorded and tracked through resolution. (*GP, HPY, TSYS*)	For a selection of servers and databases, inspected the job configurations to determine whether backup activities were scheduled on at least a weekly basis. Inspected the alerting configurations within the job scheduling tools to determine whether automated notification emails were sent to appropriate personnel when a scheduled backup job failed. For a selection of backup failures, if any, inspected evidence to determine whether the backup failures were documented, assigned, and resolved in accordance with procedures.	No exceptions noted.
7.04	**Data Redundancy** Production systems are configured to support data redundancy. (*GP, HPY, TSYS*)	Inspected redundancy configurations for a selected server or database for in-scope systems to determine whether production systems were configured to support data redundancy.	No exceptions noted.

Section 5

Other Information Provided by Management of Global Payments

Management Responses to Control Testing Exceptions

Control Objective 4 - Change Management:

Controls provide reasonable assurance that development of new systems and changes to existing systems are documented, tested, and approved.

#	Global Payments' Control Activities	Results of Tests	Management's Response
4.03	**Segregation of Duties** Global Payments employs segregation of duties so that accounts with development access are restricted from migrating source code to production. *(HPY)*	For the Passport application, four out of nine accounts with development access have the ability to migrate source code to production.	Beginning in August 2024, management implemented a detective monitoring control (4.05b) whereby on a monthly basis, a review is performed to confirm changes were not developed by accounts with access to migrate changes. During the first instance of this monthly control, management confirmed no changes were developed by accounts with access to migrate changes during the examination period.
4.06	**File Integrity Monitoring** File Integrity Monitoring tools are configured in accordance with policies and procedures to detect changes to production systems and applications. Changes are reviewed to determine if they were authorized and followed the change control process. (*TSYS*)	For the OnTrak application, alerts were configured to send to an employee who was no longer with the company.	As of May 22, 2024, Management updated the distribution group that receives email alerts for the Ontrak application to help ensure that appropriate individuals are notified of changes made to the OnTrak Application. For the period of November 1, 2023 to May 22, 2024, as part of Control 4.06, management confirmed that changes pushed to the OnTrak application were authorized and followed the change management process.

Control Objective 5 - Logical Access:

Controls provide reasonable assurance that logical access to production operating systems, applications, and databases is limited to authorized individuals.

#	Global Payments' Control Activities	Results of Tests	Management's Response
5.04	**Access Removal** Application, operating system, and database access is restricted by termination of network access within 3 business days upon notification of employee termination. (*TSYS*)	For 11 of 15 terminated users selected, access to the eConnections application was not removed within 3 business days of termination.	Company policy is to remove user access within 3 business days of employee termination. Oversight by the individuals responsible for disabling access to the eConnections application caused the untimely termination process. Responsibility has now been centralized within the IAM team, and management has reinforced the requirement to remove access within 3 business days with appropriate team members. Exceptions related to untimely termination processes were identified by management through the user access review process. In addition, management inspected the last login date for the 11 terminated users and confirmed that the users did not access the system as of their termination date.

#	Global Payments’ Control Activities	Results of Tests	Management’s Response
5.05	**Centralized Entitlement Reviews** On a quarterly basis, management utilizes an identity governance lifecycle management tool to perform a review of users and corresponding access permissions to in-scope production systems (i.e., applications, operating systems, and databases). Required modifications to users and corresponding access permissions are documented within the tool and access is modified as requested. (*GP, HPY, TSYS*)	For 1 of 2 selected user access reviews for GMAS, the user access review was not performed timely.	Due to enhancements underway with the user access review process, completion of the Q1 user access review was delayed, which also impacted the timely completion of the Q2 user access review. Beginning in Q3, user access reviews were performed timely.
		For one of two quarters' user access reviews for one of 25 systems selected for testing within that quarter, three of the 35 access modifications selected for testing were not processed timely.	For the exception related to one of two quarters’ user access review, the system and team responsible for administering access does not relate to the US Merchant Payment Processing system but is reported since this is a homogeneous control. The user modifications requested in the user access review were overlooked due to human error, which resulted in a delay in completion of the requested modifications. Access has subsequently been removed and management confirmed that the users' LAN accounts had been disabled timely as applicable. Management has and will continue to reinforce the requirement to perform detailed reviews to those responsible for performing these activities.
		In addition, see exception identified in control 7.01.	For the exceptions noted in 7.01, the terminated user accounts were not identified for removal during the subsequent quarterly user access review due to human error. As noted in the management response to 7.01, access has since been removed. Additionally, management confirmed that the LAN account was disabled timely for one of the two users, and, for the other account, the LAN account was disabled as of the beginning of the examination period. Management has and will continue to reinforce the requirement to perform detailed reviews to those responsible for performing these activities.

Control Objective 7 - Computer Operations:

Controls provide reasonable assurance that application and system processing is scheduled and monitored, and backups are available for restoration when necessary.

#	Global Payments' Control Activities	Results of Tests	Management's Response
7.01	**Access to Job Processing Tools** Access to job scheduling and file transfer tools is restricted to authorized individuals based on job function. (*TSYS*)	Access was not disabled timely for two terminated user accounts out of the population of 295 privileged users. The two terminated user accounts were also not detected during the subsequent quarterly access review (see 5.05).	Company policy is to remove user access within 3 business days of employee termination. The removal of access to the job processing tool is manually initiated by the user's manager to notify IAM to remove users' access. Notification to IAM to remove access was not completed timely, and the terminated user accounts were not identified for removal during the subsequent quarterly user access review due to human error. Access to log into the job processing tool requires the user to have first authenticated to the user's LAN network using multifactor authentication. Management confirmed for one of the two that the user's LAN account had been disabled timely, and for the other account, the LAN account was disabled as of the beginning of the examination period. Additionally, job processing tool access for both accounts has since been removed. Management has and will continue to reinforce the requirement to notify IAM in a timely manner of employee terminations and to perform detailed user access reviews to those responsible for performing these activities.

Business Continuity and Technical Resiliency

Global Payments has established a risk-based, end-to-end framework for managing business disruption related risks. The primary components of the framework include:

- Governance through the creation and maintenance of policies, standards, and reporting program activities to the Management Risk Committee;
- Risk Assessments that include business impact analysis, facility risk assessments and single point of failure analysis that proactively identify risks and apply mitigation strategies;
- Creation of Business Continuity (BC) and Technical Resiliency (TR) Plans for Facilities, Applications, Data Centers, Infrastructure, and Business Processes which detail the procedure to respond, resume and recover services;
- Perform contingency plan exercises and training programs to respond to incidents quickly and effectively;
- Conduct risk and control assessments for third party service providers and vendors;
- Program oversight and support provided by Enterprise Risk Management; and
- Evaluation of internal controls performed by Internal Audit.

Global Payments has documented technical recovery and business continuity plans, which include detailed recovery procedures for its business processes and IT infrastructure. BC / TR Plans encompass the following areas:

- Plans are created based on the type of assets such as facility, technology, or infrastructure. There are three different plan types: Facility Plan for the recovery of operations and processes, Data Center Plan which details the recovery of infrastructure and technology, and a Technical Resiliency Plan for the recovery of an application.
- The plans:
    - Detail the purpose, scope, and assumptions of the plans, as well as ownership;
    - Define the individual's role and responsibilities for managing an event and the composition of the teams such as Incident Commander and recovery team;
    - Correspond to BIAs and related RTO and RPO targets;
    - List equipment, facilities, and vital records that are necessary for the BC / TR plan within the requirement section;
    - Provide information about plan testing and links to associated test cycles (next test), the date of the last BC/TR plan test, and the test status;
    - Contain procedures for recovery strategies such as cyber response, failover, recovery phases, data backup, network communications etc., that can be deployed during an event; and
    - Document other plan requirements such as the dependencies, third parties, communication protocols, call trees, or the roles required to recover and perform the process.

Business continuity and technical resiliency plans are updated annually, and exercised in accordance with the Company's Business Continuity Standard.

Privacy Practices

Global Payments is obligated to adhere to certain legal and regulatory privacy standards and requirements to comply with additional industry standards. Beyond these rapidly-evolving requirements, Global Payments is committed to respecting the fundamental human right to privacy and handling personal data in a manner designed to respect that right.

Global Payments' team members are entrusted with the responsibility to properly handle personal and other sensitive information about Global Payments, clients and customers, and other individuals.

Global Payments' Internal Privacy Policy, together with associated standards and procedures, provides a comprehensive compliance framework to guide the handling of personal data within the organization. Global Payments' has enabled Privacy by Design tools throughout Global Payments to help teams consider privacy-related benefits and risks at all junctures in the product deployment process. These programs dovetails with the Company's information security program in a manner designed to ensure that personal data processed by Global Payments remains protected.

Legal obligations most frequently applicable to Global Payments' handling of personal data include:

- The Gramm-Leach-Bliley Act (GLBA)
- The California Privacy Rights Act (CRPA) (amending the California Consumer Privacy Act (CCPA)), and other applicable U.S. state data privacy laws
- The European Union General Data Protection Regulation (GDPR) and its United Kingdom (UK) counterpart
- Canada's Personal Information Protection and Electronic Documents Act (PIPEDA)
- The comprehensive privacy legislation in Brazil, Singapore, Australia, Mexico, and the Philippines

Some of Global Payments' software and vertical markets businesses may also (or alternatively) be subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Family Educational Rights Privacy Act (FERPA), and other laws applicable to health and education records. As the regulations evolve rapidly, Global Payments is paying close attention to upcoming AI regulations such as the EU Artificial Intelligence Act and the new U.S. state laws.

Global Payments maintains a centralized Privacy Office which maintains the corporate strategy for compliance with privacy and data protection laws. As part of that strategy, Global Payments prioritizes understanding how personal data is collected, used, and stored to build a dynamic data inventory that forms the backbone of the Company's privacy compliance. Global Payments aspires to act deliberately throughout the data lifecycle to understand the data the Company holds, the purposes for which the Company holds the data, and the relevant regulatory and contractual requirements that attach. Data lifecycle management helps the Company complete individual rights requests, identify and manage third-party risk, respond promptly and efficiently to potential data incidents, and exercise Privacy by Design. Global Payments strives to use Privacy by Design to incorporate privacy controls throughout product development, thereby ensuring that personal data collection and processing is adequate, relevant, and necessary.

Payment Card Industry Data Security Standard Compliance

The Global Payments businesses that handle and process card data maintain compliance with the Payment Card Industry (PCI) Data Security Standard (DSS), undergoing annual audits to re-certify compliance with the standard. Global Payments has created an industry leading program to assist qualifying merchants to meet their own PCI DSS obligations through partnerships with carefully selected payment security specialists, Application Scanning Vendors (ASVs) and Qualified Security Assessors (QSAs), as certified by the PCI Council.

About Global Payments

Global Payments Inc. (NYSE: GPN) is a leading payments technology company delivering innovative software and services to our customers globally. Our technologies, services and team member expertise allow us to provide a broad range of solutions that enable our customers to operate their businesses more efficiently across a variety of channels around the world.

Headquartered in Georgia with approximately 27,000 team members worldwide, Global Payments is a Fortune 500® company and a member of the S&P 500 with worldwide reach spanning North America, Europe, Asia Pacific and Latin America. For more information, visit company.globalpayments.com and follow Global Payments on X (@globalpayinc), LinkedIn and Facebook.

About TSYS

TSYS, a Global Payments (NYSE: GPN) company, is the payment stack for the future. Our suite of scalable issuer solutions provides the next generation platform for origination, processing, and risk management. Whatever your industry, scale or ambition, we'll help you configure the ideal solution for you. Operating in more than 75 countries around the world, we process billions of transactions each year. Beyond the transaction, we deliver powerful user experiences. We give your customers more of what they want–in more ways and places. Power your growth with the only payments partner you need. For more information, visit www.TSYS.com. We're also on X (@TSYS_TSS) and Facebook.

About Heartland

Heartland, a Global Payments (NYSE: GPN) company, is the point of sale, payments, and payroll solution of choice for entrepreneurs that need human-centered technology to make every day work better. Our products and services are designed to help businesses sell more, keep customers coming back and spend less time in the back office. Nearly 1,000,000 businesses trust us to guide them through market changes and technology challenges, so they can stay competitive and focus on building remarkable businesses instead of managing the daily grind. Learn more at heartland.us