TouchNet Higher Education Processing Services

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

For the period of May 1, 2024 through April 30, 2025

touchnet
A Global Payments Company

TouchNet Higher Education Processing Services

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

TABLE OF CONTENTS

Section 1

Independent Service Auditors' Report

touchnet
A Global Payments Company

globalpayments

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

Independent Service Auditors' Report

Board of Directors of Global Payments:

Scope

We have examined management of Global Payments Inc.'s accompanying description of its TouchNet Higher Education Processing Services (the System) for processing user entities' transactions throughout the period May 1, 2024 to April 30, 2025 titled "Management of Global Payments' Description of its TouchNet Higher Education Processing Services" (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 Global Payments' Business Continuity and Technical Resiliency, Privacy Practices, and Payment Card Industry Data Security Standard Compliance 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 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 May 1, 2024 to April 30, 2025. 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 May 1, 2024 to April 30, 2025.
- 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 May 1, 2024 to April 30, 2025, and subservice organizations and user entities applied the complementary controls assumed in the design of Global Payments' controls throughout the period May 1, 2024 to April 30, 2025.
- the controls operated effectively to provide reasonable assurance that the control objectives stated in the Description were achieved throughout the period May 1, 2024 to April 30, 2025 if complementary subservice organization controls and complementary user entity controls, assumed in the design of Global Payments' controls, operated effectively throughout the period May 1, 2024 to April 30, 2025.

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 May 1, 2024 to April 30, 2025, 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, GA
June 26, 2025

Section 2

Management of Global Payments' Assertion

touchnet
A Global Payments Company

globalpayments

Management of Global Payments' Assertion

We have prepared the accompanying description of Global Payments Inc.'s TouchNet Higher Education Processing Services (the System) for processing user entities' transactions throughout the period May 1, 2024 to April 30, 2025 titled "Management of Global Payments' Description of its TouchNet Higher Education Processing Services" (the Description) for user entities of the System during some or all of the period May 1, 2024 to April 30, 2025, 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 May 1, 2024 to April 30, 2025 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 May 1, 2024 to April 30, 2025 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 May 1, 2024 to April 30, 2025. 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.

June 26, 2025

Section 3

Management of Global Payments' Description of its TouchNet Higher Education Processing Services

touchnet
A Global Payments Company

globalpayments

Scope of Report

As part of its overall internal controls reporting program, Global Payments Inc. (also referred to as "Global Payments" or the "Company") management defines and determines the scope and timing of each report. This report addresses the TouchNet Higher Education Processing System & Services.

The scope of this report is limited to the TouchNet Higher Education Processing System & Services, which include the U.Commerce, OneCard, and Platform Reporting system (collectively referred to as the TouchNet Higher Education Processing System or "system"). and the general computer controls that support these services The TouchNet Higher Education Processing System & Services include transaction processing, customer reporting, and settlement activities. As operations and management of the TouchNet Higher Education Processing System & Services and related applications may be performed by the dedicated TouchNet team or Global Payments corporate teams, shared technology and functional operations are referred to herein as "Global Payments."

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 May 1, 2024 to April 30, 2025. 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 TouchNet

TouchNet, a Global Payments Company, provides commerce management solutions for Higher Education Institutions. For three decades, TouchNet has partnered with colleges and universities to help them implement electronic payment and commerce solutions that have streamlined key business processes and integrated commerce transactions into the fabric of the campus enterprise. Approximately 1,000 colleges and universities make use of the TouchNet Higher Education Processing System & Services.

TouchNet Services include but are not limited to:

- Point of Sale solutions (POS),
- eCommerce payment processing solutions,
- PayPath Service Fee solution,
- payment plan management solutions, and
- reporting and reconciliation solutions.

TouchNet is based in the Kansas suburbs of the Kansas City metro area and its staff design, develop, implement, and support TouchNet solutions for Higher Education.

Overview of Global Payments

Global Payments Inc. is a leading payments technology company delivering innovative software and services to customers globally with worldwide reach spanning North America, Europe, Asia-Pacific, and Latin America. The payments technology industry provides financial institutions, businesses and consumers with payment processing services, merchant acceptance solutions and related information, and other value-added services. 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. Global Payments' common stock is traded on the New York Stock Exchange under the symbol "GPN."

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

- **Merchant Solutions:** Through the Merchant Solutions segment, which includes TouchNet, Global Payments provides payment technology and software solutions to customers globally. Global Payments provides payments technology and software solutions globally to primarily small and medium sized businesses and select mid-market and enterprise customers. Global Payments technology solutions are similar around the world in that we enable our customers to accept card, check, and digital-based payments. Global Payments' comprehensive offerings include, but are not limited to, authorization, settlement and funding services, customer support, chargeback resolution, reconciliation and dispute management services, terminal deployment, payment security services, consolidated billing and reporting. In addition, Global Payments offers a wide array of business management 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 ("POS") software, data analytics and customer engagement, human capital management and payroll, accounts receivable automation, inventory management and reporting that assist customers with driving demand and operating their businesses more efficiently. Global Payments' value proposition is to provide distinctive high-quality, responsive and secure services to all of Global Payments' customers. Global Payments focuses on providing differentiated customer service from the sales process, to onboarding, to ongoing support across our business.

- **Issuer Solutions:** Through the Issuer Solutions segment, Global Payments is a leading provider of comprehensive commerce solutions supporting the payment ecosystem for issuers. Global Payments offerings include core processing, enterprise tokenization, cardholder payments, authorization, card production, document production and archival, contact center services, managed services, fraud strategy, implementation services, consulting solutions and professional services. Global Payments also provides specialized solutions such as virtual cards, accounts payable and expense management, commercial processing and real-time alerts. Global Payments' operations serve diverse customer segments, including global, regional, community banks, credit unions, retailers, financial technology companies and neobanks. Global Payments go-to-market approach leverages direct engagement and partnerships with aggregators to deliver innovative service offerings across core processing, commerce enablement, managed services and professional services. Global Payments' strategic focus on fraud detection, rewards management and commerce enablement positions all Global Payments to expand opportunities across these key customer segments and drive continued growth. Global Payments is undertaking a comprehensive modernization of the Issuer Solutions segment, encompassing both technology and operations. These efforts enable Global Payments to deploy cloud-native products and services across diverse market segments, use cases and geographic regions with increased agility and speed to market, all within a secure and compliant framework. The modernization of the core processing platform allows Global Payments to deliver enhanced, unified capabilities, greater operational efficiencies and innovative features for Global Payments customers, while also offering Global Payments full suite of capabilities in a modular format or as a comprehensive, integrated solution. Global Payments has completed the development of customer-facing applications in the cloud and remains on track for commercial launches throughout 2025.

Certain corporate functions, including Legal, Enterprise Risk Management, Cyber 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, business operations, technology delivery and operations, customer relationship management, and all supporting corporate functions. The TouchNet leadership team is highly experienced in the payments and financial services industry, and meets regularly to verify alignment with overall business strategy.

The TouchNet executive and senior management team play a significant role in monitoring that the control environment within TouchNet 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 TouchNet. The following functions support the business operations and delivery of customer services of TouchNet:

- **Technology Solutions:** Technology Solutions (TS) is responsible for the definition and execution of technology strategies for the entire company worldwide. TS creates and deploys platforms and systems to drive success and deliver high-quality software, products, and solutions.
- **Cyber Security:** The Cyber Security function (formerly known as Information Security) is responsible for creating, implementing, and maintaining a comprehensive information security program to protect the Company's information systems and data assets. The Cyber 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 Cyber Security function.
- **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.
- **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 is part of Corporate Security and they ensure 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.
- **Human Resources:** The Human Resources (HR) department maintains personnel policies and standards. Human Resources has established policies and standards 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.
- **Enterprise Risk Management:** The Enterprise Risk Management (ERM) function uses a systematic approach to evaluating and improving the effectiveness of risk management 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.
- **Audit Services:** The Audit Services Group (ASG) performs financial, information technology, data security, compliance, and operational audits. 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.

TouchNet Business Operations

The following functions support the business operations of TouchNet:

- **Client Services:** The Client Services group is responsible for providing customer service to customers as well as tracking and resolving issues that have been identified by customers or through internal communications.
- **Information Technology Support (ITS):** All information technology functions are performed in-house. ITS is responsible for management of data center activities, where applicable, incident management, database administration, server management, and network management. ITS plays an integral role in performing software upgrades during the monthly maintenance periods.
- **Security and Compliance:** The Security and Compliance group is responsible for overseeing adherence to policies and procedures. This group is also responsible for monitoring the SIEM tools, identifying, and responding to potential security incidents.
- **Technical Operations:** The Technical Operations group is responsible for working alongside the Information Technology Support team to perform software upgrades to in-scope systems on a regular basis.
- **IT Infrastructure:** The IT Infrastructure group is responsible for ensuring data replication activities are performed on an on-going basis, performing restoration tests, and monitoring the production environment to identify and resolve data replication failures.

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 internal controls and for presentation in this report.

Global Payments' and TouchNet's 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 TouchNet.

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 published on the Company's intranet where all team members can access them and are updated periodically. 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 Cybersecurity Framework (CSF) and incorporate other relevant regulatory requirements and the Technology Committee provides final approval. The Chief Information Security Officer (CISO) and General Counsel are responsible for reviewing the policy and standards and provides final approval.

Human Resources Policies and Practices

Global Payments adheres to the written policies and standards that govern hiring and employment. Background checks and drug testing are 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 trainings 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. Upon Engagement, 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)), 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 Cyber 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. Terminated employee reports are provided to 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 our 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 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, ERM team is responsible for corporate risk monitoring and reporting, cyber and IT risk, business continuity and disaster recovery governance, vendor risk management, customer assurance engagement, regional risk and compliance, and federal examiner relations.

The Client Assurance and Customer Assurance functions within ERM support customer reviews and distribution of Global Payments' System and Organization Controls (SOC) report 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 its 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 business enablement function, 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, IT, Cyber 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 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 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 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 the company's internal audit 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. Cyber Security leadership meets with the Technology Committee each quarter to present and discuss information security risks that are relevant to the organization. Cyber 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.

- The Legal, ERM, and Cyber 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, assesses, and manages both existing and emerging risks to the achievement of Company strategic and operating objectives, as documented in the ERM policy, standard, handbook and risk register. Based on the policy, standard, handbook and register, ERM works with Executive Risk Owners and Risk Managers to determine risks, which are presented to the Board of Directors or an assigned subcommittee. On an annual rotation, ERM performs a risk analysis / deep dive evaluation on selected tier risks. ERM works with Executive Risk Owners and Risk Managers to establish risk appetites and risk tolerances for the risks. The appetite statements are presented to the Board of Directors or an assigned sub-committee.
- The ERM 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.
- 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.

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 a 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 to the Audit and Technology Committees of the Board of Directors and administratively to the Chief Financial Officer. ASG consists of professionals with many years of audit experience auditing information technology, financial, operational, and compliance risks and controls for the financial technology 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. 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 TouchNet 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 TouchNet 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 an 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.

TouchNet provides system bulletins and service descriptions on the Customer Portal, which is accessible to both internal and external users of the system, to communicate the design and operations of its systems.

Overview of TouchNet Higher Education Processing Environment

Description of Products and Services

Transaction Processing

TouchNet transactions, including online tuition payments, in-person tuition payments, donations, and merchandise purchases from students, parents, or other third parties, to TouchNet systems are made via automated application interfaces. These transactions are sent directly by POS or online portals to TouchNet for processing and recording. Transactions received are updated to individual student accounts or general ledger accounts in real-time and are recorded to the school’s Enterprise Resource Planning (ERP) software in real time.

Reporting

To support financial reporting, Global Payments provides standard key summary and detail reports to customers. Reports are accessed by customers through the U.Commerce web-based portal or the Platform Reporting web-based portal. Based on a customer's needs, customers can select the date range and relevant reports to support their financial reporting.

Information Systems Overview

Application Overview Table

The table below provides an overview of the in-scope applications.

Application	Relevant Processing	Primary Data Center Provider
U.Commerce	Product that offers solutions for deploying a unified suite of payment applications that streamline business office operations and provide campus-wide eCommerce transactions.	QTS Atlanta Metro (QTS) Google Cloud Platform (GCP)
OneCard	Product that offers solutions to parents and students to load student accounts with funds and allow students to redeem funds at campus locations.	QTS Atlanta Metro (QTS)
Platform Reporting	Product that offers TouchNet customers access to generate reports relevant to financial reporting.	Google Cloud Platform (GCP)

U.Commerce

The U.Commerce system has been tailored specifically for higher education institutions with the flexibility to unify campus commerce in a decentralized campus environment. The U.Commerce system is comprised of the TouchNet Payment Gateway, which combines electronic payment engines with integration technology, a centralized view of payment operations, and scalable transaction managers to provide higher education institutions with the foundations for campus wide commerce management. The TouchNet Payment gateway is the hub for processing payments from each of the modules in the U.Commerce applications and performs communication to the card processors. Each of the modules with the U.Commerce application allow higher education institutions to accept payments from various parties for various reasons. Below is a table detailing the modules within U.Commerce.

U.Commerce Module	Description
Bill + Payment	Payment module that gives students and parents the ability to view and pay tuition bills via all integrated payment methods made available by the gateway.
Payment Client	Payment Client is a web-based solution for accepting payments from the institutions' online payment points such as admissions, transcript requests, and application fees. Payments made with Payment Client are managed in the TouchNet Payment Gateway and monitored in the Payment Gateway reports.
SponsorPoint	Payment module that gives organizations the ability to pay tuition for students for which the organization is sponsoring to return to school.
Cashiering	Payment module that allows higher education personnel the ability to view student information and accept payments in person via all integrated payment methods made available by the gateway.
Student Account Advisor	Payment module that allows higher education personnel the ability to view student information and accept payments in person via all integrated payment methods made available by the gateway.
MarketPlace	Payment module that gives individuals the ability to make donations and purchase school merchandise through an online portal via all integrated payment methods made available by the gateway.
Checkout	Payment module that is designed to integrate with a campus web application. It can be a single-product webflow, can be a store with multiple products as well as used for an alumni group that accepts donations. With the Checkout API integration, the originating web application can either pass and display the grand total of the payer's purchase or a detailed breakdown of the purchase (including applicable taxes, shipping charges and other fees).

In addition to the modules detailed above, institutions have the ability to utilize the optional PayPath Service Fee solution when accepting payments via credit or debit card. The PayPath Service Fee solution is integrated into the U.Commerce application which gives higher education institutions the ability to shift the cost of accepting credit and debit card payments to the payer by adding a service fee.

U.Commerce is hosted at QTS Atlanta Metro, a third-party colocation provider, and support of the software is provided by TouchNet's Customer Services personnel. Additionally, relevant reporting data is replicated the U.Commerce databases to Platform Reporting in real time to be made available to TouchNet customers.

OneCard

The OneCard application offers students and parents the ability to preload student accounts with funds that can be redeemed at campus locations, such as cafeterias and school stores. Students and parents have the ability to load accounts via credit, debit, or ACH payment methods through an online portal. TouchNet does not manage the acceptance and processing of payments via the OneCard application, and instead, outsources this function to various third party vendors. TouchNet offers institutions the ability to choose their preferred third party vendor from the TouchNet Ready Partner Directory, and institutions are responsible for setting up and maintaining relationships with their selected third party vendor to accept and process payments made by students and parents. The third party vendors are responsible for sending relevant information to the OneCard system to track the transaction, and funds are sent directly from the third party to the institution. Institutions are responsible for verifying funds are credited and debited from the correct student account. As such transaction processing activities for the OneCard system are out of scope for this report, and this report excludes the control objectives and related controls of the third party vendors.

OneCard is hosted at QTS Atlanta Metro, a third-party colocation provider, and support of the software is provided by TouchNet's Customer Services personnel.

Platform Reporting

The Platform reporting application offers TouchNet customers the ability to generate a number of reports relevant to financial reporting through an online portal. The Platform Reporting application is hosted in GCP, and data is replicated multiple times a day from the U.Commerce databases to Platform Reporting to be made available to TouchNet customers.

Relevant Changes to Information Systems

There were no significant changes to the TouchNet Higher Education Processing System during the period.

Business Process Control Activities

Transaction Processing

The U.Commerce system accepts transactions from students, parents, or other third parties for various reasons, such as tuition payments, donations, or school merchandise, through an online portal or in person with a school representative. U.Commerce is configured to perform a series of edit checks on incoming transactions to validate if the payer has entered valid and complete data. Transactions can be submitted through online portals via credit, debit, or ACH; transactions can also be submitted in person with a school representative via credit, debit, cash, or check. Transactions submitted using credit, debit, or ACH payment methods are subject to edit checks to help verify only valid information is being submitted for processing. For transactions that are submitted via online portals, users manually enter payment information, and U.Commerce is configured to perform validation checks over the card number, expiration date, Card Verification Value (CVV), and address before the payer can submit the transaction for processing. Card transactions that are made in person are submitted via a Point of Sale (POS) device that is configured to only accept valid cards for payment. Additionally, for ACH transactions that are submitted through the online portals, U.Commerce performs a validation check over the routing number entered before the payment can be submitted. If any of the card or ACH validation checks fail, a message is displayed on the screen for the payer to review the information and resubmit the data. Payers also have the ability to submit cash and check transactions for purchases or payments in person with a school representative.

Once the U.Commerce application validates that complete and accurate information is entered, the system sends transaction requests to the data processor for processing with the card brands or to the account holders' financial institutions. Activities performed by the data processor, card brands, and the account holders' financial institutions are outside the scope of this report. Responses are received by U.Commerce and if the transaction is approved, regardless of payment method, U.Commerce records the transaction and sends the transaction data to the institution's Enterprise Resource Planning (ERP) software for recording. If the transaction is denied, a message is displayed back to the payer to resubmit the information; unsuccessful transactions (i.e., denied transactions) are not recorded in U.Commerce and data is not sent to the institution.

Credit and debit card transactions are aggregated in the U.Commerce Payment Gateway, and aggregated amounts are processed on a predefined schedule by TouchNet. TouchNet sends data to the data processor for the collection of funds and final processing. If a batch fails to transmit, appropriate personnel are notified via email and a ticket is automatically created in the Global Payment ticketing system to track the issue. The Customer Services group investigates and resolves batch failures to help verify settlement activities are being performed completely and accurately. Customers are responsible for monitoring ACH settlement files as TouchNet does not process settlement batches for ACH transactions; therefore, these activities are outside the scope of this report.

Data transmissions are actively monitored by the Customer Services Group and the IT Support (ITS) Group through alerts and live dashboards to identify and resolve any production processing issues in a timely manner. See the Computer Operations control objective below.

Customer Reporting

Customers can access reports relevant to financial reporting through the U.Commerce customer portal or through the Platform Reporting tool:

- **U.Commerce:** Reports accessed through the U.Commerce online portal are generated completely and accurately from the database hosted at the QTS data center.
- **Platform Reporting:** U.Commerce data is replicated between the U.Commerce databases to Platform Reporting on a real-time basis. Once the data has been replicated, the data is then transformed for reporting purposes. Data becomes available to customers every six hours after the transformation is performed. Both the replication and transformation of data are monitored by the IT Support (ITS) group to identify failures and help achieve complete and accurate data replication. Emails and tickets are automatically generated to alert ITS to research, track, and resolve appropriately within 1 business day.

Regardless of the application used to generate the reports, once logged in, customers can choose the reports they wish to use based on their needs. Reports made available are standard reports; customers cannot customize the reports. Customers can select the timeframe for generating the report, such as by day, month, or date range. Once the report type and date parameters are specified, reports are generated completely and accurately by aggregating data from relevant databases to create the requested report. Access to the U.Commerce customer portal and the Platform Reporting tool is granted by TouchNet personnel at the time of setup. Customers log in to the portals using a unique username and password. Customers are responsible for managing their own user accounts and restricting access to g only authorized individuals, and notifying TouchNet when access needs to be removed; therefore, user administration of customer accounts is outside the scope of this report.

The table below lists and describes the key customer reports tested in this report:

Application	Report Name	Description
U.Commerce	Payment Statistics	Report of payments made for the selected date range.
	Scheduled Payments	Report of scheduled payments that have been processed, are scheduled to be processed in the future, or failed to process on the scheduled date.
	eDeposits Report	Report of Deposit payments made for the selected date range.
	Plan Enrollment Report	Report of all active users enrolled in a payment plan.
	eRefunds Report	Report of refunds processed for the selected date range.
	Activity Report by Transaction	Report of all refunds processed for the selected merchant(s) and date range.
	Refund Report	Report of all activity for the selected merchant(s) and date range. This will include debits, credits, and voids.
	Batch Summary	Report of all transactions for the selected merchant(s) and date range for any given batch submitted for processing.

Application	Report Name	Description
Platform Reporting	Advanced Transaction Details	Dashboard that focuses on tabular delivery of data to get a detailed view of every transaction on campus. This provides a centralized view of both payment data, including sales totals and item modifiers associated with purchases to give a full view of all items sold on campus for use in resolving balance issues.
	Accounting Code Report	Dashboard of a summary view as well as a breakdown of the individual transactions that make up the aggregate total. This provides a single interface to help reconcile the general ledger transactions and information that is being synced with the campus general ledger solution.

Changes to reports made available to customers are documented in the Global Payments ticketing system and are subject to testing and approval in accordance with the Change Management process as described below.

Data transmissions relevant to customer reporting are actively monitored by the ITS group through alerts and live dashboards to identify and resolve any production processing issues in a timely manner. See the Computer Operations control objective below.

General Information Technology Control Activities

Change Management

Global Payments maintains formal Change Management policies and standards that govern the intake, development, testing, approval, and deployment of application and infrastructure changes utilizing Agile delivery, modified Waterfall, and ITIL approaches. The policies and procedures are reviewed, updated, and approved on an annual basis. These policies govern all IT-related changes, including new or existing (modified) applications and emergency changes/fixes.

Application Change Management

All application 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. Emergency changes, defined as changes to production that fall outside of scheduled change windows, must be approved by the Change Review Board and must also undergo testing prior to release (accelerated).

After development and testing 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 implementation. Approval requirements for emergency changes are documented in the Global Payments policies. After all required approvals are obtained, the Release Management team pushes the change to the production environment.

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. Access to promote changes to production are restricted to appropriate individuals based on job function. As of February 10, 2025, management migrated to a DevOps model that systematically enforces secondary approval of changes that restricts developers from making a code change without secondary approval.

Infrastructure Changes and Patch Management

The TouchNet patch management team meets on a regular basis to review significant infrastructure changes to the TouchNet systems, which are patched on a monthly basis. Patches are initially applied to the non-production instances to determine stability before being deployed into the production environment. Infrastructure changes are reviewed and approved prior to being deployed to production. The patch management team is responsible for deploying patches and monitoring that the applications are not adversely impacted by the patch. If functionality problems are encountered, management will conduct backout procedures and restore the last operational version of the operating system or database until the issue can be resolved.

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.

The in-house Information Technology Support (ITS) group manages the administration of user access, including remote access, user additions, deletions, changes, and profile builds for the LAN and in-scope systems. All access to Global Payments systems is initiated with an access request, which must be approved by an authorized manager, and is processed by the ITS group. Access to privileged functionality within applications, operating systems, and databases is based on the principle of least privileged access.

Users' managers or HR notify the ITS group via email or Global Payments ticketing systems 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 termination, managers are responsible for obtaining company hardware (e.g., laptop, badge, mobile phone). Managers are responsible for initiating a termination workflow in Workday for processing by Human Resource Business Partners (HRBP) within 5 business days of the termination (or otherwise as required by local laws). Upon receipt of the termination notification from HR, access is manually disabled by ITS personnel within 3 business days.

Entitlement reviews are performed on a semi-annual basis to assess the appropriateness of user access to in-scope applications, operating systems, and databases. Support groups are responsible for generating the listing of users used for the semi-annual reviews and confirming the completeness and accuracy of the extraction from in-scope applications and supporting infrastructure by verifying 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 file for review. Additionally, the ITS group is responsible for facilitating the completion of the review with appropriate parties and are responsible for following up on any reviews not completed in a timely manner. Appropriate parties 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 and are validated as performed as part of the user access review process.

Password configurations follow corporate standards on password rules. Logical access must conform to established account and password configuration standards and comply with corporate security requirements. If technology does not permit the systems to follow the corporate standard, the system owner is responsible for documenting approval for any exceptions to the policy as well as identifying alternative controls to mitigate the risk.

Computer Operations

The ITS group actively 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. ITS 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.

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 TouchNet Higher Education Processing System & Services cover only a portion of overall internal controls for each user entity of Global Payments. The subservice organizations related to the TouchNet Higher Education Processing System & Services 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 related to the TouchNet Higher Education Processing System & Services 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)
Google Cloud Platform (GCP)	Provides Infrastructure as a Service for the Platform Reporting system.	GCP should have relevant controls in place to limit logical access to properly authorized individuals.	Control Objective 4 – Logical Access
		GCP should have relevant controls in place for change management procedures that support the infrastructure of their cloud services.	Control Objective 3 – Change Management

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 (see the scope of report for any scope exclusions for which the below would also not address). 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 for notifying Global Payments in a timely manner of errors received when submitting data for processing.	CO 1: Transaction Processing
2	User entities should have controls in place to notify Global Payments of any failures in receiving complete and accurate transactions sent from TouchNet systems to the Institution's ERP.	CO 1: Transaction Processing
3	User entities should have controls in place for notifying TouchNet personnel of incomplete or inaccurate funds sent to the institution's bank accounts.	CO 1: Transaction Processing
4	User entities should have controls in place to monitor that ACH settlement batch files are submitted completely and accurately to the data processor.	CO 1: Transaction Processing
5	User entities should have controls in place to help ensure that refunds are initiated and approved by appropriate personnel and that these responsibilities are appropriately segregated.	CO 1: Transaction Processing
6	User entities should have controls in place to help ensure that transactions are completely and accurately transferred to the appropriate accounting ledgers and financial statements.	CO 1: Transaction Processing
7	User entities should have controls in place to help ensure payment transactions are authorized by the consumer when the Institutions assist the consumer with submitting a payment.	CO 1: Transaction Processing
8	User entities should have controls in place to help ensure Global Payments is notified of any misuse of Global Payments services and any fraudulent use of transactional details, including but not limited to, stolen credit card numbers, and stolen ABA routing numbers/account numbers.	CO 1: Transaction Processing
9	User entities should have controls in place to help ensure that any unsuccessful transaction messages are reviewed and resolved timely.	CO 1: Transaction Processing

#	Complementary User Entity Control	Relevant Control Objective(s)
10	User entities should have controls in place for reviewing reports made available by Global Payments for completeness and accuracy based on the parameters input by the user entities and notifying Global Payments in a timely manner to resolve any discrepancies.	CO 2: Customer Reporting
11	User entities should have controls in place to notify Global Payments of any reporting errors in a timely manner.	CO 2: Customer Reporting
12	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 3: Change Management
13	User entities should have controls in place to help ensure tests are performed for changes installed in their environment and for notifying Global Payments of any issues.	CO 3: Change Management
14	User entities should have controls in place to help ensure that customer user accounts with access to Global Payments systems and applications are appropriately managed, including the 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 4: Logical Access
15	User entities should have controls in place to help ensure that the password lock-out, password expiration, and password history configurations in the applicable TouchNet systems are set to a period of time that adheres to their password policy requirements.	CO 4: Logical Access

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 Control Activities and KPMG's Tests of Controls and Results of Tests

touchnet
A Global Payments Company

globalpayments

KPMG's 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.

Business Process Control Activities

Control Objective 1 – Transaction Processing

Controls provide reasonable assurance that transaction activities are recorded completely, accurately, and in a timely manner and settlement files are monitored.

#	TouchNet's Control Activities	KPMG's Tests of Controls	Results of Tests
1.01	**Card Transaction Requests** U.Commerce applications are configured to accept only valid card information, and invalid data is not accepted. Appropriate messages are sent back to the submitter indicating if the transaction was successful or unsuccessful.	Inspected the results of management inputting test data with known errors in the U.Commerce non-production environment via direct user interface to determine whether data submitted was evaluated by the application logic for accuracy (i.e., invalid card number, invalid expiration date, and invalid CVV) and appropriate error messages were generated. Inspected the results of management submitting test merchant data with no known errors via direct user interface to determine whether the transaction was processed successfully. Inspected the version numbers of the U.Commerce non-production and production environments and inquired of appropriate management personnel to determine whether the test results in the U.Commerce non-production environment would be replicated in the production environment.	No exceptions noted.

#	TouchNet's Control Activities	KPMG's Tests of Controls	Results of Tests
1.02	**ACH Transaction Requests** U.Commerce applications are configured to accept only valid ACH information, and invalid data is not accepted. Appropriate messages are sent back to the submitter indicating if the transaction was successful or unsuccessful.	Inspected the results of management inputting test data with known errors in the U.Commerce non-production environment via direct user interface to determine whether data submitted was evaluated by the application logic for accuracy (i.e., invalid routing number) and appropriate error messages were generated. Inspected the results of management submitting test merchant data with no known errors via direct user interface to determine whether the transaction was processed successfully. Inspected the version members of the U.Commerce non-production and production environments and inquired of appropriate management personnel to determine whether the test results in the U.Commerce non-production environment would be replicated in the production environment.	No exceptions noted.
1.03	**Transaction Recording** Successful transactions are recorded in the U.Commerce system and sent to the institution's Enterprise Resource Planning (ERP) software completely, accurately, and timely.	Inspected successful Card, ACH, Cash, and Check transactions submitted to U.Commerce applications to determine whether the transaction was recorded in the U.Commerce system. Inspected successful Card, ACH, Cash, and Check transactions submitted to the U.Commerce system to determine whether the transaction was subsequently sent to and recorded in a test customer's ERP software completely, accurately, and timely.	No exceptions noted.

#	TouchNet's Control Activities	KPMG's Tests of Controls	Results of Tests
1.04	**Settlement Files Monitoring** Settlement files are monitored on a continuous basis. Failed transactions are tracked and resolved as appropriate.	Inspected the Incident Response Policy to determine whether procedures were in place for identifying and responding to settlement file processing incidents. Inspected configurations within the system to determine whether the system was configured to monitor the processing of settlement files and generate alert notifications for errors requiring investigation. Inspected tickets for a selection of settlement file processing alerts to determine whether alerts were tracked, researched, and resolved within 1 business day.	No exceptions noted.

Control Objective 2 – Customer Reporting:

Controls provide reasonable assurance customer reporting data is complete and accurate.

#	TouchNet's Control Activities	KPMG's Tests of Controls	Results of Tests
2.01	**Completeness and Accuracy of Reports** Key customer reports are generated completely and accurately.	Observed the report generation for each of the key customer reports and compared the generated report to the production database to determine whether the data displayed within the production database completely and accurately matched the data displayed within the key customer reports.	No exceptions noted.
2.02	**Platform Reporting Data Replication** Relevant reporting data from the TouchNet system is replicated multiple times a day from the U.Commerce databases to Platform Reporting completely and accurately. Once the data has been replicated, the data is transformed completely and accurately for reporting purposes. Access to tools used to replicate data from the U.Commerce databases to Platform Reporting is restricted to authorized individuals.	Inspected replication configurations to determine whether the U.Commerce databases was configured to replicate data to Platform Reporting multiple times a day. Inspected data in the Platform Reporting tool and compared data in U.Commerce to determine whether the data was transformed completely and accurately for reporting purposes. Inspected system-generated listings of accounts with access to the tools used to replicate data from the U.Commerce databases to Platform Reporting to determine whether access was restricted to authorized personnel.	No exceptions noted.

#	TouchNet's Control Activities	KPMG's Tests of Controls	Results of Tests
2.03	**Data Replication Monitoring** Data transmissions between the U.Commerce databases and Platform Reporting and the transformation of data are monitored on a continuous basis to identify failures. Emails and tickets are automatically generated to alert IT Support personnel. Issues are tracked through to resolution within 1 business day.	Inspected configurations within the tools to determine whether the tools were configured to generate alert notifications for errors requiring investigation. Inspected tickets for a selection of data transmission alerts to determine whether alerts were investigated and resolved within 1 business day.	No exceptions noted.

General Information Technology Control Activities

Control Objective 3 - Change Management:

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

#	TouchNet’s Control Activities	KPMG's Tests of Controls	Results of Tests
3.01	**Change Testing and Approval** Application changes are documented within the change ticketing system and are tested and approved by business and/or IT management prior to being deployed to the production environment.	Inspected the Change Management Standard to determine whether the policy outlines the process for documenting the testing and approval of changes prior to implementation into the production environment. Inspected supporting documentation, including change tickets, for a selection of changes to determine whether changes were tested and approved before the changes were implemented into the production environment.	No exceptions noted.
3.02	**Segregation of Duties** Access to promote changes into the production environment for in-scope applications is restricted to appropriate individuals based on job function and segregated from accounts with access to develop.	Inspected a system generated listing of accounts with access to promote changes into the production environment and the corresponding job titles to determine whether accounts with access were appropriate based on job function and segregated from accounts with access to develop.	No exceptions noted.

#	TouchNet's Control Activities	KPMG's Tests of Controls	Results of Tests
3.03	**Peer Review Configuration** (as of February 10, 2025) Production systems are configured to restrict developers from deploying their own changes to the production environment without secondary approval.	Inspected approval configurations for in-scope repositories to determine whether in-scope repositories were configured to require a secondary approver prior to deployment. Inspected a system generated listing of accounts with access to modify the approval configurations for in-scope repositories to determine whether access was appropriate based on job function.	No exceptions noted.
3.04	**Infrastructure Changes** Routine patches to infrastructure, such as operating system updates, are applied during monthly maintenance windows. *Refer to Control 4.03 for coverage over access to implement infrastructure changes.*	Inspected the Maintenance and Patching Standard to determine whether procedures for the maintenance and patching of information systems were formally documented and maintained. Inspected the patch reports for a selection of months and services to determine whether routine patches to infrastructure were applied during the maintenance window.	No exceptions noted.

Control Objective 4 – Logical Access:

Controls provide reasonable assurance that logical access to the network, in-scope applications, their related databases, and operating systems is restricted to appropriate individuals.

#	TouchNet's Control Activities	KPMG's Tests of Controls	Results of Tests
4.01	**User Access Provisioning** New user access requests to the operating systems, in-scope applications, and their related databases are approved by business and/or IT management and access granted is aligned to each employee's roles and responsibilities.	Inspected completed access requests and access listings for a selection of new and modified users to operating systems, in-scope applications, and their related databases to determine whether requested access was approved prior to access being granted and access granted matched the access requested.	No exceptions noted.
4.02	**User Access Deprovisioning** User access is revoked from the network, operating systems, in-scope applications, and their related databases following employee termination.	For a selection of terminated employees, compared the users' disabled dates from the network, operating system, in-scope applications, and their related databases, as applicable, to their termination dates to determine whether user accounts were disabled in a timely manner.	No exceptions noted.
4.03	**User Access Review** Business and/or IT management reviews the appropriateness of user access privileges to the in-scope applications and their related databases and operating systems on a semiannual basis. If any modifications are required, the system administrators modify the access privileges.	For a selection of applications and related databases and operating systems, inspected evidence of the user access reviews for both semiannual review periods to determine whether management performed the review and whether required modifications arising from the review were communicated and processed.	No exceptions noted.

#	TouchNet's Control Activities	KPMG's Tests of Controls	Results of Tests
4.04	**Password Parameters** Password parameters are required to be in compliance with the Global Payments Password Management Standard (e.g., expiration, minimum length, history, lockout, complexity). If the system is not in compliance, the system owner has identified, documented, and approved any exceptions to the policy as well as alternative controls to mitigate the risk.	Inspected the Global Payments Password Management Standard to determine whether password standards were defined. Inspected security settings for the network, operating systems, in-scope applications, and their related databases to determine whether the password and account lockout parameters were configured in accordance within the Global Payments Password Management Standard. For non-compliant systems, inspected the password exception acceptance form to determine whether the system owner has approved the exception and identified alternative controls to mitigate the risk.	No exceptions noted.

Control Objective 5 – Computer Operations:

Controls provide reasonable assurance that application and system processing is scheduled and monitored.

#	TouchNet's Control Activities	KPMG's Tests of Controls	Results of Tests
5.01	**Monitoring of Data Transmissions** The IT Support group is alerted of data transmission issues.	Inspected configurations within the tool used to monitor data transmissions between in-scope systems to determine whether the tool was configured to generate alert notifications for errors requiring investigation.	No exceptions noted.
5.02	**Resolution of Data Transmission Failures** The IT Support group monitors the production processing environment by investigating and resolving alerts.	Inspected the Incident Response Policy to determine whether procedures were in place for identifying and responding to production processing incidents. Inspected history logs for a selection of data transmission alerts to determine whether alerts were investigated and resolved within 1 business day.	No exceptions noted.

Section 5

Other Information Provided by Management of Global Payments

touchnet
A Global Payments Company

globalpayments

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;
- 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.
- BC/TR plans include:
  - The purpose, scope, and assumptions, as well as ownership;
  - Define individual's role and responsibilities for managing an event and the composition of the teams such as Incident Commander and recovery team, including communications;
  - Correspond to BIAs and related RTO and RPO targets;
  - List equipment, facilities, and vital records that are necessary for deploying response strategies;
  - 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, customers and customers, and other individuals.

The Company's 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, 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), 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 AI regulations including the EU Artificial Intelligence Act and the new U.S. state laws which will also bring new obligations for personal data as well as other data types.

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 TouchNet

TouchNet unifies campuswide payments and ID management software solutions for institutions of higher education around the world. Colleges and universities rely on TouchNet to integrate and secure payments, permissions, and other related business transactions for a comprehensive, actionable view campuswide. TouchNet's unmatched integration, transparency, and security give institutions greater control over transactions, costs, and compliance. As the market leader in higher education commerce technology, our platform-driven approach enables greater operational efficiencies and self-service access to real-time information for students and staff. TouchNet is a Global Payments company (NYSE: GPN).

touchnet
A Global Payments Company

globalpayments
globalpayments.com