System and Organization Controls – SOC 3 Report

For the period November 1, 2023, to October 31, 2024

Management's Report of its Assertion on the Design and Effectiveness of its Controls Over Lightspeed Commerce System based on the Trust Services Criteria related to Security and Confidentiality

TABLE OF CONTENTS

SECTION 1 ASSERTION OF LIGHTSPEED'S MANAGEMENT

ASSERTION OF LIGHTSPEED'S MANAGEMENT

January 22, 2025

We are responsible for designing, implementing, operating, and maintaining effective controls within Lightspeed Commerce Inc.'s (hereinafter referred to as 'Lightspeed,' 'the Company,' or 'the Service Organization') description of its Lightspeed Commerce System throughout the period November 1, 2023, to October 31, 2024, to provide reasonable assurance that Lightspeed's service commitments and system requirements relevant to security and confidentiality were achieved. Our description of the boundaries of the system is presented in Attachment A, which identifies aspects of the system covered by our assertion.

Lightspeed uses Cloud Service Providers for data management and environment hosting (subservice organizations). The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Lightspeed, to achieve Lightspeed's service commitments and system requirements based on the applicable trust services criteria. The description presents Lightspeed's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Lightspeed's controls. The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with the controls at Lightspeed, to achieve Lightspeed's service commitments and system requirements based on the applicable trust services criteria. The description presents Lightspeed's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Lightspeed's controls.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period November 1, 2023, to October 31, 2024, to provide reasonable assurance that Lightspeed's service commitments and system requirements were achieved based on the trust services criteria relevant to security and confidentiality (applicable trust services criteria) set forth in *TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy with Revised Points of Focus – 2022 (AICPA, Trust Services Criteria).*

Lightspeed's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Attachment B.

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

We assert that the controls within the system were effective throughout the period November 1, 2023, to October 31, 2024, to provide reasonable assurance that Lightspeed's service commitments and system requirements were achieved based on the applicable trust services criteria relevant to Security and Confidentiality as set forth in the *AICPA's TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy with Revised Points of Focus-2022(AICPA, Trust Services Criteria),* if subservice organizations and user entities applied the complementary controls assumed in the design of Lightspeed's controls throughout the period November 1, 2023, to October 31, 2024.

Sincerely,

Dan Micak
Chief Legal Officer & Company Secretary
Lightspeed Commerce Inc.

ATTACHMENT A

DESCRIPTION OF LIGHTSPEED'S SYSTEM RELEVANT TO SECURITY AND CONFIDENTIALITY

COMPANY OVERVIEW

Lightspeed Commerce Inc. ("Lightspeed" or the "Company") was incorporated on March 21, 2005, under the Canada Business Corporations Act. Its head office is located at Gare Viger, 700 Saint-Antoine St. East, Suite 300, Montréal, Quebec, Canada. Lightspeed's one-stop commerce platform provides its customers with the critical functionalities they need to engage with consumers, manage their operations, accept payments, and grow their business. Lightspeed has customers globally in over 100 countries, empowering single- and multi-location small and medium-sized businesses to compete in an omni-channel market environment by engaging with consumers across online, mobile, social, and physical channels.

The Company's shares are listed on both the Toronto Stock Exchange ("TSX") and the New York Stock Exchange ("NYSE") under the stock symbol "LSPD".

Headquartered in Montreal, Canada, Lightspeed is trusted by favorite local businesses worldwide, where communities go to shop and dine. Lightspeed has staff located in Canada, the USA, Europe, and APAC.

DESCRIPTION OF THE COMPANY'S SERVICES PROVIDED

Lightspeed is a cloud-based commerce platform powering small and medium-sized businesses in over 100 countries worldwide.

Lightspeed Retail (Omni + eCommerce)

Lightspeed Retail is an all-in-one solution for small and medium businesses. From optimizing stock, making sales, and learning from insights to grow the business, Lightspeed provides all the capabilities to run a successful business:

- Retail point of sale
- Smart inventory management
- Powerful reporting
- Flexible payment options
- Multi-store capabilities
- eCommerce integration

Lightspeed Hospitality

For driven hospitality professionals who want to accelerate revenue growth while providing the best guest experience, Lightspeed Restaurant is the fast, flexible, multi-location Platform that simplifies your processes and connects your teams so you can focus on what matters.

Unlike basic solutions that slow you down with extra steps, downtime, and unreliable support, Lightspeed tailors your system to your unique business with flexible POS, menuing, and back-of-house tools and integrations, plus industry-leading insights and personalized onboarding and support from a team of hospitality experts.

The capabilities include:

- Restaurant points of sale
- Smart inventory management
- Advanced Insights
- Flexible payment options
- Multi-store capabilities
- Order anywhere

Lightspeed Payment

Lightspeed Payments provides everything you need to process sales and get paid in one place. This service was built and integrated within the Retail and Hospitality platform to:

- Easily accept payments online and in-store.
- Provide a better experience for merchants and their customers.
- Provide built-in protection by complying with PCI DSS, providing constant monitoring for suspicious activity, and active global fraud prevention.
- Providing everything a merchant needs in one place.

LIGHTSPEED PRODUCTS

Lightspeed Products encompasses ten distinct offerings designed for three specific business types. Each of these products operates within its dedicated runtime environment, with individual Infrastructure as a Service (IaaS) cloud accounts. Architecturally, each product typically consists of two zones: the first, equipped with an Internet-facing firewall, and the second, within the VPC. The initial zone filter protects and routes traffic to the subsequent zone. Within the second zone, a variety of cloud services are employed to provide applications and data services.

The products include:
➢ Lightspeed Retail: Lightspeed Retail POS (X-Series); Lightspeed Retail POS (R-Series); Lightspeed eCom (C-Series); and Lightspeed eCom (E-Series);
➢ Lightspeed Hospitality: Lightspeed Restaurant POS (K-Series); Lightspeed Restaurant POS (L-Series); Lightspeed Restaurant POS (O-Series); Lightspeed Restaurant POS (U-Series);
➢ Lightspeed Payments;
➢ Lightspeed Golf

BOUNDARIES OF THE SYSTEM

The boundaries of the system are the specific aspects of Lightspeed's infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support customer services are not included within the system's boundaries.

SYSTEM COMPONENTS

The system is comprised of the following components:

Infrastructure includes the physical structures, information technology (IT), and other hardware.

The software includes key assets in providing services.

People include dedicated teams supporting the Lightspeed Commerce System. These include but are not limited to the following:

- Corporate. Executives, senior operations staff, global functions, and company administrative support staff, such as Finance, Go To Market (GTM), Information Systems (IS), IT, Security, Privacy, Legal, Office Operations, and People and Culture.

- Finance encompasses Accounting, Internal Audit, Financial Reporting, and Procurement functions;

- Go To Market (GTM) encompasses Customer Support, Sales, Partnerships, Marketing, Global Supply Chain & Hardware, and Revenue Operations;

- Information Systems (IS) provides pivotal support for core systems across the entire customer journey, including Customer Relationship Management (CRM).

- Legal encompasses Commercial, Employment, Corporate, and Privacy aspects.

- Product & Technology. Executives, senior operations staff, and product build staff such as designers, developers, QA, Product Managers, Service Reliability Experts (SRE), and Security and Data engineers. They build, operate, and monitor the Retail (Omni, e-commerce), Hospitality (Restaurant), Golf, and Payment systems to ensure the security and availability of services for Lightspeed's customers.

- Lightspeed software development staff develops and maintains Retail (Omni, e-commerce), Hospitality (Restaurant), Golf, and Payment systems software.

- The information security team supports Corporate, Retail, Hospitality, Golf, and Payment systems indirectly by building security architecture, implementing security strategy, performing security risk assessments, monitoring internal and external security threats, responding to security incidents and events, addressing security vulnerabilities, and maintaining internal and external security compliance programs.

- The SRE team is responsible for maintaining and monitoring all production infrastructure and ensuring the availability of services for Lightspeed's customers.

Procedures

Lightspeed has documented policies, standards, and procedures to support the operation and controls over the system.

Lightspeed's Information Security Policy establishes the organizational information security policy for Lightspeed Commerce. Lightspeed Commerce is committed to managing business risk at an appropriate level and in a manner that protects Lightspeed Commerce, its clients, and its clients' customers from unauthorized use or breach of private information and protects the Company's information system resources from accidental or intentional unauthorized use, modification, compromise, disclosure, or destruction.

Adherence to the Company's Information Security Policy is mandatory and helps safeguard the security, privacy, confidentiality, and availability of sensitive information. It also protects the interests of Lightspeed Commerce, its customers, personnel, and business partners. The Security group is responsible for drafting, reviewing, updating, managing executive sign-off, and publishing the Information Security Policy. The policy is reviewed at least on an annual basis.

The comprehensive Information Security Policy includes the following sections:

- Information security policy
- Artificial Intelligence Security Policy
- Backup Policy
- Data Classification Policy
- Data Retention & Disposal Policy
- Identity and Access Management policy
- Security Event Management policy
- Secure SDLC & Change Management policy
- Use Lightspeed Assets Responsibly Policy
- Vulnerability Management Policy
- Vendor Management policy

The Lightspeed Commerce Information Security Policy is supplemented by many formal operating processes and procedures.

Data

In its Information Security Policy, Lightspeed has established written policies and procedures related to Information classification, labeling, storage, isolation of confidential information, and disposal.

Within the context of Lightspeed Commerce, Lightspeed has defined four levels of data classification and associated data controls. They are defined as follows:

- Public - Information that has no restrictions on distribution inside or outside of the Company.
- Internal Use - Information not for distribution outside the Company.

- Confidential -Information which has compliance, contractual, and regulatory implications if it is improperly handled
- Restricted -Information that is handled on a need-to-know basis within the Company.

RELEVANT ASPECTS OF CONTROL ENVIRONMENT, RISK ASSESSMENT, INFORMATION AND COMMUNICATION, MONITORING ACTIVITIES, AND CONTROL ACTIVITIES

CONTROL ENVIRONMENT

At Lightspeed, the control environment is meticulously cultivated, commencing at the highest echelons of the organization. Executive and senior leadership play pivotal roles in establishing the Company's core values and setting the tone at the top. Every employee acknowledges the Company's Code of Business Conduct and Ethics, a foundational document that outlines guiding principles and serves as a cornerstone for ethical behavior upon hiring.

Leadership and Governance: The Lightspeed Chief Executive Officer (CEO) and the executive team bear the responsibility of setting the Company's strategy and corporate governance. They report to the Board of Directors, overseeing the overall direction of Lightspeed. The Executive Team, in collaboration with departmental leaders, formulates policies and procedures, ensuring their development and adherence. The commitment to a robust governance framework is exemplified by a management team that coordinates day-to-day operations and fosters a clear understanding of roles and responsibilities among employees.

Board Oversight: Lightspeed is dedicated to having a highly qualified and diverse Board of Directors. The Compensation, Nominating, and Governance Committee periodically reviews the composition and performance of the Board, incorporating a comprehensive annual self-assessment process. This evaluation includes peer assessments of individual Board members to ensure a high standard of governance.

Compliance and Risk Management: Lightspeed's commitment to customer data protection and compliance with regulatory requirements is evident in its consolidated annual operational plan. This plan outlines regulatory and compliance objectives, facilitating the identification and assessment of associated risks. Policies and procedures provide guidance on operational and information security, establishing a framework that supports Lightspeed environments.

Whistleblower Mechanism: An ethics hotline is in place for employees and third-party contractors to report any misconduct or violations of Lightspeed's policies. Material violations are handled according to the Company’s Whistleblower Policy and Procedure or other relevant policies, emphasizing disciplinary actions, including termination if necessary. Vendor or third-party contractor violations are reported to their Lightspeed relationship managers for appropriate action.

Organizational Structure and Performance Evaluation: Lightspeed's organizational structure is designed to align activities with company-wide objectives. Defining key areas of authority and responsibility and establishing appropriate reporting lines ensures effective planning, execution, control, and monitoring. The Company formally evaluates resourcing and staffing to align employee qualifications with business objectives, providing valuable feedback during the annual performance review process.

Information Security Framework: The Lightspeed Security team has implemented a robust information security framework. Regular reviews and updates of security policies, as well as comprehensive security training, including data classification and application security reviews, ensure the availability, confidentiality, and integrity of data. These measures align with the Company's commitment to maintaining a secure operational environment.

INFORMATION AND COMMUNICATION

Information and communication are an integral component of Lightspeed's internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations.

The Product and Technology team is pivotal in establishing and maintaining Lightspeed Products information services. This includes services supporting system operations, data science, software engineering, software architecture, security, and disaster recovery. Reporting directly to the Chief Product and Technology Officer, the team adheres to established policies and procedures safeguarding applications, services, and client data and enforcing logical security, physical security, and environmental controls. Cloud Service Providers provide the server and network hardware components for Lightspeed Products.

The information systems infrastructure supporting Lightspeed Products at Lightspeed Commerce is diligently managed by dedicated full-time employees. Robust communication methods are implemented to ensure that employees comprehend their individual roles and responsibilities and that significant events are communicated promptly. These methods encompass comprehensive training programs for new hires, ongoing on-the-job training initiatives, as well as periodic staff meetings and training workshops as deemed necessary. Each employee is furnished with a written job description explicitly outlining their responsibility to promptly communicate significant issues and exceptions to the appropriate higher level of authority.

RISK MANAGEMENT

Lightspeed has instituted an Enterprise Risk Management process to systematically identify and address potential risks that could impact on the Company's ability to deliver reliable services to its clients. This comprehensive approach necessitates management to pinpoint significant risks within their respective areas of responsibility and implement tailored measures to mitigate these risks.

In the formulation of its controls, the Company considers the potential risks that might hinder the effective achievement of its objectives.

Key risks that the Company is actively focused on managing encompass:

- Reputational Risks: Arising from errors or fraud occurrences.
- Compliance Risks: Ensuring adherence to relevant regulations.
- Data Security Risks: Safeguarding the security of sensitive information.

Lightspeed adopts a holistic perspective, identifying risks throughout the entity and conducting a thorough analysis as the foundation for determining risk management strategies. This process involves evaluating possible threats and vulnerabilities relative to each objective, considering both internal and external factors and their potential impact on goal attainment.

The risk management process actively engages appropriate levels of management, involving an in-depth analysis that estimates the likelihood and significance of a risk's manifestation. Decisions on risk management encompass acceptance, avoidance, mitigation, or sharing of the identified risks. In tandem with the risk management process, Lightspeed formulates mitigation strategies for identified risks.

The Information Security department plays a pivotal role by establishing an Information Security Risk Management Framework and Security Risk Assessment Procedures that align seamlessly with the broader Enterprise Risk Management process. These procedures outline a meticulous step-by-step process, including the identification of security risks, the creation of tickets, the managerial review of risk assessments, and the submission of security risk assessments. Upon completion, the risk level and treatment plan are finalized.

To ensure ongoing effectiveness, the Information Security Risk Register is subject to regular measurement and review by senior management, underscoring Lightspeed's commitment to proactively managing and adapting to the evolving risk landscape.

MONITORING ACTIVITIES

Lightspeed’s management performs monitoring activities to assess the quality of internal control over time, monitors activities throughout the year, and takes corrective actions to address deviations from company policy and procedures. The Risk Committee routinely reviews internal controls, aided by reports from Privacy, Security, Product, and Technology on anomalies and exceptions. It tracks, analyzes, and resolves issues systematically. Executive management meets regularly to discuss policies, procedures, workload, and other key matters.

Lightspeed implements robust monitoring and alerting mechanisms to identify and respond to operational incidents. Automated monitoring systems track key operational metrics, detect unauthorized activities, and alert management when early warning thresholds are crossed. A ticketing system logs incidents, assigns severity ratings, and tracks resolutions.

CONTROL ACTIVITIES

Personnel Security

The People and Culture department manages HR policies, hiring, onboarding, and terminations. Hiring includes background checks and confidentiality agreements. New employees receive orientation and mandatory Security Awareness training. For terminations, IT promptly deactivates accounts to ensure secure access.

Logical Security

Ensuring tightly controlled access to Lightspeed Products systems is critical to overall system security. Only authorized users are granted access to Lightspeed Products systems. The IT team grants system access following relevant processes and procedures. Service owners grant granular roles in the system based on business requirements. Lightspeed has established policies and procedures to delineate standards for logical access to Lightspeed's systems.

Procedures and mechanisms are in place to restrict unauthorized internal and external access to data, and access to customer data is appropriately segregated from other customers.

Lightspeed employs the concept of least privilege, allowing only the necessary access for users to accomplish their job functions. User accounts are created to have minimal access.

Access above these least privileges requires an appropriate and separate authorization. Access control lists or permission groups granting access to critical Infrastructure are periodically reviewed for appropriateness. Access is revoked when an employee’s record is terminated in Lightspeed's HR system. Strong password parameters, including minimum length, expiration, complexity, history retention, and account lockout, are in place for the network and applications.

Access to all assets is facilitated remotely via the Identity and Access Management (IAM) platform, with multi-factor authentication (MFA) enforced for enhanced security.

Network Security

Lightspeed enforces strict firewall rules and intrusion prevention systems (IPS) to control network traffic and detect potential threats. Access to cloud resources is restricted to authorized employees based on defined roles. Continuous monitoring analyzes network traffic to enhance threat detection and security. A combination of native cloud security services and third-party solutions strengthens Lightspeed’s security posture, with all cloud resources subject to continuous monitoring and logging.

Lightspeed implements IDS and IPS for continuous monitoring, event filtering, and breach prevention, and management regularly reviews the outputs.

Security Configuration

Lightspeed has established configuration standards and utilizes security monitoring tools to continuously oversee, alert, and validate cloud resource configurations. Additionally, CIS policies are enforced to ensure compliance and maintain a secure cloud environment.

Vulnerability Management

Lightspeed ensures security through annual penetration tests, regular vulnerability scans, and a bug bounty program. The Security team monitors threats and vendor patches. Employee workstations have MDM, encryption, firewalls, and endpoint protection. Any unusual activity is promptly addressed.

Malware Prevention & Detection

Lightspeed has implemented Malware Prevention and Detection software on all end-user computers. This software plays a crucial role in detecting threats and shielding our systems from malicious program activity.

Asset Inventory

An inventory listing of all hardware and software within the scope of services is maintained and reviewed on at least an annual basis during the risk assessment process.

Encryption

Data at rest and in transit is encrypted using industry-standard encryption technologies to ensure confidentiality and integrity. SSL/TLS and other encryption technologies are used for defined points of connectivity and to protect communications between the processing center and users connecting to the processing center from within or external to customer networks.

Change Management

Lightspeed's change management process governs all application and infrastructure changes, including production updates, new feature development, patch requests, and network modifications. Change requests are managed through issue tracking and change management tools for transparency and accountability. The process includes segregated environments, automated testing, stakeholder approvals, feature flags for controlled rollouts, and rollback procedures. Security reviews all major code changes, prioritizing critical fixes before deployment.

Software Development Lifecycle (SDLC)

Lightspeed follows an agile development process, integrating planning, design, development, testing, and implementation into an iterative framework. New feature development aligns with business objectives and undergoes risk assessment and design review. Agile teams break projects into tasks, ensuring security, performance, maintainability, and testability.

Patch Management

Lightspeed has implemented a patch management process to ensure infrastructure systems are patched according to vendor-recommended operating system patches. Lightspeed also implements administrative and logical controls to ensure the effective execution of patching activities. Patches and upgrades follow a unified change management process, ensuring consistency and adherence to established procedures.

Security Incident Management

Lightspeed has documented a Security Event Management policy and plan that outlines an organized approach for responding to security breaches and incidents. The Lightspeed Security team is responsible for monitoring systems, tracking issues, and documenting findings of security-related events. Records are maintained for security breaches and incidents, which include status information, information required for supporting forensic activities, trend analysis, and evaluation of incident details. As part of the process, potential breaches of customer content are investigated and escalated to Lightspeed Security and Lightspeed Legal. Affected customers and regulators are notified of breaches and incidents where legally required.

Business Continuity and Disaster Recovery

Lightspeed has a documented Business Continuity and Disaster Recovery Plan to ensure the restoration of system services in line with customer commitments. Annual BCP testing is conducted to validate the effectiveness of recovery procedures.

Backup and Recovery

Lightspeed Products exclusively relies on 100% cloud-hosted infrastructure, eliminating the presence of any physical servers. Continuous backup procedures are integral to the Company's operations, with customer data systematically backed up on regular schedules. These backups are executed within the respective cloud providers with redundancy measures implemented across different regions within the same cloud vendor. This approach ensures the resilience and availability of critical data, aligning with Lightspeed's commitment to robust data protection and recovery practices.

Third-Party Security

Management has established requirements for third-party vendors and service providers. Agreements are established with third-party vendors and service providers relevant to the System, and they include clearly defined terms, conditions, and responsibilities. Responsibilities include confidentiality and privacy commitments as applicable. Agreements include clauses to terminate relationships when necessary. Management obtains and reviews the SOC reports from service providers to ensure controls are operating effectively and any identified risks are addressed to the service providers in a timely manner.

Physical and Environmental Security

Lightspeed Products' production servers are maintained at the Cloud Service Providers data centers. Physical security and environmental protection are the responsibility of the subservice organization. Lightspeed's management obtains and reviews SOC reports annually. Access to all production data centers is restricted to authorized users only. Multi-factor authentication is used to secure access to the production network, which is accessible only through tightly controlled jump hosts. All activity is logged and audited.

Confidentiality

Lightspeed Commerce has defined a set of policies and procedures to ensure the confidentiality of clients' sensitive information. Lightspeed Commerce's Code of Conduct requires that employees maintain the highest degree of confidentiality when handling customer matters and information.

SUBSERVICE ORGANIZATIONS

Lightspeed relies on Cloud Service Providers (CSPs) for data management and hosting of its operational environments. To ensure the security, availability, and reliability of these services, Lightspeed conducts an annual risk assessment review of vendors that provide mission-critical support for its production environment.

This assessment evaluates various risk factors, including vendor security controls, compliance with regulatory standards, data protection measures, service availability, and incident response capabilities. The review process helps identify potential vulnerabilities, assess vendor performance, and ensure service providers align with Lightspeed's security and operational requirements. Based on the findings, necessary remediation measures are implemented to mitigate risks and strengthen overall resilience.

COMPLEMENTARY USER ENTITY CONTROLS

Lightspeed Commerce defines key internal control responsibilities for user entities to ensure a secure and efficient interaction with its platform. User entities must adhere to contractual obligations, keep contact information up to date, and maintain accurate system records. They are responsible for overseeing platform usage, safeguarding credentials, reporting security incidents, and establishing disaster recovery plans. Additionally, they must enforce access controls, ensure data accuracy, maintain backups, and comply with all relevant policies and regulations.

ATTACHMENT B

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Service commitments

Lightspeed communicates service commitments to user entities (Lightspeed customers) in the form of customer agreements, contracts, or through the description of the service offerings provided online through the Lightspeed website (https://www.lightspeedhq.com/).

At the customer level, Lightspeed has also implemented various methods of external communication to support its customer base and the community. Mechanisms are in place to allow the customer support team to be notified and to notify customers of potential operational issues that could impact the customer experience. A Service Status page is available and maintained to alert customers of issues that may be of broad impact. Current status can be checked by the customer on the site or by subscribing via e-mail to be notified of interruptions.

Customers have the ability to contact Lightspeed via chat, e-mail, and phone for any issue related to the Lightspeed services they are subscribed to. Lightspeed also deploys monitoring and alerting mechanisms to identify and notify operational and management personnel of incidents when early warning thresholds are crossed on key operational metrics. Additionally, incidents are logged within a ticketing system, assigned severity ratings, and tracked to resolution.

System requirements

The selection and use of services by Lightspeed's customers must be set up and operated under a shared responsibility model so that the functionality of the services and the associated security are appropriately managed. Lightspeed is responsible for protecting the infrastructure that runs the service(s) offered in the Cloud. Lightspeed's responsibility changes depending on the service level and responsibility matrices set forth by the cloud provider.

The customer's responsibility is determined by the service(s) that a customer selects and the interdependencies of those services within the Lightspeed-managed Cloud. Customers are responsible for their own IT infrastructure and connectivity, as well as managing access to their Lightspeed accounts through built-in role-based access control mechanisms within all products and services.

Lightspeed has defined the following objectives to support the security, change, and operational processes underlying their service commitments and business requirements. The objectives ensure the system operates and mitigates the risks that threaten the achievement of the service commitments. The objectives below provide reasonable assurance that:

- Data integrity and confidentiality are maintained through all phases, including transmission, storage, and processing.
- Procedures have been established so that Lightspeed employee user accounts are added, modified, and deleted in a timely manner and reviewed regularly.

- Policies and mechanisms are in place to appropriately restrict unauthorized internal and external access to data, and customer data is appropriately segregated from other customers.
- System incidents are recorded, analyzed, and resolved.
- Changes (including emergency/non-routine and configuration) to existing IT resources are logged, authorized, tested, approved, and documented.
- Critical system components are replicated across multiple Availability Zones, and authoritative backups are maintained and monitored to ensure successful replication to meet the service commitments.
- Controls are implemented to safeguard data from within and outside of the boundaries of environments that store a customer's content to meet service commitments.

SECTION 2 INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To Management of Lightspeed Commerce Inc.

Scope

We have examined Lightspeed Commerce Inc. (hereinafter referred to as 'Lightspeed,' 'the Company' or 'the Service Organization') accompanying assertion titled "Assertion of Lightspeed's Management" (assertion) that the controls within Lightspeed's system were effective throughout the period November 1, 2023, to October 31, 2024, to provide reasonable assurance that Lightspeed's service commitments and system requirements were achieved based on the trust services criteria relevant to security and confidentiality (applicable trust services criteria) set forth in *TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy with Revised Points of Focus – 2022 (AICPA, Trust Services Criteria).*

Lightspeed uses Cloud Service Providers for data management and environment hosting (subservice organization). The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Lightspeed, to achieve Lightspeed's service commitments and system requirements based on the applicable trust services criteria. The description presents Lightspeed's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Lightspeed's controls. Our examination did not extend to the controls of subservice organizations.

The description indicates that certain applicable trust services criteria specified in the description can be achieved only if complementary user entity controls contemplated in the design of Lightspeed's controls are suitably designed and operating effectively, along with the related controls at the service organization. Our examination did not extend to such complementary user entity controls.

Service Organization Responsibilities

Lightspeed is responsible for its service commitments and system requirements and for designing, implementing, and operating adequate controls within the system to provide reasonable assurance that Lightspeed's service commitments and system requirements were achieved. Lightspeed has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Lightspeed is responsible for selecting and identifying the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with the attestation standards established by the American Institute of Certified Public Accountants.

Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

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

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

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Lightspeed's 'Lightspeed Commerce System' were effective throughout the period November 1, 2023, to October 31, 2024, to provide reasonable assurance that Lightspeed's service commitments and system requirements were achieved based on the applicable trust service criteria, is fairly stated, in all material respects, if subservice organization and user entity controls assumed in the design of Lightspeed's controls operated effectively throughout the period November 1, 2023, to October 31, 2024.

Sincerely Yours,

ControlCase SOC Audit Services

January 22, 2025

APPENDIX A: GLOSSARY

Applicable trust services criteria. The criteria codified in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022), in AICPA Trust Services Criteria, used to evaluate controls relevant to the trust services category or categories included within the scope of a particular examination.

Authentication. The process of verifying the identity or other attributes claimed by or assumed of an entity (user, process, or device) or to verify the source and integrity of data.

Authorization. The process of granting access privileges to a user, program, or process by a person who has the authority to grant such access.

Boundaries of the system (or system boundaries). The boundaries of a system are the specific aspects of a service organization's infrastructure, software, people, procedures, and data necessary to provide its services. When systems for multiple services share aspects, infrastructure, software, people, procedures, and data, the systems will overlap, but the boundaries of each system will differ. In a SOC 2 engagement that addresses the confidentiality and privacy criteria, the system boundaries cover, at a minimum, all the system components as they relate to the life cycle of the confidential and personal information within well-defined processes and informal ad hoc procedures.

Carve-out method. Method of addressing the services provided by a subservice organization in which the components of the subservice organization's system used to provide the services to the service organization are excluded from the description of the service organization's system and the scope of the examination. However, the description identifies (a) the nature of the services performed by the subservice organization; (b)the types of controls expected to be performed at the subservice organization that are necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization's service commitments and system requirements were achieved; and (c) the controls at the service organization used to monitor the effectiveness of the subservice organization's controls.

Complementary subservice organization controls (CSOCs). Controls that service organization management assumed, in the design of the service organization's system, would be implemented by the subservice organization and that are necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization's service commitments and system requirements are achieved.

Commitments. Declarations made by management to customers regarding the performance of one or more systems that provide services or products. Commitments can be communicated in written individualized agreements, standardized contracts, service level agreements, or published statements (for example, a security practices statement). A commitment may relate to one or more trust service categories. Commitments may be made on many different aspects of the service being provided, or the product, production, manufacturing, or distribution specifications.

Criteria. The benchmarks are used to measure or evaluate the subject matter.

APPENDIX A: GLOSSARY

Environmental protection and safeguards. Controls and other activities are implemented by the entity to detect, prevent, and manage the risk of casualty damage to the physical elements of the information system (for example, protection from fire, flood, wind, earthquake, power surge, or power outage).

Information and systems. Refers to information in electronic form (electronic information) during its infrastructure. The collection of physical or virtual resources that support an overall IT environment, including the server, storage, and network elements.

Internal control. A process effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance.

Personal information. Information that is or can be about or related to an identifiable individual.

Policies. Management or board member statements of what should be done to effect control. Such statements may be documented, explicitly stated in communications, or implied through actions and decisions. Policies serve as the basis for procedures.

Practitioner. A CPA performs an examination of controls within an entity's system relevant to security, availability, processing integrity, confidentiality, or privacy.

Risk. The possibility that an event will occur and adversely affect the achievement of objectives.

Security incident. A security event that requires action on the part of an entity in order to protect information assets and resources.

System. Refers to the infrastructure, software, people, processes, and data that are designed, implemented, and operated to work together to achieve one or more specific business objectives in accordance with management-specified requirements.

System components. Refers to the individual elements of a system. System components can be classified into the following five categories: infrastructure, software, people, processes, and data.

SOC 3 Engagement. An examination engagement to report on management's assertion about whether controls within the system were effective in providing reasonable assurance that the service organization's service commitments and system requirements were achieved based on the trust services criteria relevant to one or more of the trust services categories (applicable trust services criteria.)

subservice organization. A vendor used by a service organization performs controls that are necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization's service commitments and system requirements were achieved.

APPENDIX A: GLOSSARY

System requirements. Specifications about how the system should function to (a) meet the service organization's service commitments to user entities and others (such as user entities' customers); (b) meet the service organization's commitments to vendors and business partners; (c) comply with relevant laws and regulations and guidelines of industry groups, such as business or trade associations; and (d) achieve other
objectives of the service organization that are relevant to the trust services categories addressed by the description. Requirements are often specified in the service organization's system policies and procedures, system design documentation, contracts with customers, and government regulations.

Trust services. A set of professional attestation and advisory services based on a core set of criteria (trust services criteria) related to security, availability, processing integrity, confidentiality, or privacy.

Unauthorized access. Access to information or system components that (a) has not been approved by a person designated to do so by management and (b) compromises segregation of duties, confidentiality commitments, or otherwise increases risks to the information or system components beyond the levels approved by management (that is, access is inappropriate). User entity. An entity that uses the services provided by a service organization.

User entity. An entity that uses the services provided by a service organization.

Vendor. An individual or business (and its employees) engaged to provide services to the service organization. Depending on the services a vendor provides (for example, if it operates certain controls on behalf of the service organization that is necessary, in combination with the service organization's controls, to provide reasonable assurance that the service organization's service commitments and system requirements were achieved), a vendor might also be a subservice organization.

{Remainder of the page is left blank intentionally}

END OF REPORT