System and Organization Controls – SOC 3 Report

For the period October 1, 2024, to September 30, 2025

Management's Report of its Assertion on the Effectiveness of its Controls Over Lightspeed NuORDER System based on the Trust Services Criteria Related to Security.

TABLE OF CONTENTS

SECTION 1: ASSERTION OF LIGHTSPEED NuORDER'S MANAGEMENT

ASSERTION OF THE MANAGEMENT OF LIGHTSPEED NuORDER INC.

December 11, 2025

We are responsible for designing, implementing, operating, and maintaining effective controls within Lightspeed NuORDER Inc.'s (hereinafter referred to as 'Lightspeed NuORDER,' 'the Company,' or 'the Service Organization') description of its Lightspeed NuORDER System throughout the period October 1, 2024, to September 30, 2025, to provide reasonable assurance that Lightspeed NuORDER's service commitments and system requirements relevant to Security 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 NuORDER 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 NuORDER, to achieve Lightspeed NuORDER's service commitments and system requirements based on the applicable trust services criteria. The description presents Lightspeed NuORDER's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Lightspeed NuORDER'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 NuORDER, to achieve Lightspeed NuORDER's service commitments and system requirements based on the applicable trust services criteria. The description presents Lightspeed NuORDER's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Lightspeed NuORDER's controls.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period October 1, 2024, to September 30, 2025, to provide reasonable assurance that Lightspeed NuORDER's service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in *TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy with Revised Points of Focus – 2022 (AICPA, Trust Services Criteria).*

Lightspeed NuORDER'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 October 1, 2024, to September 30, 2025, to provide reasonable assurance that Lightspeed NuORDER's service commitments and system requirements were achieved based on the applicable trust services criteria relevant to Security 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 subservice organization controls assumed in the design of Lightspeed NuORDER's controls throughout the period October 1, 2024, to September 30, 2025.

Sincerely,

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

ATTACHMENT A

DESCRIPTION OF LIGHTSPEED NUORDER SYSTEM RELEVANT TO SECURITY

COMPANY OVERVIEW

Lightspeed Commerce is a one-stop commerce platform that helps merchants innovate to simplify, scale, and provide exceptional customer experiences. Since 2005, Lightspeed's cloud commerce solution has been transforming and unifying online and physical operations, multichannel sales, expansion to new locations, global payments, financial solutions, and connection to supplier networks. Lightspeed acquired NuORDER, a B2B eCommerce platform, in 2021.

The Lightspeed NuORDER platform provides brands and retailers with a central hub to browse products and catalogs, access real-time inventory data, and place orders from a computer or native iOS app. Lightspeed NuORDER integrates directly with over 100 ERPs, 3PL, CRM, PLM, and accounting systems, including NetSuite, Microsoft Dynamics, SAP, Oracle, Sage, and A2000.

Lightspeed NuORDER clients include many top brands within the Apparel, Footwear, Sports & Outdoor, Home & Gift, and Consumer Electronics industries.

DESCRIPTION OF THE COMPANY'S SERVICES PROVIDED

Wholesale Ordering Platform: (Web & Mobile) Lightspeed NuORDER provides the clients with an e-commerce platform for their wholesale business. They are able to load their product and inventory data, create catalogs, place orders, run reports, and market directly to their customers via campaigns. Retailers are able to log in and place orders directly with brands that they have been connected with on the platform. The wholesale ordering platform is available as both a web client and as a native iOS application.

Retail Assortments Platform (Web): Lightspeed NuORDER provides clients with a digital platform to optimize their retail buying. Buyers, planners, and merchandisers are able to browse vendor catalogs, select products, add notes and photos, plan units per size and location, and compare totals to targets. Analytic tools allow the retailer to review the assortment from multiple perspectives, including flexible categorization, financial metrics, and visual aesthetics, within a single vendor or across multiple vendors and departments. Live collaboration allows multiple users to work together in real time, streamlining the interactions between the buying team and vendors.

Network (Web): Lightspeed NuORDER and Lightspeed Commerce provide a close integration between the Wholesale Ordering Platform and the Lightspeed Retail POS, allowing retail store owners and buyers to sync orders and product data between the two systems, simplifying their workflows and letting them focus on running their store.

Digital Tradeshow: Lightspeed NuORDER maintains an online tradeshow where brands and retailers can connect.

Payment Processing: Lightspeed NuORDER provides (optional) credit card processing for clients that sign up for the service. Credit card processing is provided through Lightspeed Payments, which is a payment facilitator service. Lightspeed NuORDER also offers "Bring Your Own Processor" support through an integration with Spreedly.

AuthLS: Lightspeed's internal authentication application provides for secure verification of a user's credentials and management of Single Sign-On functionality.

Integration with External Systems: Lightspeed NuORDER provides data integrations with numerous external systems. These integrations may be API or SFTP-based, depending on the capabilities and needs of the external System. The System can process both incoming and outgoing integrations, and will typically integrate product, retailer, inventory, order, and pricing data.

BOUNDARIES OF THE SYSTEM

The boundaries of the System are the specific aspects of Lightspeed NuORDER'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 NuORDER System. These include, but are not limited to, the following:

- Executive - The executive team is responsible for general oversight and strategic planning.
- Engineering - The engineering team is responsible for delivering a performant, stable, and secure application that meets all feature specifications.
- Quality Assurance - The Quality Assurance team is responsible for validating that the application adheres to specifications through manual/exploratory and automated testing.
- Product - The Product team is responsible for feature planning (with assistance from engineering) & specification building, as well as user acceptance testing.
- Onboarding - The onboarding team is responsible for assisting new clients with setup and training, as well as integration with their ERPs & systems.
- Customer Support - Customer support is responsible for assisting clients with technical questions, product and functionality questions/support, and ongoing training.
- Account Management - Account management is responsible for working with clients to ensure they are utilizing the application to its full potential.
- IT - The IT team is responsible for provisioning and maintaining office workstations and networks.
- Payments - The payments team is responsible for managing business development, marketing, sales, account management, and new client setup for payment-enabled customers.
- Retail - The retail team is responsible for account management, success, onboarding, business development, and brand relationship management for enterprise retail customers.

- Digital Trade Event and Marketplace - This team is responsible for enterprise trade show partners' account management, success, onboarding, business development, and brand relationship management.
- Sales - The sales team is responsible for identifying and engaging prospective clients to learn more about their needs, teach them about Lightspeed NuORDER, and ultimately expand the client base.
- Marketing - The marketing team is responsible for driving revenue generation and communicating product launches, platform enhancements, and general company updates.
- Operations - The operations team is a global-spanning, problem-solving department whose mission is to foster a great working environment for each and every Lightspeeder. The Lightspeed Operations organization includes Information Technology, Project Management Office, Office Operations, Facilities, Payment Operations, Capital Operations, and Procurement. The team operates as a service center for the organization and provides its resources to help improve the experience for internal and external customers.
- Security - Responsible for protecting the System and Company from internal and external threats and for assessing and managing risk.

Procedures

Lightspeed NuORDER follows formal documented policies, standards, processes, and procedures that are established by Lightspeed Commerce around Data Security, Endpoint Security, Identity and Access Management, Risk Management, SDLC and Change Management, Security Event Management, Vendor Management, and Vulnerability Management. All teams are expected to adhere to the policies, which are located within the company intranet and can be accessed at any time by any team member. Our 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 of the Information Security Policy. The policy is reviewed on at least 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, four levels of data classification and associated data controls have been defined. 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 that 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, along with establishing appropriate reporting lines, ensures effective planning, execution, control, and monitoring. The Company conducts a formal evaluation of 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, 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. This process encompasses the primary classes of transactions of the organization, including the dependence on and complexity of information technology. At Lightspeed, information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, regulators, and employees.

Company-wide and departmental OKRs are updated regularly in Lightspeed's internal tool, providing insight and information into strategic initiatives within the organization. Leadership teams within departments meet regularly to discuss operational efficiencies within their functional areas and to disseminate new policies, procedures, and controls.

Additionally, town hall meetings are held regularly in each geographic location to provide staff with updates on the firm and key issues affecting the organization and its employees. Senior executives lead the town hall meetings with information gathered from formal automated information systems and informal databases, as well as conversations with various internal and external colleagues.

Lightspeed-wide priorities, goals, and results across privacy and Security are discussed in recurring Privacy and Security Steering Committee meetings, which are attended by representatives from all business units, executives, and legal. General updates to entity-wide security policies and procedures are usually communicated to the appropriate Lightspeed NuORDER personnel via e-mail messages and Slack notifications.

RISK MANAGEMENT

Lightspeed NuORDER aligns with Lightspeed Commerce's security risk management framework. This framework includes processes that identify and manage risks that could potentially affect Lightspeed NuORDER's ability to provide reliable services to user organizations. This ongoing process requires that management identify significant risks inherent in products or services as they oversee their areas of responsibility. Lightspeed NuORDER identifies the underlying sources of risk, measures the impact on the organization, establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks.

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

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

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

Integration with Risk Assessment

The environment in which the System operates, the commitments, agreements, and responsibilities of Lightspeed's NuORDER Commerce Platform Services System, as well as the nature of the components of the System, result in risks that the criteria will not be met. Lightspeed addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because each System and the environment in which it operates are unique, the combination of risks to meet the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the System, Lightspeed's management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

MONITORING ACTIVITIES

Lightspeed's management conducts quality assurance monitoring on a regular basis, and additional training is provided based on the results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications. Management's close involvement in Lightspeed NuORDER's operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in the Company's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of Lightspeed NuORDER's personnel.

Lightspeed implements robust monitoring and alerting mechanisms to identify and respond to operational incidents. Automated monitoring systems track key operational metrics, detect unauthorized activity, 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

Lightspeed NuORDER has implemented procedures and technical mechanisms to restrict unauthorized internal and external access to data. Logical access controls are designed to ensure that access to customer data is appropriately restricted and that customer data is logically segregated from that of other customers.

User access to systems is managed through centralized identity and access management processes operating under a role-based access control model. Access to resources is granted based on job responsibilities and business needs. Strong authentication mechanisms, including multi-factor authentication, are required for employees accessing Lightspeed NuORDER systems.

Network Security

Lightspeed has implemented network security controls to protect its cloud environment and restrict unauthorized access. Firewall and network traffic control mechanisms are in place to manage data flows between internal and external networks and to prevent unauthorized traffic. Intrusion detection and prevention capabilities are used to monitor network activity and identify potential security events.

Access to cloud network resources is limited to authorized personnel and is granted based on defined access roles and business requirements. Network activity is continuously monitored using centralized monitoring and logging capabilities to support proactive threat detection and response.

Cloud infrastructure resources are protected through a combination of native cloud security services and third-party security solutions. These controls provide continuous visibility into network activity and support a layered defense strategy designed to maintain a secure cloud environment.

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 are equipped with 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 NuORDER 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 NuORDER 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 sets forth an organized approach to 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 of security breaches and incidents, including status information, information required to support forensic activities, trend analysis, and evaluations 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.

Backup and Recovery

Lightspeed NuORDER maintains regular, automated backups of all critical production datastores using native cloud-provider backup mechanisms. Backups are encrypted, retained in accordance with defined retention schedules, and stored securely within cloud provider environments. Access to backup systems and data is restricted to authorized engineering and SRE personnel only. Backup operations are actively monitored, and alerts are generated to ensure timely completion and reliability.

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 by the service providers in a timely manner.

Physical and Environmental Security

Lightspeed NuORDER's production servers are maintained at the Cloud Service Providers' data centers. Physical Security and environmental protection are the responsibility of the subservice organization. Lightspeed NuORDER'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.

SUBSERVICE ORGANIZATIONS

Lightspeed NuORDER 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 risk factors, including vendor security controls, regulatory compliance, 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 NuORDER'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 NuORDER defines key internal control responsibilities for user entities to ensure a secure and efficient interaction with its platform. User entities must comply with contractual obligations, keep contact information current, 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

Lightspeed NuORDER designs its processes and procedures to meet its objectives for its B2B Commerce Platform Services System. Those objectives are based on the service commitments that Lightspeed NuORDER makes to user entities, the laws and regulations that govern the provision of services, and the financial, operational, and compliance requirements that Lightspeed NuORDER has established for the services. The services of Lightspeed NuORDER are subject to the security and privacy requirements of the General Data Protection Regulation (where applicable), the Payment Card Industry Data Security Standard, as well as state privacy and security laws and regulations in the jurisdictions in which Lightspeed NuORDER operates. Additionally, Lightspeed NuORDER follows and enforces sanctions as required by the Office of Foreign Assets Control.

Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following:

Security principles exist within the fundamental designs of the NuORDER Commerce Platform Services System that are designed to permit system users to access the information they need based on their role in the System, while restricting them from accessing information not needed for their role.

Lightspeed NuORDER uses appropriate encryption technologies to protect customer data both at rest and in transit.

Lightspeed establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Lightspeed system policies and procedures, system design documentation, and contracts with customers. Lighspeed NuORDER follows Lightspeed Commerce's Information Security Policies and Standards. Those information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the System is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the NuORDER Commerce Platform Services System.

{Remainder of the page is intentionally left blank}

SECTION 2 INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To the Management of Lightspeed NuORDER Inc.

Scope

We have examined Lightspeed NuORDER Inc.'s (hereinafter referred to as 'Lightspeed NuORDER,' 'the Company' or 'the Service Organization') accompanying assertion titled "Assertion of Lightspeed NuORDER's Management" (assertion) that the controls within Lightspeed NuORDER system were effective throughout the period October 1, 2024, to September 30, 2025, to provide reasonable assurance that Lightspeed NuORDER's service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in *TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy with Revised Points of Focus – 2022 (AICPA, Trust Services Criteria).*

Lightspeed NuORDER uses Cloud Service Providers for data management and environment hosting. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Lightspeed NuORDER, to achieve its service commitments and system requirements related to the Lightspeed NuORDER system based on the applicable trust services criteria. The description presents Lightspeed NuORDER's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Lightspeed NuORDER'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 NuORDER'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 NuORDER 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 NuORDER's service commitments and system requirements were achieved. Lightspeed NuORDER has also provided the accompanying assertion about the effectiveness of controls within the System. When preparing its assertion, Lightspeed NuORDER 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 NuORDER'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 NuORDER'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 NuORDER system were effective throughout the period October 1, 2024, to September 30, 2025, to provide reasonable assurance that Lightspeed NuORDER's service commitments and system requirements were achieved based on the applicable trust service criteria, is fairly stated, in all material respects, if subservice organizations and user entity controls assumed in the design of Lightspeed NuORDER's controls operated effectively throughout the period October 1, 2024, to September 30, 2025.

Sincerely yours,

ControlCase SOC Audit Services

Attinkom LLC, dba ControlCase SOC Audit Service

December 11, 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