COALFIRE
CONTROLS

Report on Fluent Retail Pty Ltd.'s Fluent Order Management System Relevant to Security, Availability, Confidentiality, and Privacy Throughout the Period January 1, 2023 to April 30, 2023

SOC 3® - SOC for Service Organizations: Trust Services Criteria for General Use Report

fluentcommerce
order management. accelerated.

Table of Contents

Section 1

Section 1

Independent Service Auditor's Report

Independent Service Auditor's Report

To: Fluent Retail Pty Ltd. ("Fluent")

Scope

We have examined Fluent's accompanying assertion titled "Assertion of Fluent Retail Pty Ltd. Management" (assertion) that the controls within the Fluent Order Management System (system) were effective throughout the period January 1, 2023 to April 30, 2023, to provide reasonable assurance that Fluent's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, and privacy (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

The description of the boundaries of the system indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Fluent, to achieve Fluent's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the complementary user entity controls assumed in the design of Fluent's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Fluent uses a subservice organization to provide Platform as a Service (PaaS) services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Fluent, to achieve Fluent's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the types of complementary subservice organization controls assumed in the design of Fluent's controls. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

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

Service Auditor's Responsibilities

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

![Coalfire Controls logo]

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

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.

- Assessing the risks that controls were not effective to achieve Fluent'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 to achieve Fluent's service commitments and system requirements based on the applicable trust services criteria.

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

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 the Fluent Order Management System were effective throughout the period January 1, 2023 to April 30, 2023, to provide reasonable assurance that Fluent's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls and complementary user entity controls assumed in the design of Fluent's controls operated effectively throughout that period is fairly stated, in all material respects.

Coalfire Controls LLC

Greenwood Village, Colorado
June 21, 2023

Section 2

Assertion of Fluent Retail Pty Ltd. Management

Assertion of Fluent Retail Pty Ltd. ("Fluent") Management

We are responsible for designing, implementing, operating and maintaining effective controls within the Fluent Order Management System (system) throughout the period January 1, 2023 to April 30, 2023, to provide reasonable assurance that Fluent's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, and privacy (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). Our description of the boundaries of the system is presented in attachment A and identifies the aspects of the system covered by our assertion.

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

Fluent uses a subservice organization for Platform as a Service (PaaS) services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Fluent, to achieve Fluent's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the types of complementary subservice organization controls assumed in the design of Fluent's controls. The description of the boundaries of the system does not disclose the actual controls at the subservice organization.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period January 1, 2023 to April 30, 2023, to provide reasonable assurance that Fluent's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls and complementary user entity controls assumed in the design of Fluent's controls operated effectively throughout that period. Fluent'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 January 1, 2023 to April 30, 2023, to provide reasonable assurance that Fluent's service commitments and system requirements were achieved based on the applicable trust services criteria.

Fluent Retail Pty Ltd.

Attachment A

Fluent Retail Pty Ltd.'s Description of the Boundaries of Its Fluent Order Management System

Type of Services Provided

Fluent Retail Pty Ltd. ("Fluent Commerce," "Fluent," or "the Company") is an order orchestration and inventory management company headquartered in Sydney, Australia. The Fluent Order Management System ("the Platform") is a cloud-native, distributed platform that provides retailers with automation, in-store tooling, and smart order orchestration software for order fulfillment, inventory availability tracking, and customer service.

The boundaries of the system in this section of the report details the Fluent Order Management System. Any other Company services are not within the scope of this report. The accompanying description includes only the policies, procedures, and control activities at the Company. It does not include the policies, procedures, and control activities at any subservice organizations (see below for a further discussion of the subservice organization).

The Boundaries of the System Used to Provide the Services

The boundaries of the Fluent Order Management System are the specific aspects of the Company'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 the services provided to customers are not included within the boundaries of the Fluent Order Management System.

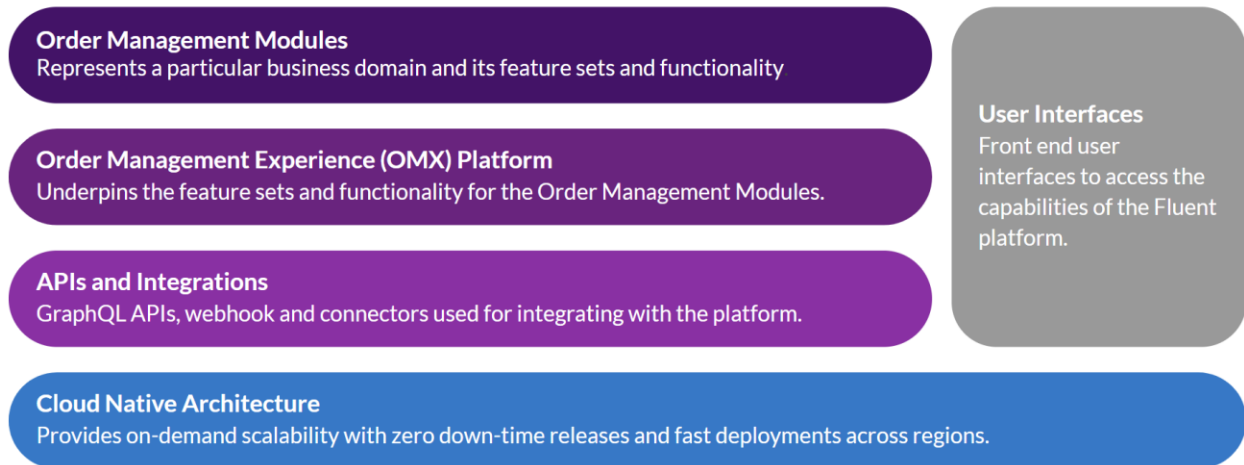The Fluent Order Management System consists of the key components described in the figure below:

Order Management Modules
Represents a particular business domain and its feature sets and functionality

Order Management Experience (OMX) Platform
Underpins the feature sets and functionality for the Order Management Modules.

APIs and Integrations
GraphQL APIs, webhook and connectors used for integrating with the platform.

Cloud Native Architecture
Provides on-demand scalability with zero down-time releases and fast deployments across regions.

User Interfaces
Front end user interfaces to access the capabilities of the Fluent platform.

Figure 1: Fluent Order Management System Key Components

The components that directly support customer services are described in the subsections below.

Infrastructure

The Company utilizes Amazon Web Services (AWS) to provide the resources to host the Fluent Order Management System. The Company leverages the experience and resources of AWS to scale quickly and securely as necessary to meet current and future demand. However, the Company is responsible for designing and configuring the Fluent Order Management System architecture within AWS to ensure security, availability, confidentiality, and privacy requirements are met.

There is no additional in-scope hosted infrastructure outside of the AWS ecosystem.

Software and Services

Software consists of the programs and software that support the Fluent Order Management System (operating systems [OSs], middleware, and utilities). The list of software and ancillary software used to build, support, secure, maintain, and monitor the Fluent Order Management System include the following applications, as shown in the table below:

Software	
Production Application	**Business Function**
Amazon OpenSearch Service (Elasticsearch)	Application monitoring
AWS Security Hub, AWS CloudTrail, Amazon GuardDuty, and Splunk	Security information and event management (SIEM), logging system, infrastructure monitoring
Amazon CloudWatch	Infrastructure monitoring
AWS Config	Configuration management
AWS Fargate, Amazon Elastic Container Service (ECS)	Containerization
Jira Service Desk	Help desk, ticketing system
JumpCloud	SaaS identity provider, mobile device management
Crowdstrike, Darktrace	Endpoint anti-malware protection
Bitbucket	Hosting code, configuration and build, deployment orchestration
Maven Repository	Hosting Java packages
Amazon Inspector	Vulnerability scanning
Ping Identity	Third party identity provider (IdP) that provides SSO access to the Fluent Order Management System for Client staff
Amazon Relational Database Service (RDS)	Backup scheduling and replication

People

The Company develops, manages, and secures the Fluent Order Management System via separate departments. The responsibilities of these departments are defined in the following table:

People	
Group/Role Name	**Function**
Executive Management	Responsible for overseeing company-wide activities, establishing and accomplishing goals, and managing objectives. Includes the Chief Executive Officer (CEO), Chief Financial Officer (CFO), Chief Operating Officer (COO), Chief Technology Officer, and Chief Strategy Officer (CSO)
Software Engineering	Responsible for the development, testing, and maintenance of new code for the Fluent Order Management System.
Cloud Engineering	Responsible for the orchestration and deployment of new code for the Fluent Order Management System, as well as for the design and deployment of the cloud infrastructure that hosts the Fluent Order Management System.
Site Reliability Engineering	Responsible for ensuring the ongoing performance of the production environment.
Information Security	Responsible for managing access controls and the security of the production environment.
Product	Responsible for overseeing the product life cycle, including adding new functionality.
People and Culture (P&C)	Responsible for onboarding new personnel, working with individual departments to define the roles and positions of new hires, performing background checks, and facilitating the employee termination process.
Privacy Working Groups	Responsible for ensuring compliance with privacy laws and regulations. This involves developing and implementing data privacy policies, conducting privacy impact assessments, liaising with supervisory authorities, and handling data subjects' queries and requests. The Privacy Working Groups also provides advice on data protection issues, manages potential data breaches, and maintains a comprehensive and accessible record of all data processing activities conducted by the company. Furthermore, they ensure data privacy training and awareness activities occur with employees to ensure they understand and comply with data privacy standards.

Procedures

Procedures include the automated and manual procedures involved in the operation of the Fluent Order Management System. Procedures are developed and documented by the respective teams for a variety of processes, including those relating to product management, engineering, technical operations, security, information technology (IT), and P&C. These procedures are drafted in alignment with the overall information security policies and are updated and approved as necessary for changes in the business, but no less than annually.

The following table details the procedures related to the operation of the Fluent Order Management System:

Procedures	
Procedure	**Description**
Logical Access	A centralized authentication and authorization platform is used to manage access to the system. This access is managed and monitored regularly to ensure that access is added and removed within the specified policy requirements.
System Operations	Through monitoring of the platform, integrated applications, and processes, actions are taken to detect and mitigate any unauthorized actions for both internal and external sources.
Change Management	As a standard operating procedure, changes to the Platform must meet a series of requirements to control and validate changes before implementation.
Risk Mitigation	Through an ongoing process identified within the Risk Management Policy, Fluent Commerce continually identifies and mitigates risks from external and internal sources, including vendors and business partners.

Data

Data refers to transaction streams, files, data stores, tables, and output used or processed by the Company. Through the application programming interface (API), the customer or end-user defines and controls the data they load into and store in the Fluent Order Management System production network. Once stored in the environment, the data is accessed remotely from customer systems via the Internet.

Customer data is managed, processed, and stored in accordance with relevant data protection and other regulations and with specific requirements formally established in client contracts.

The Company has deployed secure methods and protocols for the transmission of confidential or sensitive information over public networks. Encryption in transit is enforced through all Fluent Order Management System layers. Encryption is enabled for data stores housing sensitive customer data.

The following table details the types of data contained in the production Platform for the Fluent Order Management System:

Data	
Production Application	**Description**
Core API, GraphQL API, Events API, Rubix APIs	The Company keeps track of user activity in relation to the types of services customers and their users use and performance metrics related to their use of the services.
Core API, GraphQL API, Events API, Rubix APIs	The Company logs information about customers and their users, including Internet Protocol (IP) addresses. Log files are immutable records of events about an application or user activity that form an audit trail. These records may be used to assist in detecting security violations, performance problems, and application flaws.
Core API, GraphQL API, Events API, Rubix APIs	The company retains information about customers and their users, including order information, shipping information, and inventory records.

Complementary User Entity Controls (CUECs)

The Company's controls related to the Fluent Order Management System cover only a portion of overall internal control for each user entity of the Fluent Order Management System. It is not feasible for the service commitments, system requirements, and applicable criteria related to the system to be achieved solely by the Company. Therefore, each user entity's internal control should be evaluated in conjunction with the Company's controls taking into account the related CUECs identified for the specific criterion. In order for user entities to rely on the controls reported herein, each user entity must evaluate its own internal control to determine whether the identified CUECs have been implemented and are operating effectively.

The CUECs presented should not be regarded as a comprehensive list of all controls that should be employed by user entities. Management of user entities is responsible for the following:

Criteria	Complementary User Entity Controls

CC2.1	• User entities have policies and procedures to report any material changes to their overall control environment that may adversely affect services being performed by the Company according to contractually specified time frames.
	• Controls to provide reasonable assurance that the Company is notified of changes in:
	  – User entity vendor security requirements
	  – The authorized users list

CC2.3	• It is the responsibility of the user entity to have policies and procedures to:
	  – Inform their employees and users that their information or data is being used and stored by the Company.
	  – Determine how to file inquiries, complaints, and disputes to be passed on to the Company.

CC6.1	• User entities grant access to the Company's system to authorized and trained personnel. • Controls to provide reasonable assurance that policies and procedures are deployed over user IDs and passwords that are used to access services provided by the Company.
CC6.4	• User entities deploy physical security and environmental controls for all devices and access points residing at their operational facilities, including remote employees or at-home agents for which the user entity allows connectivity.
P5.1	• User entities retrieve personal information from the Company's system for data subject requests for access to their stored personal information on a timely basis.
P5.2 P6.7	• User entities correct PII data provided by data subjects in the Company's system timely. • User entities forward PII data deletion requests provided by data subjects to Fluent Commerce on a timely basis. • User entities forward data subject requests for an accounting of their PII to Fluent Commerce on a timely basis.
P8.1	• User entities forward data subject inquiries, complaints, and disputes related to their PII held by Fluent Commerce on a timely basis.

Subservice Organization and Complementary Subservice Organization Controls (CSOCs)

The Company uses AWS as a subservice organization for Platform as a Service (PaaS) services. The Company's controls related to the Fluent Order Management System cover only a portion of the overall internal control for each Fluent Order Management System user entity.

Although the subservice organization has been carved out for this report, certain service commitments, system requirements, and applicable criteria are intended to be met by controls at the subservice organization. CSOCs are expected to be in place at AWS related to physical security and environmental protection, as well as backup, recovery, and redundancy controls related to availability. AWS' physical security controls should mitigate the risk of unauthorized access to the hosting facilities. AWS' environmental protection controls should mitigate the risk of fires, power loss, climate, and temperature variabilities.

Company management receives and reviews the AWS SOC 2 report annually. In addition, through its operational activities, Company management monitors the services performed by AWS to determine whether operations and controls expected to be implemented are functioning effectively. Management also communicates with the subservice organization to monitor compliance with the service agreement, stay informed of changes planned at the hosting facility, and relay any issues or concerns to AWS management.

It is not feasible for the Company to achieve the service commitments, system requirements, and applicable criteria related to the Fluent Order Management System. Therefore, each user entity's internal control must be evaluated with the Company's controls considering the related CSOCs expected to be implemented at AWS as described below.

Criteria	Complementary Subservice Organization Controls
CC6.1	- AWS is responsible for encrypting databases in its control. - AWS is responsible for requiring unique usernames and passwords for authentication to the underlying operating system.
CC6.3	AWS is responsible for restricting privileged access to the underlying operating system to only authorized users.
CC6.4	- AWS is responsible for restricting data center access to authorized personnel. - AWS is responsible for the 24/7 monitoring of data centers by closed circuit cameras and security personnel.
CC6.5 CC6.7	AWS is responsible for securely decommissioning and physically destroying production assets in its control.
CC6.6 CC6.8 CC7.1 CC7.2 CC7.3	AWS is responsible for maintaining and managing the AWS Fargate underlying server infrastructure for their users and for keeping the host OS patched, secure, and up to date.
CC6.8	AWS is responsible for deploying antivirus technology on servers supporting the service.

Criteria	Complementary Subservice Organization Controls
CC7.2 A1.2	• AWS is responsible for the installation of fire suppression and detection and environmental monitoring systems at the data centers. • AWS is responsible for protecting data centers against disruption in power supply to the processing environment by an uninterruptible power supply (UPS). • AWS is responsible for overseeing the regular maintenance of environmental protections at data centers.

Specific Criteria Not Relevant to the System

The following Trust Services Criteria were determined to be not relevant to the Fluent Order Management System:

TSC Reference	Criteria	Reasoning
P1.1	The entity provides notice to data subjects about its privacy practices to meet the entity's objectives related to privacy. The notice is updated and communicated to data subjects in a timely manner for changes to the entity's privacy practices, including changes in the use of personal information, to meet the entity's objectives related to privacy.	The Company provides the Fluent Order Management System (OMS) and services to customers that collect and maintain personal information of data subjects, but the Company does not collect personal information from the data subjects directly. The customers of Fluent OMS as data controllers are responsible for the notice and communication of privacy objectives and are responsible for obtaining all necessary rights or consents required to allow the Company to process personal information of data subjects. Therefore, the privacy criterion related to notice and communication is not applicable to the Company, as it acts as a data processor.
P2.1	The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice. Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons, if required. Such consent is obtained only for the intended purpose of the information to meet the entity's objectives related to privacy. The entity's basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented.	The Company provides the Fluent OMS and services to customers that collect and maintain personal information of data subjects, but the Company does not collect personal information from the data subjects directly. The customers of Fluent OMS as data controllers are responsible for the integrity, accuracy, completeness, and quality of the personal information provided to the Company and are responsible for obtaining all necessary rights or consents required to allow the Company to process personal information of data subjects. Therefore, the privacy criterion related to choice and consent is not applicable to the Company, as it acts as a data processor.

TSC Reference	Criteria	Reasoning
P3.1	Personal information is collected consistent with the entity's objectives related to privacy.	The Company provides the Fluent OMS and services to customers that collect and maintain personal information of data subjects, but the Company does not collect personal information from the data subjects directly. The customers of Fluent OMS as data controllers are responsible for the integrity, accuracy, completeness, and quality of the personal information provided to the Company and are responsible for obtaining all necessary rights or consents required to allow the Company to process personal information of data subjects. Therefore, the privacy criterion related to collection is not applicable to the Company, as it acts as a data processor.
P3.2	For information requiring explicit consent, the entity communicates the need for such consent, as well as the consequences of a failure to provide consent for the request for personal information, and obtains the consent prior to the collection of the information to meet the entity's objectives related to privacy.	The Company provides the Fluent OMS and services to customers that collect and maintain personal information of data subjects, but the Company does not collect personal information from the data subjects directly. The customers of Fluent OMS as data controllers are responsible for obtaining explicit consent to collect the personal information provided to the Company and are responsible for obtaining all necessary rights or consents required to allow the Company to process personal information of data subjects. Therefore, the privacy criterion related to collection is not applicable to the Company, as it acts as a data processor.

There were no other specific security, availability, confidentiality, or privacy Trust Services Criteria as set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, Trust Services Criteria) that were not relevant to the system as presented in this report.

Attachment B

Principal Service Commitments and System Requirements

Principal Service Commitments and System Requirements

Commitments are declarations made by management to customers regarding the performance of the Fluent Order Management System. Commitments are communicated in a written Master Services Agreement (MSA), Data Privacy Addendum (DPA), and published documentation on the Company portal (Lingo), including the Security Policy and Service Agreements.

System requirements are specifications regarding how the Fluent Order Management System should function to meet the Company's principal commitments to user entities. System requirements are specified in the Company's policies and procedures.

The Company's principal service commitments and system requirements related to the Fluent Order Management System include the following:

Trust Services Category	Service Commitments	System Requirements
Security	- The Company will maintain, implement, and adhere to a Security Policy. - The Company will maintain technical and organizational security measures to protect customer information against unauthorized access, loss of use, modification, disclosure, destruction, threats, or hazards. - The Company will notify the customer without undue delay of any incident or data breach.	- Implement access controls and authentication mechanisms to restrict access to only authorized users. - Utilize encryption to protect all client and server data transmissions. - Employ measures to prevent, detect, and mitigate unauthorized access or attacks, such as firewalls, intrusion detection systems, and threat intelligence. - Support multi-factor authentication to access the system. - Implement mechanisms for detecting and preventing cross-site scripting (XSS), SQL injection attacks, and other Platform vulnerabilities. - Perform security assessments and penetration testing to identify and remediate vulnerabilities in the Platform. - Maintain a documented incident response plan to handle security incidents, including data breaches and unauthorized access attempts. - Maintain a security awareness training program for all employees. - Maintain logging and auditing capabilities to enable tracking of user activity and system changes and to facilitate forensic investigations. - Apply security updates and patches to the Platform promptly and effectively. - Ensure that all third-party services and integrations used in the Platform meet the same security requirements as the core Platform itself.

Trust Services Category	Service Commitments	System Requirements
Availability	- The Company will ensure that the Fluent Order Management System will be available to customers, with an uptime commitment of at least 99.95% per month. - The Company will utilize real-time performance monitoring and alerting for any issues that may impact the availability of the Fluent Order Management System. - The Company will utilize auto-scaling mechanisms to dynamically meet client demand and regenerate hosts on demand.	- The Platform will be designed and architected for high availability and fault tolerance, with redundant systems and failover mechanisms in place to minimize downtime. - The Platform will have a monitoring and alerting system to detect and alert the support team about any issues that may impact availability. - The Platform will be able to handle spikes in traffic or usage without experiencing significant slowdowns or downtime. - The Platform will be regularly tested for its ability to handle various failures, including hardware failures, network outages, and software bugs. It will have procedures in place for recovering from such failures.
Confidentiality	- The Company will maintain the confidentiality of all data and information provided by customers and will not, without prior written consent, publish, use, or otherwise disclose to any person the confidential information except for the purposes contemplated, and as permitted, by contractual agreements. - The Company will implement appropriate security measures to protect the confidentiality of customer data, including access controls, encryption, and data masking. - The Company will promptly notify customers in the event of any unauthorized access, disclosure, or loss of customer data, and will work with the customer to mitigate the impact of any such incidents. - Upon termination of the services, the Company will anonymize, aggregate and/or delete all customer data.	- The Software-as-a-Service (SaaS) Platform is designed to minimize the collection and storage of sensitive data from customers and data minimization techniques are implemented to only collect the data that is strictly necessary for the service to function. - The Platform has access controls and encryption mechanisms to protect the confidentiality of customer data, both in transit and at rest. - The Support team will be trained to handle confidential data with the utmost care and respect. It will be required to sign non-disclosure agreements (NDAs) and adhere to strict confidentiality policies and procedures. - The Company will have a clearly defined incident response plan in place to handle any security breaches or other incidents that may impact the confidentiality of retail customer data and will notify affected customers in a timely and transparent manner in the event of any such incidents.

Trust Services Category	Service Commitments	System Requirements
Privacy	- The Company will process customer data solely for the purpose of providing the Fluent Order Management System. - The Company will implement appropriate security measures to protect the privacy of customer data, including access controls, encryption, and data masking. - The Company will comply with all applicable laws and regulations governing data privacy, including but not limited to the GDPR, CCPA, and other applicable privacy regulations. - The Company will notify customers of any new third parties with whom Fluent will share personal information, if any, at least 30 days in advance.	- The Company will provide information about data collection and processing practices, including how personal data is used, who it is shared with, and how long it is retained. - The Platform will give customers granular control over their data, including viewing, editing, deleting, and exporting their data as needed. - The Company will implement appropriate technical and organizational measures to protect personal data privacy, such as access controls, encryption, and anonymization in respect of the Platform. - The Company will maintain an up-to-date privacy policy that outlines its data collection and processing practices and will make this policy accessible to customers. - The Company will regularly review its compliance with all applicable laws and regulations governing the confidentiality of personal data, such as the GDPR, CCPA, and other applicable privacy regulations.