Fireloft, Inc.

d.b.a. StandardFusion

SOC 3

Independent Service Auditor's Report on Management's Description of a Service Organization's System Relevant to Security, Availability, and Confidentiality

January 1, 2023 – December 31, 2023

200 Second Avenue South, Suite 478
St. Petersburg, FL 33701

200 Second Avenue South, Suite 478
St. Petersburg, FL 33701
www.ascendaudit.com

INDEPENDENT SERVICE AUDITOR'S REPORT

The Management of Fireloft, Inc. d.b.a. StandardFusion
300 - 303 Pender St W
Vancouver BC, Canada V6B 1T3

Scope

We have examined Fireloft, Inc.'s, d.b.a. StandardFusion, ("StandardFusion", or "the Company") description of controls for its software-as-a-service GRC platform system and related transactions throughout the period January 1, 2023 through December 31, 2023, based on the criteria for a description of a service organization's system in DC Section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report (With Revised Implementation Guidance – 2022)(AICPA, Description Criteria), and the suitability of the design and operating effectiveness of controls stated in the description throughout the period January 1, 2023 through December 31, 2023, to provide reasonable assurance that StandardFusion's service commitments and system requirements were achieved based on the trust service criteria for security, availability, and confidentiality set forth 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.

Subservice Organizations

StandardFusion utilizes subservice organizations for the following services and applications:

- Hosting
- Identity management
- Email and file storage
- Infrastructure as a service
- Source code repository and version control
- Human resources management

StandardFusion LLC's Responsibilities

StandardFusion 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 StandardFusion's service commitments and system requirements were achieved. In section II, StandardFusion has provided its assertion titled "Assertion of Fireloft, Inc.'s, d.b.a. StandardFusion Service Organization Management" about the description and the suitability of design and operating effectiveness of controls stated therein. StandardFusion is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Ascend Audit & Advisory's Responsibilities

Our responsibility is to express an opinion on the description of the suitability of the design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs. 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 are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating 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 policies or procedures may deteriorate.

Opinion

In our opinion, StandardFusion's controls over the system were effective throughout the period January 1, 2023 through December 31, 2023 to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period.

Ascend Audit & Advisory

January 26, 2024

ASSERTION OF STANDARDFUSION SERVICE ORGANIZATION MANAGEMENT

We have prepared the description of Fireloft, Inc.'s, d.b.a. StandardFusion, software-as-a-service GRC platform system ("system" or "the system") throughout the period January 1, 2023 to December 31, 2023, ("the description") based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization System in a SOC 2 Report (With Revised Implementation Guidance – 2022)*(AICPA, Description Criteria). The description is intended to provide report users with information about the system that may be useful when assessing the risks arising from interactions with StandardFusion Service Organization's system, particularly information about system controls that StandardFusion has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality 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).

StandardFusion uses subservice organizations, Microsoft Office 365, Hibob Ltd., Microsoft Azure, and Amazon Web Services for enterprise office productivity software, a software-as-a-service HR information system platform, cloud based infrastructure, and cloud computing, respectively. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at StandardFusion, to achieve StandardFusion's service commitments and system requirements based on the applicable trust services criteria of security, availability, and confidentiality. The description presents StandardFusion's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of StandardFusion's controls. The description does not disclose the actual controls at the subservice organization. The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at StandardFusion, to achieve StandardFusion's service commitments and system requirements based on the applicable trust services criteria. The description presents StandardFusion's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of StandardFusion's controls.

We confirm, to the best of our knowledge and belief, that:

a. The description presents StandardFusion's system that was designed and implemented throughout the period of January 1, 2023 to December 31, 2023, in accordance with the description criteria.

   i. The description contains the following information:

      (1) The types of services provided.

      (2) The components of the system used to provide the services, which are the following:

      - *Infrastructure* – The physical and hardware components of a system (facilities, equipment, and networks).
      - *Software* – The programs and operating software of a system (systems, applications, and utilities).
      - *People* – The personnel involved in the operation and use of a system (developers, operators, users, and managers).
      - *Procedures* – The automated and manual procedures involved in the operation of a system.
      - *Data* – The information used and supported by a system (transaction streams, files, databases, and tables).

      (3) The boundaries or aspects of the system covered by the description.

(4) How the system captures and addresses significant events and conditions.

(5) The process used to prepare and deliver reports and other information to user entities and other parties.

(6) If information is provided to, or received from, subservice organizations or other parties, how such information is provided or received; the role of the subservice organization and other parties; and the procedures performed to determine that such information and its processing, maintenance, and storage are subject to appropriate controls.

(7) For each category being reported on, the applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, complementary user-entity controls contemplated in the design of the Company's system.

(8) For subservice organizations presented using the carve-out method, the nature of the services provided by the subservice organization; each of the applicable trust services criteria that are intended to be met by controls at the subservice organization, alone or in combination with controls at the Company, and the types of controls expected to be implemented at carved-out subservice organizations to meet those criteria; and for privacy, the types of activities that the subservice organization would need to perform to comply with privacy commitments.

(9) Any applicable trust services criteria that are not addressed by a control at the Company or a subservice organization and the reasons, therefore.

(10) Other aspects of the Company's control environment, risk assessment process, information and communication systems, and monitoring of controls that are relevant to the services provided and the applicable trust services criteria.

(11) Relevant details of changes to the Company's system during the period covered by the description.

ii. The description does not omit or distort information relevant to the Company's system while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs.

b. The controls stated in the description were suitably designed throughout the period January 1, 2023 to December 31, 2023, to provide reasonable assurance that StandardFusion's commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of StandardFusion's controls throughout that period.

c. The controls stated in the description operated effectively throughout the period January 1, 2023 to December 31, 2023, to provide reasonable assurance that StandardFusion'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 StandardFusion's controls operated effectively throughout that period.

By: /S/ Paul Guenette

Paul Guenette
Chief Technology Officer

January 26, 2024

DESCRIPTION OF STANDARDFUSION'S SOFTWARE-AS-A-SERVICE GRC PLATFORM SYSTEM

Company Overview

StandardFusion offers a governance, risk, and compliance (GRC) platform to help Organizations manage risk, compliance, audits, policies, and other workloads. StandardFusion's vision is to help companies simplify the complexities of GRC by providing a unified SaaS solution to manage processes, assessments, and make compliance operations more scalable.

The platform was built to solve three core challenges:

i. eliminate high costs of implementation and operations;
ii. add value to the bottom line by reducing risk and disruption, and;
iii. reduce complexity wherever possible through technology and automation.

StandardFusion is a privately held organization headquartered in Vancouver.

Products and Services Overview

The platform offers the possibility of seamless Risk and Compliance management, as a single pane of glass. The following features/modules are included in StandardFusion GRC:

- Risk Management
- Compliance Management
- Controls Assessments
- Vendor Management
- Audit Management
- Policy Management
- among others

The GRC platform is offered as both a cloud-based and on-premise solution and it enables customers to manage their compliance programs (in different areas, such as Information Security, Privacy, ESG, Finance) efficiently and effectively, all in one place.

System Description

Principal Services Commitments and System Requirements

StandardFusion's service commitment is to provide information security and compliance services in a secure and reliable manner. StandardFusion has designed and implemented policies and procedures to support its security directive for the GRC platform and its control environment. These documents are communicated internally to employees and external service providers.

Service commitments are documented and communicated to customers in the Terms of Service posted on the StandardFusion Website, and to applicable vendors via service level agreements and contracts.

Components of the System

StandardFusion's control environment (the "System") is comprised of the following components:

- Infrastructure (corporate office, workstations, and cloud hosting)
- Software (cloud-based solutions and applications)

- People (developers, users, and managers)
- Controls, Policies, and Procedures (manual and automated)
- Data (transaction streams, files, databases, and tables)

The company's environment and platform are designed and managed with security, availability, and confidentiality in mind. The following sections of this description define each of these five components comprising the System.

Infrastructure

StandardFusion uses Amazon Web Services ("AWS") and Microsoft Azure ("Azure") for its cloud-based hosting infrastructure. The production network that contains customer data and the StandardFusion proprietary software provided to customers is hosted in AWS data centers in multiple regions around the world, including Canada, United States, Australia, and Germany. For each AWS region, the data is replicated at the relevant Microsoft Azure data centers. Microsoft Azure operates as the disaster recovery environment for backups of customer data and key procedures to enact when backup protocols are required. When subscribing to the StandardFusion services, customers can select which region they would like their data to reside. For both the primary (AWS) and secondary (Azure) data centers, the data remains in the geographic location specified by the customers during the onboarding process. Each customer dataset is logically segregated in their own database and encrypted.

StandardFusion also offers an on-premise solution for its customers. The customer is provided with code to install on their own network and to operate internally with their environment. For this type of scenario, StandardFusion will provide support and guidance with the solution, however the customer is fully responsible for the security, availability, and confidentiality of their own data. On-premise solutions are excluded from scope in this audit.

Within AWS, StandardFusion also has non-production environments which are used for the development of new features for the platform (test environment) and demonstration of the platform's functionality (demo environment). Both these platforms are similar to the production environment, but they do not contain any customer data. Only fabricated and fictious data is used for the purposes of code development and platform demonstration purposes for the non-production environments.

The StandardFusion environment operates predominantly in the cloud. With the exception of company-issued workstations, there are no on-premise equipment or servers used for its daily operations or provision of services to customers.

Software/Systems

Software utilized to manage and support the StandardFusion IT environment includes:

- Backup and disaster recovery management
- Network and performance logging and monitoring
- Security detection and endpoint protection of workstations and servers
- GRC platform built-in audit logging
- Change management and software development
- Customer and help desk support
- Corporate user account management
- Internal document repository
- Human Resources management system

People and Organizational Structure

StandardFusion has an experienced Management team to govern all activities of the organization, ranging from development of its strategy to leading operating activities to achieve its business objectives. Management meets on a recurring basis with the functional departments to ensure that initiatives are proactively discussed and aligned with the business direction.

Teams are structured to ensure the highest level of integrity, competence, segregation of duties, and operational efficiency in the provision of services to customers. The organizational chart defines all reporting lines and authorities. The organizational chart is reviewed and updated at least annually to reflect changing business commitments and requirements.

StandardFusion is comprised of the following functional areas: Customer Success, Development, Hosting, Operations, Sales and Marketing, and Professional Services.

Segregation of duties is critical to an effective internal control environment, by reducing the risk of inappropriate or conflicting actions. StandardFusion has established and implemented clear segregation for key roles in accordance with the principle of least privilege.

Policies and Procedures

StandardFusion has designed and implemented formal policies, procedures, and runbooks to support its business operations and security commitments. These policies are reviewed and approved by Management at least annually, and when there are changes made to the policies.

The following is a select list of information security policies implemented by StandardFusion:

- Access Management
- Backup and Recovery
- Business Continuity and Disaster Recovery
- Change Management and Software Development Lifecycle
- Configuration Management
- Cryptography Management
- Data Loss Prevention, Retention and Destruction
- Device Management and Bring Your Own Devices (BYOD)
- Human Resources Security
- Incident Response Management
- Information Classification and Handling
- Logging and Monitoring
- Network Security
- Password Protection
- Physical and Environmental Security
- Removable Media
- Risk Management
- Third Party Management
- Vulnerability Management

These policies are communicated to employees and accessible via the StandardFusion platform.

Data

Customer data is logically segregated within the production environment. Access to customer data is restricted to authorized personnel who provide management and support services, and in accordance with StandardFusion's security policies. The Hosting team is responsible for the overall availability of the data, including system and data backups, monitoring of data processing, and resolving issues identified.

Disclosures

For the period under review, there were no significant security incidents with respect to the security of the platform or control environment. There were no material changes committed during the period that were within the boundaries of the System Description.