Report on Fanplayr's eCommerce Optimization System Relevant to Security, Availability, and Confidentiality Throughout the Period February 1, 2020 to January 31, 2021

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

940 Main Street | Louisville, CO 80027 | 303-665-8060 | info@kfinancial.com | www.kfinancial.com

TABLE OF CONTENTS

SECTION 1

INDEPENDENT SERVICE AUDITOR'S REPORT

940 Main Street
Louisville, CO 80027
tel 303.665.8060 fax 303.665.0813
www.kfinancial.com

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Fanplayr

Scope

We have examined Fanplayr's accompanying assertion titled "Assertion of Fanplayr Management" (assertion) that the controls within Fanplayr's eCommerce Optimization System (system) were effective throughout the period February 1, 2020 to January 31, 2021, to provide reasonable assurance that Fanplayr's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (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)*.

Service Organization's Responsibilities

Fanplayr 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 Fanplayr's service commitments and system requirements were achieved. Fanplayr has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Fanplayr 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 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 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.

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 Fanplayr'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 Fanplayr'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 Fanplayr's eCommerce Optimization System were effective throughout the period February 1, 2020 to January 31, 2021, to provide reasonable assurance that Fanplayr's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

K Financial

Louisville, Colorado
March 4, 2021

SECTION 2

ASSERTION OF FANPLAYR MANAGEMENT

Assertion of Fanplayr Management

We are responsible for designing, implementing, operating and maintaining effective controls within Fanplayr's eCommerce Optimization System (system) throughout the period February 1, 2020 to January 31, 2021, to provide reasonable assurance that Fanplayr's service commitments and system requirements relevant to security, availability, and confidentiality were achieved. Our description of the boundaries of the system is presented in attachment A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period February 1, 2020 to January 31, 2021, to provide reasonable assurance that Fanplayr's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (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)*. Fanplayr'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 February 1, 2020 to January 31, 2021 to provide reasonable assurance that Fanplayr's service commitments and system requirements were achieved based on the applicable trust services criteria.

Rajiv Sunkara
CTO / Founder
Fanplayr

ATTACHMENT A

FANPLAYR'S DESCRIPTION OF THE BOUNDARIES OF ITS ECOMMERCE OPTIMIZATION SYSTEM

TYPE OF SERVICES PROVIDED

Fanplayr ("the Company") provides a SaaS service to help business websites optimize and improve their conversion rate, average order value and revenue. This is done by gathering browsing information about anonymous users, identifying behavioral patterns and segments, targeting the users using visual components and offers, making product recommendations, and connecting with users through the use of mechanisms such as Web Push Notifications, SMS and emails. Fanplayr works with business websites in verticals such as retail eCommerce, travel, automotive manufacture, telecom, energy, insurance, banking, B2B and others.

THE COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICES

The boundaries of the 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 system.

The components that directly support the services provided to customers are as follows:

Infrastructure

The Company utilizes cloud services offered by third party providers to support the overall IT environment.

Software

The Company utilizes the following application programs and IT system software:

- Fanplayr Behavioral Personalization Services Portal and Runtime
  - This is the Fanplayr service provided to customers as an external-facing web application.
- A document management system is used by Fanplayr to maintain and track all relevant digital assets pertaining to operations, customers and sales.
- Internal Reporting application
  - This is a web based application that is used for internal reporting and access to various internal metrics.
- A third party system is used for security on the local network in the office and device endpoint protection.

People

The personnel involved in the governance, management, operation and security of the system include:

- Engineering
  - The engineering personnel are responsible for the building, maintenance, operation and security of the systems.
  - The roles are segregated to avoid conflicts.
- Executive management
  - Responsible for overseeing Company-wide activities, establishing and accomplishing goals, overseeing objectives and supporting Fanplayr's culture of compliance externally and internally.

- Human resources
  - Responsible for onboarding new personnel, defining role/position of new hires, performing background checks and facilitating the employee termination process.

Procedures

Fanplayr has the following security policies and procedures in place:

- Policy management and communication - policies are maintained by the CTO and communicated via annual training. The information security policies are hosted in an area available to all employees.
- Operations security – the Company has established procedures on the proper management of IT production, including change management, backup, logging, monitoring, installation, and vulnerabilities.
- Enterprise change management - changes to the architecture and the configuration of servers is managed by the IT team and overseen by the Change Advisory Board.
- Incident / problem management – the Company has established incident management procedures including reporting events and weaknesses, defining responsibilities, and response procedures.
- Backup and offsite storage - regular backups are routinely carried out to ensure that the Company can recover from unforeseen events, system failure, accidental or deliberate loss of information or facilities.
- System development - a systems development life cycle (SDLC) is in place. SDLC is a process that governs the development, acquisition, implementation, changes and maintenance of computerized information systems and related technology requirements.

Data

Secure data transmission protocols are used to encrypt confidential and sensitive data when it is transmitted over public networks. A data classification policy is in place to help ensure that confidential data is properly secured and restricted to authorized personnel.

User data stored on the Fanplayr System is classified in the following categories according to their respective definitions:

- Public – Information being public cannot harm the organization in any way.
- Internal Use – Unauthorized access to information may cause minor damage and/or inconvenience to the organization.
- Restricted – Unauthorized access to information may considerably damage to the business and/or reputation.
- Confidential – Unauthorized access to information may cause catastrophic (irreparable) damage to the business and/or reputation.

SUBSERVICE ORGANIZATIONS

The Company uses subservice organizations for data center colocation services. Fanplayr's controls related to the eCommerce Optimization System cover only a portion of the overall internal control for each user entity of the eCommerce Optimization System. The description does not extend to the services provided by the subservice organizations that provide colocation services for IT infrastructure.

Although the subservice organizations have been carved out for the purposes of this report, controls are expected to be in place at the subservice organizations related to physical security and environmental protection, as well as backup, recovery, and redundancy controls related to availability. The subservice organizations' physical security controls mitigate the risk of fires, power loss, climate, and temperature variabilities.

Management of the Company receives and reviews the subservice organizations' SOC 2 reports on an annual basis. In addition, through its operational activities, management of Fanplayr monitors the services performed by the subservice organizations to determine whether operations and controls expected to be implemented at the subservice organizations are functioning effectively. Management also has communication with the subservice organizations to monitor compliance with the service agreements, stay abreast of changes planned at the hosting facilities, and relay any issues or concerns to management of the subservice organizations.

ATTACHMENT B

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Principal Service Commitments

Commitments are communicated to customers in the Company's Media Services Agreements (MSAs) and online Privacy Policy. The Company's commitments include the following:

- Fanplayr shall develop, implement, maintain, and monitor a comprehensive security program that includes administrative, physical and technical safeguards and controls sufficient to ensure the security, confidentiality and integrity of data; including confidential information.
- Fanplayr shall keep confidential information secure and protected from any use, disclosure or access that is inconsistent with the service agreement.
- Fanplayr will support ongoing operations of the service on a continuous basis (7 days a week, 24 hours a day) using system resources provided by Fanplayr.
- Fanplayr will provide a reasonable response via phone or email from designated support staff members.
- Recipient shall not disclose Confidential Information to anyone except an employee, agent, affiliate, or third party who has a need to know same
- If Fanplayr learns of a security systems breach, then Fanplayr will undertake to notify users electronically through the contact information that user has provided in using the Services so that they can take appropriate protective steps.

Principal System Requirements

System requirements are specifications regarding how the Fanplayr System should function to meet the Company's commitments to user entities. Requirements are specified in the Company's policies and procedures, which are available to all employees. The Company's system requirements include the following:

- Employee provisioning and deprovisioning standards
- Logical access controls such as use of user IDs and passwords to access systems
- Protection of data in transit
- Risk assessment and risk mitigation standards
- System monitoring
- Change management procedures