HACKERBAY, INC. SOC 2 REPORT

FOR

FYIPE PLATFORM

A TYPE 2 INDEPENDENT SERVICE AUDITOR'S REPORT ON CONTROLS RELEVANT TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY

FOR THE PERIOD OF OCTOBER 1, 2018, TO SEPTEMBER 30, 2019

SES
COMPLIANCE AND ATTESTATION

Proprietary & Confidential

Reproduction or distribution in whole or in part without prior written consent is strictly prohibited.

This report is intended solely for use by the management of HackerBay, Inc., user entities of HackerBay, Inc.’s services, and other parties who have sufficient knowledge and understanding of HackerBay, Inc.’s services covered by this report (each referred to herein as a “specified user”).

If report recipient is not a specified user (herein referred to as a "non-specified user"), use of this report is the non-specified user's sole responsibility and at the non-specified user's sole and exclusive risk. Non-specified users may not rely on this report and do not acquire any rights against SES compliance and attestation as a result of such access. Further, SES Compliance and Attestation, SSS INC. does not assume any duties or obligations to any non-specified user who obtains this report and/or has access to it.

Unauthorized use, reproduction or distribution of this report, in whole or in part, is strictly prohibited.

TABLE OF CONTENTS

SECTION 1

INDEPENDENT SERVICE AUDITOR'S REPORT

To HackerBay, Inc.:

Scope

We have examined HackerBay, Inc.'s ("HackerBay or the service organization") accompanying description of its Fyipe Platform system, in Section 3, throughout the period October 1, 2018, to September 30, 2019, (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's System in a SOC 2 Report (AICPA, Description Criteria) ("description criteria") and the suitability of the design and operating effectiveness of controls stated in the description throughout the period October 1, 2018, to September 30, 2019, to provide reasonable assurance that HackerBay' 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, Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

HackerBay uses a subservice organization for cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at HackerBay, to achieve HackerBay' service commitments and system requirements based on the applicable trust services criteria. The description presents HackerBay' controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of HackerBay' controls. The description does not disclose the actual controls at the subservice organization. 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.

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

The information included in Section 5, "Other Information Provided by HackerBay" is presented by HackerBay management to provide additional information and is not a part of the description. Information about HackerBay' physical security processes has not been subjected to the procedures applied in the examination of the description, the suitability of the design of controls, and the operating effectiveness of the controls to achieve HackerBay' service commitments and system requirements based on the applicable trust services criteria.

Service Organization's Responsibilities

HackerBay 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 HackerBay' service commitments and system requirements were achieved. HackerBay has provided the accompanying assertion, in Section 2, ("assertion") about the description and the suitability of design and operating effectiveness of controls stated therein. HackerBay 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.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of 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 operated 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.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system and requirements;
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively;
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria;
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria;
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria; and
- Evaluating the overall presentation of the description.

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

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 the policies or procedures may deteriorate.

Description of Test of Controls

The specific controls we tested and the nature, timing, and results of those tests are presented in section 4 of our report titled "Testing Matrices."

Opinion

In our opinion, in all material respects,

a. the description presents HackerBay' Fyipe system that was designed and implemented throughout the period October 1, 2018, to September 30, 2019, in accordance with the description criteria;
b. the controls stated in the description were suitably designed throughout the period October 1, 2018, to September 30, 2019, to provide reasonable assurance that HackerBay' service 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 the user entities applied the complementary controls assumed in the design of HackerBay' controls throughout that period;
c. the controls stated in the description operated effectively throughout the period October 1, 2018, to September 30, 2019, to provide reasonable assurance that HackerBay' service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and user entity controls assumed in the design of HackerBay' controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in section 4, is intended solely for the information and use of HackerBay, user entities of HackerBay Fyipe Platform system during some or all of the period October 1, 2018, to September 30, 2019, business partners of HackerBay subject to risks arising from interactions with the Fyipe system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization; How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties;
- Internal control and its limitations;
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements;
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services;
- The applicable trust services criteria; and The risks that may threaten the achievement of the service organization's service commitments and system requirements, and how controls address those risks.

This report is not intended to be, and should not be used by anyone other than these specified parties.

SCS ATTESTATION AND
COMPLIANCE,
SCS INC.

New York City, New York. October 28, 2019

SECTION 2

MANAGEMENT'S ASSERTION

We have prepared the accompanying description of HackerBay' Fyipe system, in Section 3, throughout the period October 1, 2018, to September 30, 2019, (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's System in a SOC 2® Report (AICPA, Description Criteria), ("description criteria"). The description is intended to provide report users with information about the Fyipe system that may be useful when assessing the risks arising from interactions with HackerBay' system, particularly information about system controls that HackerBay 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 ("applicable trust services criteria") set forth in TSP section 100, Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

HackerBay uses a subservice organization for cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at HackerBay, to achieve HackerBay' service commitments and system requirements based on the applicable trust services criteria. The description presents HackerBay' controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of HackerBay' 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 HackerBay, to achieve HackerBay' service commitments and system requirements based on the applicable trust services criteria. The description presents HackerBay' controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of HackerBay' controls.

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

- the description presents HackerBay' Fyipe system that was designed and implemented throughout the period October 1, 2018, to September 30, 2019, in accordance with the description criteria;
- the controls stated in the description were suitably designed throughout the period October 1, 2018, to September 30, 2019, to provide reasonable assurance that HackerBay' service 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 organizations and the user entities applied the complementary controls assumed in the design of HackerBay' controls throughout that period;
- and the controls stated in the description operated effectively throughout the period October 1, 2018, to September 30, 2019, to provide reasonable assurance that HackerBay' service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls and user entity controls assumed in the design of HackerBay' controls operated effectively throughout that period.

SECTION 3

DESCRIPTION OF THE SYSTEM

Company Background and Description of Services Provided

Since 2014, HackerBay Inc. (“HackerBay” or the “Company”) has provided a monitoring and oncall hub called “Fyipe” (the “System”) to businesses and organizations (“user entities”), designed to allow site reliability teams monitor their software.

With Fyipe, users join a secure instance called a “Project” (“Fyipe Project”) where members add resources (like software, website, web service and more) they would like to monitor. Fyipe monitors those resources and alerts members when resources do not behave the way they should.

Fyipe integrates with a large number of third-party services and supports community-built integrations. Fyipe provides mobile apps for iOS and Android, in addition to their web browser client and electron desktop clients for macOS, Windows, and Linux. Fyipe has been used for organizational communication, as well as a community platform.

Additional detail is posted on the Company’s website and made available to internal and external users.

Principal Service Commitments and System Requirements

Fyipe makes the following security, availability, and confidentiality commitments to their customers:

- Fyipe will make the services available 99.99% of the time, except for maintenance or as otherwise provided in service level agreement (SLA) described in the service contract;
- Production cloud infrastructure hosted within multiple geographically diverse availability zones/regions;
- Encrypt data in transmission using transport layer security (TLS) or other technologies over public networks;
- Maintain commercially reasonable administrative, technical, organizational, and physical measures to protect the security of customer data against anticipated threats or hazards;
- Confidential data stored within the production services utilize advanced encryption standard (AES) encryption;
- Confidential data stored within the production services is retained per customer defined retention policies; and
- Disaster recovery plans are in place and tested at least once per year.

Fyipe has put into place a set of policies and procedures, inclusive of technology-based controls and automation, to help ensure that security, availability, and confidentiality commitments are met.

Fyipe’s commitments to security, availability, and confidentiality are described in the standard service agreement contracts for contracted customers. Customers are required to sign the Terms of Service agreement prior to receiving Fyipe’s services. These agreements describe the technical and organizational controls that Fyipe is responsible for maintaining for their customers.

Components of the System Used to Provide the Service

System Boundaries

The system is designed, implemented, and operated to achieve specific business objectives in accordance with management-specified requirements. The purpose of the system description is to

delineate the boundaries of the system, which includes the services outlined above and the five components described below: infrastructure, software, people, procedures, and data.

Infrastructure

The System production environment is hosted by infrastructure subprocessors. The Company maintains the list of current subprocessors here: https://Fyipe.com/legal/subprocessors, which included Amazon Web Services (“AWS”) among others during the period covered by this report. Development occurs on systems in environments that are separate from the production environment.

Customer data is processed by and stored in hosted infrastructure compute services (such as AWS Elastic Compute Cloud (EC2) instances and hosted infrastructure storage services (such as AWS Simple Storage Service (S3). AWS S3 is also utilized to store backup copies of customer data. AWS Simple E-mail Service (SES) is also utilized to send and receive e-mail-based communication with users.

Software

The System is implemented using Linux, Apache, NodeJS (NodeJS), and MongoDB technologies with well- understood performance, scalability, and security properties. The System’s real-time service is implemented in NodeJS using the WebSocket protocol.

People

The Company’s control environment is implemented, maintained, and supported by Service Engineering, Security, Customer Experience, People Operations (“People Ops”), Information Technology (“IT”), Quality Assurance (“QA”), Legal, Product Development, and Executive Management. All of the Company’s personnel are recruited and managed according to policies and procedures which are described in the Summary of Control Activities section below.

Processes

Formal policies and procedures codify the principles and requirements ensuring the security, availability, and confidentiality of the System. All personnel are required to adhere to the Company’s policies and procedures, which are located on the Company’s intranet and can be accessed by any Company personnel. These processes are detailed further in the *Summary of Control Activities* section below.

Data

The following table describes the information used and supported by the system.

Data Used and Supported by the System		
Data Description	**Data Reporting**	**Classification**
Customer data	Data provided by customer’s in their designated workspaces	Confidential and private to the customer

The System stores and processes all information provided by user entities without inspection; all such information is maintained as confidential and private to that user entity. This confidential and private information is available only to members of the user entity’s Fyipe Project. Each user entity has designated administrators who authorize member access to information stored in their Fyipe Project.

As described in Summary of Control Activities, access to customer data by Company personnel is restricted to authorized personnel. All other access to customer data by Company personnel requires management authorization or explicit approval from the user entity.

Subservice Organizations (Subprocessors)

The cloud hosting services provided by AWS are not included within the scope of this examination. See the Complementary Subservice Organization Controls section below for more details.

Relevant Aspects of Internal Control

As defined by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), internal control is a process affected by an entity's board of directors, management, and other personnel, and consists of the following five interrelated elements:

- **Control Environment** – Sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other internal control components by providing discipline and structure.
- **Risk Management** – The entity's identification and analysis of relevant risks to the achievement of its objectives, forming a basis for determining how the risks should be managed.
- **Information and Communication** – Surrounding these activities are information and communication systems. These enable the entity's people to capture and exchange information needed to conduct and control its operations.
- **Related Control Activities** – Control policies and procedures must be established and executed to help ensure that the actions identified by management as necessary to address risks to the achievement of the entity's control objectives are effectively carried out.
- **Monitoring** – The entire process must be monitored, and modifications made as necessary. In this way, the system can react dynamically, changing as conditions warrant.

Control Environment

The control environment at Fyipe is the foundation for the other areas of internal control. It sets the tone of the organization and influences the control consciousness of its personnel. The components of the control environment factors include the integrity and ethical values, management's commitment to competence; its organizational structure; the assignment of authority and responsibility; and the oversight and direction provided by the board of directors and operations management.

The Company's management philosophy and operating style is consistent with a sound control environment and encompasses a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks and management's attitudes toward information processing, accounting functions, and personnel (employees and contractors). The Company's management style fosters open communication among all personnel. The executive management and senior leadership are committed to reinforcing the core values for all personnel. Management has documented information security policies, which are communicated to all Company personnel. Roles and responsibilities relevant to Fyipe's control environment are documented.

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of Fyipe's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Fyipe's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards through policy statements and codes of conduct.

Board of Directors and Audit Committee Oversight

The Company's controls are influenced significantly by its senior executive management team. Attributes that define the entity's "tone at the top" are established by executive management to the extent of its involvement and scrutiny of activities, the appropriateness of its actions, the degree to which difficult questions are raised and pursued with management. The senior executive management team meets on a periodic basis to oversee operations management activities and to discuss and monitor related issues.

Organizational Structure and Assignment of Authority and Responsibility

Fyipe's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Fyipe's management believes that establishing a relevant organizational structure includes considering key areas of authority and responsibility and applicable lines of reporting. Fyipe has developed an organizational structure suited to its needs. This organizational structure is based, in part, on its size and the nature of its activities. Organizational charts are in place to communicate key areas of authority, responsibility, and applicable lines of reporting to personnel. These charts are communicated to employees and updated in real time and can be viewed through the human resources portal.

Commitment to Competence

Fyipe's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Fyipe's commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into requisite skills and knowledge. Management has considered the competence levels for jobs and translated required skills and knowledge levels into written position requirements.

Accountability

Fyipe's management philosophy and operating style encompasses a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks; and management's attitudes toward information processing, accounting functions and personnel. Specific control activities that Fyipe has implemented in this area are described below.

- Management is periodically briefed on regulatory and industry changes affecting services provided.
- Management meetings are held on a periodic basis to discuss operational issues.

Fyipe's human resources (HR) policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities. Specific control activities that Fyipe has implemented in this area are described below:

- Documented pre-hire screening procedures are in place to guide HR personnel during the hiring process.
- Formal termination procedures are in place to guide HR personnel during the termination process.
- Certain departments are notified upon employee terminations to help ensure that the respective user system accounts are disabled or revoked.
- A termination checklist is completed as a component of the termination process.

Risk Assessment

The Company has defined a risk management framework. Management identifies risks in their respective areas of responsibility, assesses the severity of those risks, and implements appropriate and timely solutions to address those risks. The risk management framework, identifiable risks, and appropriate mitigation strategies are assessed on an annual basis to ensure changes to the control environment are considered. Ongoing monitoring procedures are built into the Company's internal controls to ensure risks are consistently managed.

RELATED CONTROL ACTIVITIES

Control activities are designed to address the risks identified by management's assessment of security risk and include both detective and preventive control activities. Detailed descriptions of Control Activities are in the following Summary of Control Activities section. The control activities follow policies and procedures that instruct employees and contractors in their day-to-day security program-related responsibilities. The Company policies address: Acceptable Use, Access Control, Asset Management, Authorized Devices, Business Continuity Response and Recovery, Change Control, Data Encryption, Incident Response, Information Classification, Information Labeling & Handling, Infrastructure Security, Malicious Code Prevention, People Ops, Records Retention, Security Assessments, System Audit and Monitoring, Systems Development Lifecycle, Third-Party Relationships, and Vulnerability Management.

The Chief Security Officer ("CSO") annually reviews and updates the Company's security policy and associated controls and ensures compliance across the Company.

The People Ops department has a standard process for onboarding new hires. All personnel are required to have a background check performed before they are hired and are screened in the hiring process for appropriate job qualifications according to written job descriptions. New hires are required to read and acknowledge security policies, confidentiality agreement and code of conduct as part of the week-long onboarding period.

The Company obtains confidentiality commitments that are consistent with the Company's confidentiality requirements from vendors and other third parties whose products and services comprise part of the System or have access to confidential information.

Trust Services Criteria Not Applicable to the In-Scope System

All criteria within the security, availability, and confidentiality are applicable to the Fyipe system.

Summary of Control Activities

The Company's detailed description of related control activities is included in Section 4 in order to eliminate the redundancy that would result from listing them in two sections. Although the related control activities are listed in Section 4, they are, nevertheless, an integral part of the Company's description of the System as presented herein. The controls and procedures implemented by the Company to ensure the security, availability, and confidentiality of the System are described in the Information Security Policy and summarized below.

Physical Security

Subprocessors hosting Fyipe's production infrastructure ('hosting providers') manage the physical security of the facilities that host the development and production environments. Each hosting provider's SOC 2 report details the security measures in place; the Company's management reviews these reports annually. Further, physical security is enforced at the Company's corporate office. Personnel are required to show proof of identity to enter the office building and entrances to the office are locked and required authorized badge for entry after close of business.

Device and Network Security

Devices issued to Company personnel must meet minimum security criteria that include being locked when unattended, employing full-disk encryption, and being kept up-to-date with security patches from the operating system vendor. Company laptops and workstations running Windows, Mac OS, or Linux are required to run antivirus software with up-to-date virus definitions.

Development and production servers are configured to a baseline via configuration management tools, such as Chef, and to automatically apply security patches made available by the operating

system vendor daily. Office networks grant no elevated access to the development or production environments. The development and production environments use firewalls and multi-factor authentication to isolate themselves from the Internet. Additional security measures are undertaken in accordance with the risk management program described above. Vulnerability management, automated scanning, penetration tests, a 'bug bounty' program, restrictive firewalls, and strong encryption of data transmitted over the public Internet are among the security measures employed by the Company.

Access to Internal Systems

Access to internal systems, including web-based tools and the development and production environments, is granted based upon job responsibilities, and revoked upon termination. Access to the System production environment and source code is reviewed quarterly by management.

Company personnel must pass background checks before starting work and attend security training during the onboarding period and annually thereafter.

Two-factor authentication is required to access the production environment, source code, hosting provider interfaces, the Company's internal administrative website, and the System itself.

Access to User Data

Access to sensitive customer data is restricted to Service Engineering personnel with credentials to access such data. All access by non-Service Engineering personnel requires management authorization or explicit customer approval. Company personnel are not authorized to store customer data on laptops, phones, universal serial bus (USB) drives, or any other device or portable media outside of the Company's data center. Instead, non-sensitive user data is accessed via web-based tools. Access to these tools is managed centrally and may be revoked at any time.

Change Management

Code changes are tested in the development environment, committed to a source code management system that logs all changes in perpetuity, and reviewed through automated testing or by peers. Major releases are tested by QA before deployment.

Incident Response

An incident response plan defines roles, responsibilities, escalation paths, and communication requirements in case of incidents that affect the security, availability, or confidentiality of the System. Incidents impacting availability are communicated externally via https://status.Fyipe.com. Incidents impacting security and confidentiality of customer data are communicated to the impacted customers as per the Terms of Services ("ToS"), pertinent contractual obligations, and Security policies published on the Company's website.

Disaster Recovery and Data Backup

The Company values reliability and simplicity in its infrastructure. The System is hosted in multiple availability zones. Availability zones are designed to fail independently, thus allowing the System to remain available when any single availability zone fails.

Additionally, at least every 90 days, the Company practices recovery from backup, as would occur in the case of a complete failure and a requirement to move the System to a different region altogether.

INFORMATION AND COMMUNICATION SYSTEMS

Internal Communications

Various methods of communication are made available internally to Company personnel to ensure awareness of individual roles and responsibilities and to communicate significant events in a timely manner. New hire onboarding includes a review and acceptance of the information security policy covering the security, availability, and confidentiality of the System, in addition to a review of functional procedures according to employee roles and responsibilities.

The Company utilizes the System to communicate with all of its personnel worldwide. The System allows management and the Security Department to provide timely updates to the entire Company, to announce new policies, and to notify when changes are made. Personnel similarly acknowledge receipt and acceptance of policies.

External Communications

External communication is primarily through the Company's website and the System. User entities can check on the status of the System at https://status.Fyipe.com or https://twitter.com/FyipeStatus.

In addition, the Company has implemented various help features for external users to report incidents within the System. User entities can contact the Company's Customer Experience Department through the Company website or the System to submit inquiries and report system issues. Such inquiries are tracked in a ticketing system to ensure resolution.

MONITORING

Company management performs monitoring activities designed to ensure the effectiveness of the control environment and implements corrective actions to address deviations from its documented policies. At least annually, the Company's Risk and Compliance Department evaluates the design and operating effectiveness of controls to ensure compliance with System requirements and commitments. Remediation actions relating to identified deficiencies are tracked to resolution.

Additional monitoring of controls, as defined in the System's environment, include quarterly audits of access to the production environment and source code.

Ongoing Monitoring

The Service Engineering Department continuously monitors the health of the System from internal and external points to ensure the Company's availability and capacity and is alerted immediately when problems are detected. Members of the Security and Service Engineering departments are on-call 24 hours a day, 7 days a week (24/7) to respond to security and confidentiality, or availability issues, respectively. Incidents are documented and discussed after being resolved in order to improve the Company's response to incidents that affect the security, availability, or confidentiality of the System.

The Company engages third-party organizations to perform penetration tests and other analyses that regularly test the security of the System and identify exploitable vulnerabilities. The Company maintains a 'bug bounty' program that encourages other parties to submit reports of potential vulnerabilities to the System's security.

Separate Evaluations

The Company has implemented a self-assessment program to evaluate the performance of specific control activities and processes over time and confirm that the in-scope controls were consistently applied as designed and operating effectively.

Based on the nature of the controls and the frequency of the application processes (e.g. real time, daily, weekly, quarterly, etc.), self-assessment methodology was communicated to management, including structured inquiry, observation, inspection, or sample testing, or a combination of the

aforementioned. To ensure independence, self-assessment is performed by a competent individual different from the individuals that implemented the controls.

The nature, timing and extent of the self-assessment tests and results are documented, tracked, and communicated to management and the control owners. Senior executive management team reviews the deviations and corrective actions during periodic meetings.

Subservice Organization Monitoring

The Company performs annual reviews of subservice organization independent assessor's report(s) or security questionnaire(s) to evaluate the security, availability, and confidentiality controls relevant to the Company's commitments.

Evaluating and Communicating Deficiencies

The nature, timing and extent of the self-assessment tests and results are documented by the self-assessors in an internal tracking tool, for management review. Deviations or deficiencies associated with controls with a level High risk assignment are immediately escalated to management for immediate corrective action. Other self- assessment results are reviewed within a week of the self-assessment test procedures, and corrective action, if required, is assigned to an individual and documented once those required actions are complete. Management reviews the deviations and corrective actions during the quarterly risk assessment meeting.

COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS ("CSOCS")

The Company utilizes the following one (1) service organizations ("subservice organizations") to implement portions of the System: 1) AWS

AWS

The Company utilizes services from AWS, such as EC2 for infrastructure hosting and S3 for data storage and AWS SES to send and receive e-mail-based communication with users. AWS is responsible for operating, managing, and controlling the components from the host operating system and virtualization layer and storage, down to the physical security and environmental controls over the facilities in which the services operate. AWS is examined annually in accordance with the *AICPA Guide, Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy (SOC 2®). T*his description includes only the controls of the System and does not include any of the controls expected to be implemented at AWS.

It is expected that AWS has implemented the following types of controls to support achievement of the associated criteria:

Applicable Trust Services Criteria

CC3.2, CC3.3

Procedures are established and implemented to identify, analyze, and remediate potential security, availability, and confidentiality threats and/or risks.

CC4.1, CC4.2

Procedures are established and implemented to evaluate the designs and operating effectiveness of controls as they relate to security, availability, and/or confidentiality commitments, as well as to identify and track to resolution the corrective actions for control deficiencies.

CC6.1

Logical security has been implemented to authenticate authorized users, restrict access, prevent, and detect unauthorized access.

CC6.1

The systems are configured to identify and authenticate internal and external users with appropriate valid credentials.

CC6.1

Security measures are implemented to prevent unauthorized disclosure, usage, and/or access to confidential information.

CC6.2

Procedures are implemented to provision and de-provision user access to systems and applications based on appropriate authorization.

CC6.3

Logical access to the software and physical access to the software hosting datacenter facilities are provisioned to authorized personnel and revoked upon termination or when access is no longer needed.

CC6.4, CC6.5,

Physical access to the datacenter facilities are restricted to authorized personnel.

CC6.6

Logical security measures have been implemented to protect and detect external threats.

CC6.7

Logical security measures have been implemented to protect and detect external threats. Logical security measures have been implemented to secure the transmission, movement, and removal of information, as well as restricting users with the ability to do so.

CC6.8

Antivirus and/or malware software have been implemented to prevent or detect the introduction of unauthorized or malicious software.

CC7.2

Vulnerability scans and penetration testing are performed periodically to identify vulnerabilities threatening the systems.

CC7.3, 7.4, 7.5

Incident Response Procedures are established and implemented to identify, analyze, and remediate potential security, availability, and confidentiality events and/or incidents.

CC8.1

SDLC has been established and implemented to ensure system changes are authorized, tested, and approved prior to production deployment. Policies and procedures for SDLC or infrastructure changes have been established and reviewed and are updated periodically.

CC8.1

Policies and procedures for SDLC or infrastructure changes have been established and reviewed and are updated periodically.

CC8.1

Procedures are established and implemented to ensure changes to systems are authorized, designed, developed, configured, documented, tested, and approved prior to production deployment.

CC8.1

Procedures are implemented to ensure confidential information is protected during systems change management processes.

CC9.2

Confidential information is only obtained in accordance with the defined commitments or agreements.

A1.1

Monitoring tools are implemented to monitor and manage the systems' capacity and availability.

A1.2

Environmental protections, data backup processes, recovery infrastructure, and monitoring and alarming mechanisms have been implemented to adequately address availability requirements. Business continuity/disaster recovery procedures are tested periodically.

A1.3

Business continuity/disaster recovery procedures are tested periodically.

COMPLEMENTARY CONTROLS AT USER ENTITIES

The Company’s services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the applicable trust criteria related to the Company’s services to be solely achieved by the Company’s control procedures. Accordingly, user entities, in conjunction with the Fyipe system and related services, should establish their own internal controls or procedures to complement those of the System.

The following complementary user entities controls should be implemented by user entities to provide additional assurance that the applicable trust criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities’ locations, user entities’ auditors should exercise judgment in selecting and reviewing these complementary user entity controls:

User entities are responsible for informing Fyipe of any regulatory issues that may affect the services provided by the System.

Common Criteria 6.1; Availability Criteria 1.2

User entities are responsible for understanding and complying with their contractual obligations to Fyipe.

Common Criteria 2.2, 2.3, 6.1; Availability Criteria 1.2

User entities are responsible for keeping the technical, billing, and administrative contact information on file with Fyipe up-to-date.

Common Criteria 2.2, 2.3

User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize the System.

Availability Criteria 1.2, 1.3

User entities are responsible for configuring the System security settings appropriately for the user entity.

Common Criteria 6.1, 6.3, 6.6

User entities are responsible for ensuring the confidentiality of any user accounts and passwords assigned to them for use with the System.

Common Criteria 6.1, 6.3, 6.6

User entities are responsible for inviting new users to sign up for an account in the System, as well as removing terminated user accounts from the System.

Common Criteria 6.1, 6.3, 6.6

User entities are responsible for ensuring that entity profile information stored by the System is accurate and complete.

Common Criteria 6.1,6.3, 6.6

User entities are responsible for immediately notifying Fyipe of any actual or suspected information security breaches, including compromised user accounts.

Common Criteria 7.3, 7.4, 7.5

User entities are responsible for ensuring the appropriateness of designated Fyipe Project owner(s) and administrator(s).

Common Criteria 6.1, 6.3, 6.6

User entities are responsible for providing accurate and complete contact information to Fyipe for end users to be provisioned.

Common Criteria 6.1, 6.3, 6.6

User entities are responsible for accepting the terms and agreement for utilizing Fyipe's services.

Common Criteria 2.2, 2.3

User entities are responsible for monitoring and enforcing organizational compliance to Fyipe's terms and agreements.

Common Criteria 2.2,2.3

User entities are responsible for configuring the message retention settings appropriately for the organization.

Common Criteria 6.1; Confidentiality Criteria 1.1, 1.2

User entities are responsible for developing and implementing their own information classification policies to govern sharing Personally Identifiable Information ("PII") and other sensitive data in the System.

Common Criteria 6.1, 8.1

FYIPE'S CONTROLS MAPPING TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY CATEGORY CRITERIA

Trust Services Category Criteria No.	Criteria Common to Security, Availability, and Confidentiality Categories	Fyipe's Control No(s). (See Section 4)
Control Environment		
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	1.01, 1.02, 1.03, 1.04, 1.05, 1.06, 1.07, 1.08
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	1.09, 1.10, 1.11
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	1.01, 1.02, 1.03
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	1.04, 1.05, 1.06, 2.02
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	1.01, 1.02, 1.03, 1.09, 1.10, 1.11

Communication and Information		
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	2.01, 2.02, 2.03, 2.04, 2.05, 2.06, 2.07, 5.01

CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	1.01, 1.03, 1.04, 1.06, 2.02, 2.03, 2.04, 2.05
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	2.01, 2.03, 2.04, 2.06, 2.07, 10.05

Common Criteria Related to Risk Management and Design and Implementation of Controls		
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	3.01, 3.02, 3.03, 3.04
CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	3.01, 3.02, 3.03
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	3.01
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	3.01, 3.04, 4.04, 10.05

Monitoring Activities		
CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	3.02, 3.03, 3.04, 4.01, 4.02, 4.03, 4.04, 5.01, 5.02
CC4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	1.10, 1.11, 5.01

Control Activities		
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	5.01, 5.02, 3.01
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	1.01, 1.03, 3.01, 5.01, 5.02

Logical and Physical Access Controls

CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	6.01, 6.02, 6.05, 7.03
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	1.08, 6.01, 6.02, 6.03, 6.05
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	1.08, 6.01, 6.02, 6.03, 6.04
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	6.08 Control Activity Expected to be Implemented by AWS
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	6.09
CC6.6	The entity implements logical access security measures to protect against threats from sources outside it's system boundaries.	3.02, 3.03, 4.02
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	6.06, 6.07, 6.10, 7.03
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	4.02, 6.02, 7.03, 7.04, 7.05, 7.06, 7.07, 7.08

Systems Operation		
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	3.02, 3.03, 4.02, 7.03

CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	3.02, 3.03, 4.02, 4.03
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	2.04, 4.02, 7.01, 7.02
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	2.04, 7.01, 7.02
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	2.04, 7.01, 7.02

Change Management		
CC8.1	The entity authorizes, designs, develops, or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	6.02, 6.04, 8.01, 8.02, 8.03, 8.04, 8.05, 10.01

Risk Mitigation		
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	3.01, 9.02
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	2.01, 3.04, 4.01

Additional Criteria for Availability		
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	2.03, 2.06, 4.03
A1.2	The entity authorizes, designs, develops, or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	9.01, 9.02, 9.03, 9.05
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	9.03, 9.05

Additional Criteria for Confidentiality		
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	6.02, 6.07, 6.10, 9.04, 9.06, 10.01, 10.02, 10.03, 10.04, 10.05, 10.06
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	10.06, 10.07

SECTION 4

TESTINGMATRICES

TESTS OF OPERATING EFFECTIVENESS AND RESULTS OF TESTS

Scope of Testing

This report on the controls relates to the Fyipe system provided by Fyipe. The scope of the testing was restricted to the Fyipe system and its boundaries as defined in Section 3. SES conducted the examination testing over the period October 1, 2018, to September 30, 2019.

Tests of Operating Effectiveness

The tests applied to test the operating effectiveness of controls are listed alongside each of the respective control activities within the Testing Matrices. Such tests were considered necessary to evaluate whether the controls were sufficient to provide reasonable, but not absolute, assurance that the applicable trust services criteria were achieved during the review period. In selecting the tests of controls, SES considered various factors including, but not limited to, the following:

- The nature of the control and the frequency with which it operates;
- The control risk mitigated by the control;
- The effectiveness of entity-level controls, especially controls that monitor other controls;
- The degree to which the control relies on the effectiveness of other controls; and
- Whether the control is manually performed or automated.

The types of tests performed with respect to the operational effectiveness of the control activities detailed in this section are briefly described below:

Test Approach	Description
Inquiry	Inquired of relevant personnel with the requisite knowledge and experience regarding the performance and application of the related control activity. This included in-person interviews, telephone calls, e-mails, web-based conferences, or a combination of the preceding.
Observation	Observed the relevant processes or procedures during fieldwork. This included, but was not limited to, witnessing the performance of controls or evidence of control performance with relevant personnel, systems, or locations relevant to the performance of control policies and procedures.
Inspection	Inspected the relevant audit records. This included, but was not limited to, documents, system configurations and settings, or the existence of sampling attributes, such as signatures, approvals, or logged events. In some cases, inspection testing involved tracing events forward to consequent system documentation or processes (e.g. resolution, detailed documentation, alarms, etc.) or vouching backwards for prerequisite events (e.g. approvals, authorizations, etc.).

Sampling

Consistent with American Institute of Certified Public Accountants (AICPA) authoritative literature, SES utilizes professional judgment to consider the tolerable deviation rate, the expected deviation rate, the audit risk, the characteristics of the population, and other factors, in order to determine the number of items to be selected in a sample for a particular test. SES, in accordance with AICPA authoritative literature, selected samples in such a way that the samples were expected to be representative of the population. This included judgmental selection methods, where applicable, to ensure representative samples were obtained.

System-generated population listings were obtained whenever possible to ensure completeness prior to selecting samples. In some instances, full populations were tested in cases including but not limited to, the uniqueness of the event or low overall population size.

Reliability of Information Provided by the Service Organization

Observation and inspection procedures were performed related to certain system-generated reports, listings, and queries to assess the accuracy and completeness (reliability) of the information used in the performance of our testing of the controls.

Test Results

The results of each test applied are listed alongside each respective test applied within the Testing Matrices. Test results not deemed as control deviations are noted by the phrase “No exceptions noted.” in the test result column of the Testing Matrices. Any phrase other than the aforementioned, constitutes either a test result that is the result of non-occurrence, a change in the application of the control activity, or a deficiency in the operating effectiveness of the control activity. Testing deviations identified within the Testing Matrices are not necessarily weaknesses in the total system of controls, as this determination can only be made after consideration of controls in place at user entities and subservice organizations, if applicable, and other factors. Control considerations that should be implemented by user entities and subservice organizations, in order to complement the control activities and achieve the applicable trust services criteria are presented in the “Complementary Controls at User Entities” and “Subservice Organizations” sections, respectively, within Section 3.

SECURITY CATEGORY

Control #	Control Activity	Test Applied	Results
Control Environment			
1.01	Fyipe Technologies (the "Company") has a documented Information Security Policy that is communicated to Company personnel (employees and contractors). Roles and responsibilities are documented in the policy.	Inspected the information security policy and evidence of communication to determine that the Company had a documented Information Security Policy that was communicated to Company personnel (employees and contractors) and that roles and responsibilities were documented in the policy.	No exceptions noted.
1.02	Reporting lines and organizational structure are defined and made available to employees.	Inspected the organizational chart within the internal benefits system to determine that reporting lines and organizational structure were defined and made available to employees.	No exceptions noted.
1.03	The CSO or designee reviews and approves the Information Security Policy and other relevant security policies and standards at least annually and communicates material changes to personnel (employees and contractors).	Inspected the information security and other relevant security policies and standards and evidence of review to determine that the CSO or designee reviewed and approved the Information Security Policy and other relevant security policies and standards and communicated material changes to personnel (employees and contractors) during the review period.	No exceptions noted.
1.04	Job descriptions are defined and used as part of the hiring process to evaluate candidates and communicate job responsibilities.	Inspected the documented job descriptions for a sample of employment positions to determine that job descriptions	No exceptions noted.

		were defined and used as part of the hiring process to evaluate candidates and communicate job responsibilities for each employment position sampled.	
1.05	Background checks are completed for personnel (employees and contractors) prior to initiating employment.	Inspected the background checks for a sample of employees hired during the review period to determine that background checks were completed for personnel (employees and contractors) prior to initiating employment for each employee sampled.	No exceptions noted.
1.06	Company personnel (employees and contractors) are required to read and accept the Information Security Policy and Confidentiality Agreement during the onboarding period.	Inspected the information security policy and confidentiality agreement acknowledgement for a sample of employees hired during the review period to determine that company personnel (employees and contractors) were required to read and accept the Information Security Policy and Confidentiality Agreement during the onboarding period for each employee sampled.	No exceptions noted.
1.07	An Authorized Device Policy has been established and implemented. The policy addresses, but is not limited to, the following: • Acceptable uses for personal mobile devices (including phones, tablets, etc.) to access corporate apps and/or information Appropriate security measures required for accessing Company information via mobile devices	Inspected the authorized device policy to determine that an authorized device policy has been established and implemented and that the policy addressed the following: • Acceptable uses for personal mobile devices (including phones, tablets, etc.) to access corporate apps and/or information Appropriate security measures required for accessing Company information via mobile devices	No exceptions noted.
1.08	People Operations ("People Ops") team have established a termination checklist that is used for offboarding personnel. The checklist includes, but is not limited to, the following: • Collecting the Company assets (i.e. laptops, badges, mobile devices, etc.) • Communicate the continuation of information security responsibilities and duties that remained, as agreed per the contractual agreement signed, upon termination	Inspected the termination checklist for a sample of employees terminated during the review period to determine that People Ops have established a termination checklist that was used for offboarding personnel and that the checklist included the following for each terminated employee sampled: • Collecting the Company assets (i.e. laptops, badges, mobile devices, etc.) • Communicate the continuation of information security responsibilities and duties that remained, as	No exceptions noted.

		agreed per the contractual agreement signed, upon termination	
1.09	An Executive Risk Committee (("ERC") Charter has been established to define the responsibilities of the ERC members. The Charter is reviewed, updated if necessary, and approved on an annual basis and made available to relevant personnel.	Inspected the ERC charter to determine that an ERC charter had been established to define the responsibilities of the ERC members and that the charter was reviewed, updated if necessary, and approved and made available to relevant personnel during the review period.	No exceptions noted.
1.10	The ERC Committee meets on a quarterly basis to review and evaluate the following, but not limited to: • The alignment of the Company's policies and procedures with the established compliance frameworks • Any opportunities for improvements • The remediation and/or corrective actions taken on identified risks, findings, issues, etc. • Approve any subsequent changes made to the high- level information security policies • Resources and budget needs to implement, sustain, and continuously improve the information security and compliance frameworks	Inspected the ERC meeting minutes for a sample of quarters during the review period to determine that the ERC met on a quarterly basis to review and evaluate the following for each quarter sampled: • The alignment of the Company's policies and procedures with the established compliance frameworks • Any opportunities for improvements • The remediation and/or corrective actions taken on identified risks, findings, issues, etc. • Approve any subsequent changes made to the high- level information security policies • Resources and budget needs to implement, sustain, and continuously improve the information security and compliance frameworks	No exceptions noted.
1.11	A formal Audit Risk Committee (ARC) Charter has been established and approved by Fyipe's independent board of directors, which describes the committee members' responsibilities and oversight of management's system of internal control. On an annual basis, the board of directors meet with Fyipe's Executive Management to formally review the Company's internal control performance metrics and the results of the third-party assessment reports. Meeting minutes of the annual ARC meetings are tracked, documented, and maintained in formal meeting minutes.	Inspected the ARC Charter and the most recent committee meeting minutes during the review period to determine that a formal ARC Charter had been established and approved by Fyipe’s independent board of directors, which described the committee members’ responsibilities and oversight of management’s system of internal control, and that on an annual basis, the board of directors met with Fyipe’s Executive Management to formally review the Company’s internal control performance metrics and the results of the third-party	No exceptions noted.

		assessment reports, and that the meeting minutes of the annual ARC meetings were tracked, documented, and maintained in formal meeting minutes.	
Communication and Information			
2.01	A description of the Company's commitments to the security, availability, and confidentiality of the System are made available to the public via the Company's website and updated when necessary.	Inspected the company website and the signed customer contract for a sample of new customers during the review period to determine that a description of the Company's commitments to the security, availability, and confidentiality of the System were made available to the public via the Company's website and updated when necessary for each new customer sampled.	No exceptions noted.
2.02	Company personnel (employees and contractors) are required to complete security and privacy trainings during the onboarding period and annually thereafter.	Inspected the security and privacy training acknowledgements for a sample of current employees and employees hired during the review period to determine that company personnel (employees and contractors) completed security and privacy trainings during the onboarding period and annually thereafter for each employee sampled.	No exceptions noted.
2.03	The Company has implemented means for internal and external users to report incidents utilizing Fyipe's "help" feature. Tickets are automatically generated, and issues are tracked to resolution.	Inspected the incident reporting feature and an example incident ticket generated during the review period to determine that the Company implemented means for internal and external users to report incidents utilizing Fyipe's "help" feature and that tickets were automatically generated, and issues were tracked to resolution.	No exceptions noted.
2.04	The incident response process defining roles, responsibilities, escalation paths, and communication requirements in case of incidents that affect the security, availability, or confidentiality of the System is documented and available to personnel (employees and contractors). The incident response process is tested, at least, on an annual basis.	Inspected the incident response procedures, evidence of communication to personnel, and evidence of the most recent incident response test to determine that the incident response process defined roles, responsibilities, escalation paths, and communication requirements in case of incidents that affected the security, availability, or confidentiality of the System was documented and available to personnel (employees and contractors) and was tested during the review period.	No exceptions noted.
2.05	Product releases are communicated to external users via publicly available Release Notes.	Inspected the release notes for a sample of product releases during the review period to determine that product releases	No exceptions noted.

		were communicated to external users by publicity available release notes.	
2.06	Incidents impacting availability are communicated to customers within 24 hours.	Inspected evidence of communication for a sample of available incidents during the review period to determine that incidents impacting availability were communicated to customers within 24 hours of each incident sampled.	No exceptions noted.
2.07	Incidents impacting security and/or confidentiality are communicated to impacted customers, as per the Terms of Services ("ToS") and Security Policies published on the Company website	Inspected the listing of security incidents during the review period and determined that no incidents impacting security and/or confidentiality occurred during the review period; therefore, no testing of operating effectiveness was performed.	
Common Criteria Related to Risk Management and Design and Implementation of Controls			
3.01	The Company has defined a risk management process, which includes the review of the company's commitments and the operational, reporting, and compliance objectives to ensure they align with company's mission. On an annual basis, management performs a risk assessment to identify and evaluate potential threats, including the potential for fraud, to the effectiveness of the control environment. Mitigation strategies are defined for identified risks.	Inspected the risk management policy and most recently completed risk assessment documentation to determine that the Company had defined a risk management process, which included the review of the company's commitments and the operational, reporting, and compliance objectives to ensure they align with company's mission and performed a risk assessment during the review period to identify and evaluate potential threats, including the potential for fraud, to the effectiveness of the control environment at that mitigation strategies were defined for identified risks.	No exceptions noted.
3.02	The Company engages third parties to conduct penetration tests of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution.	Inspected the most recent penetration test report and evidence of remediation during the review period to determine that the Company engaged third parties to conduct penetration tests of the production environment during the review period and that results were reviewed by management and high priority findings were tracked to resolution.	No exceptions noted.
3.03	The Company manages a bug bounty program through which vulnerabilities are discovered and responsibly disclosed to the Company by external parties on an ongoing basis. Vulnerabilities are tracked to resolution.	Inspected evidence of remediation for a sample of vulnerabilities identified during the review period to determine that the Company managed a bug bounty through which vulnerabilities were discovered and responsibly disclosed to the Company by external parties on an ongoing basis and that the vulnerabilities were tracked to resolution for each vulnerability sampled.	No exceptions noted.

3.04	A vendor risk management process has been established per Fyipe's Third-Party Security Policy to identify, document, and, as required, mitigate vendor risks. Contracted vendors are categorized based on the Data Classification Standard.	Inspected the Third-Party Security Policy and Data Classification Standard to determine that a vendor risk management process had been established per Fyipe's Third-Party Security Policy to identify, document, and, as required, mitigate vendor risks, and that contracted vendors were categorized based on the Data Classification Standard.	No exceptions noted.
Monitoring Activities			
4.01	On an annual basis, management reviews vendors (subservice organization(s)) with access to highly sensitive data to evaluate the security, availability, and confidentiality controls relevant to the Company's commitments.	Inspected evidence of the most recently completed vendor review to determine that management reviewed vendors (subservice organizations) with access to highly sensitive data to evaluate the security, availability, and confidentiality controls relevant to the Company's commitments during the review period.	No exceptions noted.
4.02	Logs are aggregated centrally and monitored for indicators of compromise. Alerts are generated on suspicious activity and reviewed in accordance with the Security Monitoring and Auditing Standards.	Inspected the Security Monitoring and Auditing Standards, enterprise security monitoring application configurations and example alerts generated during the review period to determine that logs were aggregated centrally and monitored for indicators of compromise and that alerts were generated on suspicious activity and reviewed in accordance with the Security Monitoring and Auditing Standards.	No exceptions noted.
4.03	Management has implemented automated tools to monitor demands and to provision additional capacity.	Inspected the enterprise monitoring application and automated scaling configurations to determine that management implemented automated tools to monitor demands and to provision additional capacity.	No exceptions noted.
4.04	The Legal Team identifies, documents and tracks relevant legislative, regulatory, and contractual requirements that apply to Fyipe. Fyipe shall engage and maintain contact with experts (i.e. outside Counsel) as necessary.	Inspected evidence of tracking performed by the Legal Team during the review period to determine that the Legal Team identified, documented, and tracked relevant legislative, regulatory, and contractual requirements that applied to Fyipe and that Fyipe engaged and maintained contact with experts (i.e. outside Counsel) as necessary.	No exceptions noted.
Control Activities			
5.01	An internal control assessment is executed in accordance with the Security Program Assessment Standard.	Inspected the Security Program Assessment Standard and the most recently completed internal control assessment to determine that an internal control assessment was executed in accordance with the Security	No exceptions noted.

		Program Assessment Standard during the review period.	
5.02	The Director or Manager of Risk & Compliance reviews and approves the list of control activities on an annual basis.	Inspected the internal control matrix and the most recently completed review of control activities to determine that the Director or Manager of Risk & Compliance reviewed and approved the list of control activities during the review period.	No exceptions noted.
Logical and Physical Access Controls			
	AWS is responsible for implementing controls to manage logical access to the underlying network and virtualization management software for its cloud hosting services where Fyipe systems reside.		
	AWS is responsible for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers		
6.01	Management performs a quarterly review of access, including privileged access to sensitive customer data, to the production environment to identify unauthorized or terminated users. Any discrepancies are tracked to resolution.	Inspected the user access reviews for a sample of quarters during the review period to determine that management performed a quarterly review of access, including privileged access to sensitive customer data, to the production environment to identify unauthorized or terminated users and that any discrepancies were tracked to resolution for each quarter sampled.	No exceptions noted.
6.02	Access to the production environment and source code is restricted to appropriate users based on job responsibility. Unique accounts are required to access the production environment.	Inspected the user account listings for a sample of in-scope systems and the most recently completed user access review to determine that access to the production environment and source code was restricted to appropriate users based on job responsibility and that unique accounts were required to access the production environment to the following in-scope systems: • Identity management service • Configuration management tool • Bastion host • Application and database server operating system • Production databases • AWS management console • Source code repository tool	No exceptions noted.
6.03	Access to the production environment and source code is restricted via public key authentication or username and password; all require two-factor authentication.	Inspected the user account listings and minimum password requirements for a sample of in-scope systems to determine that	No exceptions noted.

		access to the production environment and source code was restricted via public key authentication or username and password and that all required two- factor authentication to the following in-scope systems: • Identity management service • Configuration management tool • Bastion host • Application and database server operating system • Production databases • AWS management console • Source code repository tool	
6.04	Inbound network traffic to the production environment is restricted in accordance with defined security requirements. Any changes to firewall configurations adhere to Fyipe's Change Control Policy.	Inspected the network diagram, firewall system configurations, and an example firewall rule change during the review period to determine that inbound network traffic to the production environment was restricted in accordance with defined security requirements and that any changes to firewall configuration adhered to Fyipe's Change Control Policy.	No exceptions noted.
6.05	Accounts for personnel who have been terminated or no longer require access to the production environment and/or source code are disabled within twenty-four (24) hours.	Inspected evidence of access removal, the termination checklist and the user account listings for a sample of in-scope systems and employees terminated during the review period to determine that accounts for personnel who had been terminated or no longer required access to the production environment and/or source code were disabled within (24) hours for each employee sampled to each of the following in-scope systems: • Identity management service • Configuration management tool • Bastion host • Application and database server operating system • Production databases • AWS management console • Source code repository tool	No exceptions noted.

6.06	Data transmitted between the public Internet and production servers is encrypted.	Inspected the TLS certificate to determine that data transmitted between the public Internet and production servers were encrypted.	No exceptions noted.
6.07	Sensitive customer data is encrypted at rest.	Inspected the production server encryption configurations to determine that sensitive customer data was encrypted at rest.	No exceptions noted.
6.08	Physical security is enforced at the Company's corporate office. Personnel are required to show proof of identity to enter the office building. Entrances to the office are locked and required authorized badge for entry after close of business.	Observed the physical security procedures for the office facility to determine that physical security was enforced at the Company's corporate office and that personnel were required to show proof of identity to enter the office building and that entrances to the office were locked and required authorized badge for entry after close of business.	No exceptions noted.
6.09	Disposal procedures are in place to guide personnel in performing sanitization procedures on instances where production data resides to ensure data and software is unrecoverable prior to retiring the virtual asset.	Inspected the media sanitization procedures to determine that disposal procedures were in place to guide personnel in performing sanitization procedures on instances where production data resided to ensure data and software was unrecoverable prior to retiring the virtual asset.	No exceptions noted.
6.10	EKM customer message and file data is encrypted at rest with Customer's encryption keys.	Inspected the EKM customer message and file data encryption configurations and example encrypted file data to determine that EKM customer message and file data was encrypted at rest with Customer’s encryption keys.	The test of control activity disclosed that the use of EKM Customer’s encryption keys was implemented in March 2019.
System Operations			
	AWS is responsible for monitoring any changes to the logical access controls system for the underlying network, virtualization management, and storage devices where the Fyipe systems reside.		
	AWS is responsible for monitoring physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers.		
7.01	Reported security incidents are tracked and triaged in accordance with Fyipe's Incident Response Standard. The standard includes procedures for collecting and preserving information that can serve as evidence.	Inspected the incident response procedure and the incident details for a sample of security incidents generated during the review period to determine that reported security incidents were tracked and triaged in accordance with Fyipe’s Incident Response Standard and that the standard included procedures for collecting and preserving information that could serve as evidence for each security incident sampled.	No exceptions noted.
7.02	Post-mortem meetings are conducted for security incidents according to the Incident Response Standard to discuss the root causes, remediation steps, and lessons learned. A post-mortem report is documented and archived.	Inspected the post-mortem meeting minutes and post mortem report for a sample of security incidents during the review period to determine that post-mortem meetings were conducted for security incidents according to the Incident Response Standard to discuss the root causes, remediation	No exceptions noted.

		steps, and lessons learned and that a post-mortem report was documented and archived for each security incident sampled.	
7.03	The Company has established baseline configuration standards for the production servers. The configuration management tool is run at least every three (3) days to detect and restore server configuration deviations from the standards.	Inspected the configuration management tool configurations and example job logs performed during the review period to determine that the Company established baseline configuration standards for the production servers and that the configuration management tool was set to run at least every three (3) days to detect and restore server configuration deviations from the standard.	No exceptions noted.
7.04	The Company laptops and workstations are required to be encrypted.	Inspected the configuration management tool and evidence of encryption for a sample of laptops and workstations to determine that the Company laptops and workstations were encrypted for each laptop and workstation sampled.	No exceptions noted.
7.05	The Company laptops and workstations are configured to lock themselves automatically when idle for 10 minutes.	Inspected the configuration management tool and evidence for a sample of laptops and workstations to determine that the Company laptops and workstations were configured to lock themselves automatically when idle for 10 minutes for each laptop and workstation sampled.	No exceptions noted.
7.06	Production servers are configured to check for and install security updates on a daily basis.	Inspected the configuration management tool and evidence for an example production server to determine that production servers were configured to check for and install security updates on a daily basis for each production server.	No exceptions noted.
7.07	The Company laptops and workstations are required to install the most recent operating system security updates.	Inspected the configuration management tool and evidence for a sample of laptops and workstations to determine that the Company laptops and workstations were required to install the most recent operating system security updates for each laptop and workstation sampled.	No exceptions noted.
7.08	The Company laptops and workstations are required to run antivirus software with up-to-date virus definitions.	Inspected the configuration management tool and evidence for a sample of laptops and workstations to determine that the Company laptops and workstations were required to run antivirus software with up-to-date virus definitions for each laptop and workstation sampled.	No exceptions noted.
Change Management			
8.01	A code review process is defined to ensure changes maintain the security, availability, and confidentiality of the System.	Inspected the change control policy to determine that a code review process was defined to ensure changes maintained the	No exceptions noted.

		security, availability, and confidentiality of the System.	
8.02	Independent code review and approval is required prior to deployment. Tools are utilized to monitor for changes to production environment and send alerts to engineering personnel.	Inquired of the staff risk and compliance engineer regarding the independent code review process to determine that independent code review and approval was required prior to deployment and tools were utilized to monitor for changes to production environment and sent alerts to engineering personnel.	No exceptions noted.
		Inspected the configuration management tool, source code software configurations and the evidence of deployment for an example change implemented during the review period to determine that an independent code review and approval was required prior to deployment and that tools were utilized to monitor for changes to production environment and sent alerts to engineering personnel.	No exceptions noted.
8.03	Major releases are tested prior to released.	Inspected the test cases for a sample of major releases implemented during the review period to determine that major releases were tested prior to being released for each major release sampled.	No exceptions noted.
8.04	Production and development systems are maintained separately using separate servers and databases.	Inspected the production and development server configurations to determine that production and development systems were maintained separately using separate servers and databases.	No exceptions noted.
8.05	Source code changes are logged, time-stamped, and attributed to their author in a source code management tool.	Inspected the configuration management tool, source code software configurations and example logs generated during the review period to determine that source code changes were logged, time-stamped, and attributed to their author in a source code management tool.	No exceptions noted.
Risk Mitigation			
9.01	User data is stored redundantly in at least two locations to ensure availability in case of datacenter failure.	Inspected the configuration management tool and replication configurations for an example production database server to determine that user data was stored redundantly in at least two locations to ensure availability in case of datacenter failure for each production database.	No exceptions noted.
ADDITIONAL CRITERIA FOR AVAILABILITY			
	AWS is responsible for ensuring the data center facilities are equipped with environmental security safeguards and utilizing an environmental monitoring application to monitor for environmental events.		
9.02	User data is automatically replicated in real-time between two database instances and backed up on a nightly basis. Operations is alerted of backup	Inspected the configuration management tool, replication configurations and backup	No exceptions noted.

	failures. Failures that impact backups of both database instances are resolved.	configurations for an example database server and evidence of a backup failure during the review period to determine that user data was automatically replicated in real-time between two database instances and backed up on a nightly basis and that Operations was alerted of backup failures and that failures that impacted backups of both database instances were resolved for each production database.	
9.03	Backups are restored at least every ninety (90) days to confirm processes and tools function as expected.	Inspected evidence of backup restoration for a sample of quarters during the review period to determine that backups were restored at least every ninety (90) days to confirm processes and tools functioned as expected for each quarter sampled.	No exceptions noted.
9.05	A Disaster Recovery ("DR") Plan has been documented. The DR Plan is reviewed, tested, updated as necessary, on an annual basis.	Inspected the DR Plan and the results of the most recent DR Plan test to determine that a DR Plan was documented and that the DR Plan was reviewed, tested, updated as necessary during the review period.	No exceptions noted.
9.06	Monitoring and alerting controls are implemented to ensure that compliance with customer commitments related to data retention are met.	Inspected security monitoring and auditing standards, the monitoring and alerting configurations, and an example alert generated during the review period to determine that monitoring and alerting controls were implemented to ensure that compliance with customer commitments related to data retention were met.	No exceptions noted.
ADDITIONAL CRITERIA FOR CONFIDENTIALITY			
10.01	Management has established procedures to ensure that customer data is not used for testing.	Inspected the change control policy and evidence of test data during the review period to determine that management established procedures to ensure that customer data was not used for testing.	No exceptions noted.
10.02	Access to sensitive customer data is restricted to appropriate personnel with credentials to access such data.	Inspected the user account listings for systems with access to customer data and the most recently completed user access review to determine that access to sensitive customer data was restricted to appropriate personnel with credentials to access such data.	No exceptions noted.
10.03	The System's multi-tenant architecture is configured to allow users to only access their own Fyipe Project(s). Each Fyipe Project is assigned a unique ID, which is verified with the associated access token during the authentication process.	Inspected the multi-tenant architecture configurations to determine that the System's multi- tenant architecture was configured to allow users to only access their own Fyipe Project(s) and that each Fyipe Project was assigned a unique ID, which was verified with the associated	No exceptions noted.

		access token during the authentication process.	
10.04	The Company requires third parties with access to confidential customer data to sign an agreement with confidentiality provision.	Inspected the confidentiality agreements for a sample of third parties with access to confidential customer data to determine that the Company required third parties with access to confidential customer data to sign an agreement with confidentially provision for each third-party sampled.	No exceptions noted.
10.05	The Company communicates its Privacy Policy and Terms of Service through the Company's website. Material changes to the Privacy Policy or Terms of Service are communicated through the Fyipe communication channel or e- mail messages.	Inspected evidence of communication of the Privacy Policy and Terms of Service during the review period to determine that the Company communicated its privacy Policy and Terms of Service through the Company's website and that material changes to the Privacy Policy or Terms of Service were communicated through Fyipe communication channel or e-mail messages.	No exceptions noted.
10.06	The Company has defined and published its default commitments for retaining and deleting sensitive customer data via its public-facing website. The default data retention and deletion policy can be overridden by customer-defined retention periods.	Inspected the default data retention and deletion commitments on the company's website to determine that the Company defined and published its default commitments for retaining and deleting sensitive customer data via its public-facing website.	No exceptions noted.
		Inspected the data retention configurations for an example Project to determine that the default data retention and deletion policy could be overridden by customer-defined retention periods.	No exceptions noted.
10.07	Fyipe utilizes automated scripts to dispose of customer data in accordance with the default and/or customer customized data retention settings.	Inspected the automated disposal script and an example data deletion log during the review period to determine that Fyipe utilized automated scripts to dispose of customer data in accordance with the default and/or customer customized data retention settings.	No exceptions noted.

SECTION 5

OTHERINFORMATION PROVIDED BY HackerBay (Fyipe)

Additional Information Provided by Management

Physical Security

Physical presence in a HackerBay office or a connection to Company WiFi does not confer any elevated access to the System production environment, source code, or internal tools.