System and Organization Controls (SOC) 2 Type II

Report on Management's Description of its

Pequity Compensation Management Platform

And the Suitability of Design of Controls Relevant to the

Controls Placed in Operation and Test of Operating Effectiveness Relevant to the Security, Availability, and Confidentiality Categories

For the Period
June 5, 2021 to September 5, 2021

Together with

Pequity

Independent Service Auditors' Report

TABLE OF CONTENTS

I. INDEPENDENT SERVICE AUDITORS' REPORT 1

II. ASSERTION OF PEQUITY MANAGEMENT..... 5

III. DESCRIPTION OF THE PEQUITY COMPENSATION MANAGEMENT PLATFORM..... 7

IV. DESCRIPTION OF CRITERIA, PEQUITY CONTROLS, TESTS, AND RESULTS OF TESTS..... 22

I. INDEPENDENT SERVICE AUDITORS' REPORT

INDEPENDENT SERVICE AUDITORS' REPORT

To the Management of Pequity, Inc. (Pequity)

Scope

We have examined Pequity's accompanying description of its Pequity Compensation Management Platform titled "Description of the Pequity Compensation Management Platform" (description) throughout the period June 5, 2021 to September 5, 2021 (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*), and the suitability of the design and operating effectiveness of controls stated in the description throughout the period June 5, 2021 to September 5, 2021, to provide reasonable assurance that Pequity's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Pequity uses subservice organizations to provide application maintenance and support services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Pequity, to achieve Pequity's service commitments and system requirements based on the applicable trust services criteria. The description presents Pequity's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Pequity's controls. Our examination did not include the services provided by the subservice organizations, 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 Pequity, to achieve Pequity's service

commitments and system requirements based on the applicable trust services criteria. The description presents Pequity's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Pequity's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

Pequity 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 Pequity service commitments and system requirements were achieved. Pequity has provided the accompanying assertion titled "Assertion of Pequity Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. Pequity 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 Auditors' 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 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
- 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 Tests of Controls

The specific controls we tested, and the nature, timing, and results of those tests are listed in section IV.

Opinion

In our opinion, in all material respects,

a. the description presents the Pequity Compensation Management Platform that was designed and implemented throughout the period June 5, 2021 to September 5, 2021, in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period June 5, 2021 to September 5, 2021, to provide reasonable assurance that Pequity's 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 user entities applied the complementary controls assumed in the design of Pequity's controls throughout that period.

c. the controls stated in the description operated effectively throughout the period June 5, 2021 to September 5, 2021, to provide reasonable assurance that Pequity's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Pequity's controls operated effectively throughout that period.

Restricted Use

This report, including the description of test of controls and results thereof in section IV, is intended solely for the information and use of Pequity, user entities of Pequity's Pequity Compensation Management Platform during some or all of the period June 5, 2021 to September 5, 2021, business partners of Pequity subject to risks arising from interactions with the Pequity Compensation Management Platform, 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
- 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.

San Jose, California
October 15, 2021

II. ASSERTION OF PEQUITY MANAGEMENT

Pequity

ASSERTION OF PEQUITY MANAGEMENT

We have prepared the accompanying description of Pequity Inc.'s (Pequity) Pequity Compensation Management Platform entitled "Description of the Pequity Compensation Management Platform," throughout the period June 5, 2021 to September 5, 2021, (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). The description is intended to provide report users with information about the Pequity Compensation Management Platform that may be useful when assessing the risks arising from interactions with Pequity's system, particularly information about system controls that Pequity 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, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, Trust Services Criteria).

Pequity uses subservice organizations to provide application maintenance and support services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Pequity, to achieve Pequity's service commitments and system requirements based on the applicable trust services criteria. The description presents Pequity's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Pequity's controls. The description does not disclose the actual controls at the subservice organizations.

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

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

a. the description presents the Pequity Compensation Management Platform that was designed and implemented throughout the period June 5, 2021 to September 5, 2021, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period June 5, 2021 to September 5, 2021, to provide reasonable assurance that Pequity's 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 user entities applied the complementary controls assumed in the design of Pequity's controls throughout that period.
c. the controls stated in the description operated effectively throughout the period June 5, 2021 to September 5, 2021, to provide reasonable assurance that Pequity's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Pequity's controls operated effectively throughout that period.

Signed by Pequity Management - October 15, 2021

III. DESCRIPTION OF THE PEQUITY COMPENSATION MANAGEMENT PLATFORM

DESCRIPTION OF THE PEQUITY COMPENSATION MANAGEMENT PLATFORM

Company Background

Pequity, Inc. (Pequity) was founded in late 2019 with the goal of simplifying the compensation process for teams looking to attract and retain world class talent. The platform helps companies make streamlined compensation and hiring decisions, benchmark their current team members against each other and market norms for compensation, and collaborate with key decision makers surrounding candidates and their compensation.

Today, the tool is being used by recruiters, compensation professionals, and executives at companies like Instacart, May Mobility, and Clearco to make smarter and more transparent compensation decisions.

Services Provided

Pequity provides a SaaS platform accessible in the web browser that helps teams make smarter compensation decisions. Notably, the platform:

- Allows companies to work together internally to approve a candidate's compensation (pay + equity)
- Compare compensation market data against existing team members
- Create a company's pay philosophy through compensation ranges based on a candidate's experience and geographic location
- Allows companies to update their application tracking system through Pequity to keep track of where a candidate is in their offer pipeline.

Generally, market data for compensation ranges is imported by the client and delivered through a third-party external data source. Pequity provides companies with a snapshot into whether candidates and current team members are currently overpaid, underpaid, or paid correctly given this market data and given the company's pay ranges built off of this market data.

Principal Service Commitments and System Requirements

Pequity designs its processes and procedures related to its platform to meet its objectives as outlined in our customer contracts and SLA's. Those objectives are based on the service commitments that Pequity makes to user entities, the laws and regulations that govern the provision of our Platform, and the financial, operational, and compliance requirements that Pequity has established for the Platform. Pequity's Platform is subject to the security and privacy requirements of state and local privacy security laws and regulations in the jurisdictions in which Pequity operates.

Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online.

Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of the Pequity Platform that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role.
- Use of encryption technologies to protect customer data both at rest and in transit

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

Components of the System

Infrastructure

Primary infrastructure used to provide Pequity's Compensation Management Platform includes the following:

Primary Infrastructure		
Hardware	Type	Purpose
DigitalOcean (DO)	Droplet	Serve application and host database
Amazon Web Services (AWS)	EC2 Instance	Serve application and host database backups

Software

Primary software used to provide Pequity's Compensation Management Platform includes the following:

Primary Software		
Software	Operating System	Purpose
Cloudflare	Cloudflare	Configure firewalls and additional security as well as DNS management for DO

Primary Software		
Software	Operating System	Purpose
AppCues	AppCues	Collect user analytics and provide onboarding guidance for new user experience
Google Analytics	Google Analytics	Application usage analytics
Fullstory	Fullstory	Application usage analytics
Sentry	Sentry	Security monitoring and threat detection

People

Pequity has a staff of approximately 20 people as of date of writing, divided by responsibility as follows:

Leadership: Seniorstaff, including executives and co-founders of the company as well as operations, legal, and engineering leadership staff that support strategic decision making and ongoing operations of the company. The leadership team today is comprised of four individuals.

Engineering: Pequity's engineering team is made up of both employees and independent contractors, some of which have been contracted through a third-party software development organization. The engineering team is tasked with product development, code maintenance, feature implementation, ensuring up-time, and quality assurance of the product. Currently, there are ten, soon to be eleven, members of the engineering team.

Growth: The growth team interfaces routinely with prospective clients and existing clients to build pipeline, increase sales, and keep our clients satisfied in the hopes of keeping churn as low as possible. Currently, Pequity has two team members on sales and another on client success.

We expect our team to more than double in the coming months as we grow.

Data

Data is defined by Pequity as either:

Client Data: any proprietary or confidential content, information, data, or materials which is provided to or processed by Pequity in connection with the provision of the Pequity Platform. This includes identifying data (names, contact information, professional status), user activity audit data (permissions,

product activity, and historical reports), and administrative and security monitoring data.

End User Data: all data and information collected from an employer, contractor, or agent of one of Pequity's clients including any personally identifiable information and compensation data pertaining to our Client's employees and anonymized compensation and market data.

Data is encrypted at rest and in transit. Pequity is granted a license to Client Data and End User Data that is anonymized such that it does not contain any identifiable elements to connect it back to an individual.

Processes, Policies and Procedures

Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. All teams are expected to adhere to the Pequity policies and procedures that define how services should be delivered. These are located on the Company's internal communication and management systems and can be accessed by any Pequity team member.

Physical Security

All data is hosted by DO and AWS. DO and AWS data centers do not allow Pequity employees physical access. At present, all work is conducted remotely.

Logical Access

Pequity uses the DO security architecture. The user types are predefined. The members are given access to DO based on roles. The highest permissions role is owner. The rest of the users are members. MFA or another type of secure login (Google authentication) is being enforced for all members, owners included. Owners can provide access to the DO resources. There is an inventory of the resources in place. Everybody is responsible for certain resources. Their SSH pub keys are added to the resources they are responsible for and access is granted only to a restricted number of members. We enforce MFA at SSH level for such access.

Access to company systems are monitored routinely, and policies are in place for team member on-boarding and offboarding to ensure smooth transitions without improper access to company technology or resources for a given team member.

Computer Operations – Backups

Customer data is backed up by Pequity's engineering team. In the event of an exception, engineering personnel perform troubleshooting to identify the root cause and then re-run the backup job immediately or as part of the next scheduled backup job.

Backup infrastructure is maintained in AWS, with physical access restricted according to applicable AWS policies. All backups are encrypted using KMS-managed encryption keys, with access restricted to key personnel via AWS IAM permissions.

Computer Operations – Availability

All Pequity production environment security and availability are monitored in real-time, and all security threats (whether resolved or not) are immediately reported to Pequity security and infrastructure

channels. Availability and usage spikes are also immediately reported and general capacity is reviewed on a recurring cadence. Automated load balancing, availability zones, and multi-infrastructure systems are employed to quickly respond to service demands and maintain a consistent level of product quality and integrity.

Incident response policies and procedures are in place to guide Pequity personnel through the steps required to respond to, evaluate, patch, and report an incident internally and externally to affected parties. Review of the incident is conducted to prevent repeating incidents and ensure the rigor of the Pequity platform going forward.

Change Control

Pequity leverages a number of industry leading tools in the pursuit of change control and change management. Firstly, GitHub is used as a code repository for tracking code changes and identifying those changes to the writer of said code as well as for Git-enabled version control. Additionally, a ticketing system is used to document changes made to the application - all team members have visibility over the work of others. JIRA is the ticketing system leveraged for this purpose. When changes are made to the application, they are pushed to a pre-production staging server for quality-assurance testing that is logically separated from the production environment. The engineering team runs a series of automated test suites in addition to manual UI/UX testing on pre-production to ensure proper functioning prior to pushing to production.

Data Communications

Pequity's production infrastructure is protected using a host-based firewall to only allow encrypted access in and out a limited amount of ports. All inbound traffic is filtered on IP addresses and other control rules. Pequity also uses Cloudflare as a DNS manager and network-based firewall to protect from further security threats and ensure availability and capacity.

The Pequity platform is built upon a multi-tenancy architecture, thus every subdomain (and every Pequity client) is proxied by Cloudflare. We are using a public-key certificate to protect our domains and we have enabled TLS 1.3, XSS protection, as well as other security headers.

We are performing annual security penetration testing and vulnerability scans. The third-party vendor is GWAPT certified. They audit the application source code repository, cloud environment (DO), web application, testing for vulnerabilities. Once tests are concluded the final deliverables are detailed in a final report, and a remediation report is sent to us so we can take immediate measures.

The tests are performed on a snapshot of our application droplet, on another instance where we use anonymized and testing data.

Boundaries of the System

The scope of this report includes the Compensation Management Platform performed by Pequity.

This report does not include the data center hosting services provided by DO and AWS.

The applicable trust services criteria and the related controls

Common Criteria (to the Security, Availability, and Confidentiality Categories)

Security refers to the protection of

i. information during its collection or creation, use, processing, transmission, and storage and

ii. systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

Availability

Availability refers to the accessibility of information used by the entity's systems, as well as the products or services provided to its customers. The availability objective does not, in itself, set a minimum acceptable performance level; it does not address system functionality (the specific functions a system performs) or usability (the ability of users to apply system functions to the performance of specific tasks or problems). However, it does address whether systems include controls to support accessibility for operation, monitoring, and maintenance.

Confidentiality

Confidentiality addresses the entity's ability to protect information designated as confidential from its collection or creation through its final disposition and removal from the entity's control in accordance with management's objectives. Information is confidential if the custodian (for example, an entity that holds or stores information) of the information is required to limit its access, use, and retention and restrict its disclosure to defined parties (including those who may otherwise have authorized access within its system boundaries). Confidentiality requirements may be contained in laws or regulations or in contracts or agreements that contain commitments made to customers or others. The need for information to be confidential may arise for many different reasons. For example, the information may be proprietary, intended only for entity personnel.

Confidentiality
(Continued) Confidentiality is distinguished from privacy in that privacy applies only to personal information, whereas confidentiality applies to various types of sensitive information. In addition, the privacy objective addresses requirements regarding collection, use, retention, disclosure, and disposal of personal information. Confidential information may include personal information as well as other information, such as trade secrets and intellectual property.

Control Environment

Integrity and Ethical Values

Pequity takes the integrity of our team members seriously given that we entrust access to confidential and identifiable data that is leveraged by our clients for their HR and compensation purposes. We ensure that team members are operating in an ethical manner in relation to the Pequity platform and are not using data for improper purposes. Access to the Platform is monitored through various tools such as GitHub for code base changes, the DO console, and Cloudflare which provides logs for access to the tool. Background checks are performed for all team members that have the potential to have access to sensitive client data or to the code base or other configurable back-end tools related to the Pequity Platform. Team members are required to sign off on policies hosted in the Drata compliance platform as they relate to team member responsibilities when accessing Pequity and any related data. A confidentiality statement agreeing not to disclose proprietary or confidential information, including confidential information, to unauthorized parties is a component of team member onboarding.

Specific control activities that the service organization has implemented in this area are described below:

- Formally, documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel.
- Policies and procedures require employees to sign an acknowledgment form indicating they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual.
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employee handbook.
- Background checks are performed for employees as a component of the hiring process.

Commitment to Competence

Pequity's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into the requisite skills and knowledge.

Specific control activities that the service organization has implemented in this area are described below:

- Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements.

- Training is provided to maintain the skill level of personnel in certain positions.

Management's Philosophy and Operating Style

Pequity's management philosophy and operating style encompass 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 the service organization has implemented in this area are described below:

- Management is periodically briefed on regulatory and industry changes affecting the services provided.
- Executive management meetings are held to discuss major initiatives and issues that affect the business as a whole.
- Management engages with core areas of the business routinely to ensure that all security protocols and processes are routinely tested and in place

Organizational Structure and Assignment of Authority and Responsibility

Pequity's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

Pequity's assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

Specific control activities that the service organization has implemented in this area are described below:

- Organizational charts are in place to communicate key areas of authority and responsibility. • Organizational charts are communicated to employees and updated as needed.

Human Resource Policies and Practices

Pequity's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top quality personnel who ensures the service organization is operating at maximum efficiency. Pequity's human resources policies and practices relate to team member hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

Specific control activities that the service organization has implemented in this area are described below:

- New employees are required to sign a confidentiality agreement prior to their first day ● Routine evaluations and team member meetings are performed by management

Risk Assessment Process

Pequity's risk assessment process identifies and manages risks that could potentially affect Pequity's ability to provide reliable services to user organizations. This ongoing process requires that management identify significant risks inherent in products or services as they oversee their areas of responsibility. Pequity identifies the underlying sources of risk, measures the impact to organization, establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks.

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

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

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

<u>Integration with Risk Assessment</u>

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

Information and Communications Systems

Information and communication is an integral component of Pequity's internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations. This process encompasses the primary classes of transactions of the organization, including the dependence on, and complexity of, information

technology. At Pequity, information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, regulators, and employees.

Various weekly calls are held to discuss operational efficiencies within the applicable functional areas

and to disseminate new policies, procedures, controls, and other strategic initiatives within the organization. Additionally, all hands meetings are held frequently to provide staff with updates on the firm and key issues affecting the organization and its employees. Senior executives lead the all-hands meetings with information gathered from formal automated information systems and informal databases, as well as conversations with various internal and external colleagues.

Monitoring Controls

Pequity enforces all user provisioning procedures, engineering version control auditing, and monitors all user activity. Administrative access is controlled through user roles, which are enforced throughout - from the platform to the database. Security threats and any identified risks are escalated and documented through established Pequity policies.

Management reviews the control systems in place to establish that a) all corrective actions are implemented to resolve current threats and prevent future ones of the same nature, b) the timeliness and response rate for previous control incidents, and c) identifying and adjusting monitoring processes for anticipated or potential vulnerabilities.

Reporting Deficiencies

An internal tracking tool is utilized to document and track the results of ongoing monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

Changes to the System in the Last 12 Months

No significant changes have occurred to the services provided to user entities in the 12 months preceding the end of the review date.

Incidents in the Last 12 Months

No significant incidents have occurred to the services provided to user entities in the 12 months preceding the end of the review date.

Criteria Not Applicable to the System

All Common, Availability, and Confidentiality criteria were applicable to the Pequity Compensation Management Platform.

Subservice Organizations

Pequity's services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all the trust services criteria related to Pequity's services to be solely achieved by Pequity control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Pequity.

The following subservice organization controls should be implemented by DigitalOcean and AWS to

provide additional assurance that the trust services criteria described within this report are met.

Subservice Organization – AWS		
Category	Criteria	Control
Common Criteria / Security	CC6.4	Physical access to data centers is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		Physical access to data centers reviewed on a quarterly basis by appropriate personnel.
		Physical access points to server locations are recorded by closed circuit television camera (CCTV). Images are retained for 90 days, unless limited by legal or contractual obligations.
		Physical access points to server locations are managed by electronic access control devices.
		Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.
Availability	A1.2	Amazon-owned data centers are protected by fire detection and suppression systems.
		Amazon-owned data centers are air conditioned to maintain appropriate atmospheric conditions. Personnel and systems monitor and control air temperature and humidity at appropriate levels.

Subservice Organization – AWS		
Category	Criteria	Control
		Uninterruptible Power Supply (UPS) units provide backup power in the event of an electrical failure in Amazon-owned data centers.

		Amazon-owned data centers have generators to provide backup power in case of electrical failure.
		Contracts are in place with third-party colocation service providers which include provisions to provide fire suppression systems, air conditioning to maintain appropriate atmospheric conditions, Uninterruptible Power Supply (UPS) units, and redundant power supplies.
		Critical DO and AWS system components are replicated across multiple Availability Zones and backups are maintained.
		Backups of critical DO and AWS system components are monitored for successful replication across multiple Availability Zones.

Subservice Organization – DigitalOcean		
Category	Criteria	Control
Common Criteria / Security	CC6.4	Physical access control systems are in place to restrict access to and within the corporate facility and data center housing the facilities, backup media, and other system components such as firewalls, routers, and servers to properly authorized individuals.
		Procedures exist and are followed to establish and make changes to physical access privileges for customers.
		Procedures exist and are followed to establish and make changes to physical access privileges for employees.

Subservice Organization – DigitalOcean		
Category	Criteria	Control
		Security personnel review a government issued ID prior to allowing off-site employees, visitors, customers, vendors, and contractors access to the facility.

		Visitors are required to sign a visitor log upon entering the facility, and be escorted by an authorized employee when accessing the facility.
		A proximity card system and / or a biometric reader and PIN are required to restrict access to the facility.
		Physical access system logs are recorded and maintained for a minimum of six months.
		Internal and external monitoring of physical activity is performed through the use of 24x7 security monitoring and digital surveillance cameras.
		Surveillance camera logs are recorded and maintained for a minimum of 30 days.
		Access to the colocation areas requires a valid badge access card. Each customer has a defined space within the data center that is physically secured within a locked cage and / or cabinet.
		The data center floor does not have any windows leading to the exterior of the building. In case due to the existing infrastructure there are windows leading to the exterior then they need to be locked from the inside or access controlled.
		Physical access reviews for data center facilities in South America are documented and approved on a quarterly basis by information security personnel.
Availability	A1.2	Fire detection and suppression equipment is in place at each facility.
		Scheduled maintenance procedures are performed to ensure that fire detection and suppression equipment is working properly.

Subservice Organization – DigitalOcean		
Category	Criteria	Control
		Power management equipment is in place for each facility.

		Scheduled maintenance procedures are performed to test and confirm the operation of the power management systems.
		Air conditioning and ventilation equipment is in place at each facility to ensure that humidity levels and the required temperature are maintained.
		Scheduled maintenance procedures are performed to ensure that the HVAC equipment and temperature and water detection sensors are working properly.
		IBX facilities are monitored 24x7 by facilities engineers. Equinix has staff in place either on-site or on call 24x7 who are alerted by the BMS for system exceptions.
		Backup systems are in place to perform scheduled backups of production data at predefined times.
		Emergency procedures are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.

Pequity management, along with the subservice organizations, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts,such as service level agreements. In addition, Pequity performs monitoring of the subservice organization controls, including the following procedures:

- Holding periodic discussions with vendors and subservice organizations
- Reviewing attestation reports over services provided by vendors and subservice organizations
- Monitoring external communications,such as customer complaints relevant to the services by the subservice organizations

Complementary User Entity Controls

Pequity'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 the Trust Services Criteria related to Pequity's services to be solely achieved by Pequity control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Pequity's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services 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.

1. User entities are responsible for understanding and complying with their contractual obligations to Pequity.
2. User entities are responsible for notifying Pequity of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record. 4. User entities are responsible for ensuring the supervision, management, and control of the use of Pequity services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Pequity services.
6. User entities are responsible for providing Pequity with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying Pequity of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.

IV. DESCRIPTION OF CRITERIA, PEQUITY CONTROLS, TESTS, AND RESULTS OF TESTS

DESCRIPTION OF CRITERIA, PEQUITY CONTROLS, TESTS AND RESULTS OF TESTS

Relevant trust services criteria and Pequity related controls are an integral part of management's system description and are included in this section. Sensiba San Filippo LLP performed testing to determine if Pequity's controls were suitably designed and operating effectively to achieve the specified criteria for the security, availability, and confidentiality categories set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria)*, throughout the period June 5, 2021 to September 5, 2021.

Tests of the controls included inquiry of appropriate management, supervisory and staff personnel, observation of Pequity activities and operations and inspection of Pequity documents and records. The results of those tests were considered in the planning, the nature, timing and extent of Sensiba San Filippo LLP's testing of the controls designed to achieve the relevant trust services criteria. As inquiries were performed for substantially all Pequity controls, this test was not listed individually for every control in the tables below.

Trust Services Criteria for the Security Category	***Description of Pequity Controls***	***Service Auditor Test of Controls***	***Result of Test of Controls***
Control Environment			
CC1.1 *The entity demonstrates a commitment to integrity and ethical values.*	CC1.1.1 The entity has a documented code of conduct that includes its commitments to integrity and ethical values.	Inspected the entity's code of conduct to determine that it included its commitments to integrity and ethical values.	No exceptions noted
	CC1.1.2 Personnel are required to read and accept the code of conduct upon being hired.	Inspected policy acknowledgements for a sample of employees to determine that the code of conduct was acknowledged by new employees upon being hired.	No exceptions noted
	CC1.1.3 Employees are required to pass a background check as a condition of their employment.	Inspected evidence of completed background checks for a sample of employees to determine that background checks were completed for all employees as a condition of their employment.	No exceptions noted
	CC1.1.4 Contractors are required to read and accept the code of conduct, read and accept an acceptable use agreement and pass a background check.	Inspected policy acknowledgements and evidence of completed background check to determine that contractors were required read and accept the code of conduct, read and accept an acceptable use	No exceptions noted

				agreement and pass a background check.		

Trust Services Criteria for the Security Category		*Description of Pequity Controls*		*Service Auditor Test of Controls*		*Result of Test of Controls*
Control Environment						
CC1.2 *The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.*		CC1.2.1 The members of the board of directors are independent of management.		Inspected the members of the board of directors to determine that the members of the board of directors were independent of management.		No exceptions noted
		CC1.2.2 The Head of Operations exercises oversight of security controls by reviewing security policies on an annual basis.		Inspected review evidence to determine that the Head of Operations exercises oversight of security controls by reviewing security policies and making recommendations on an annual basis.		No exceptions noted
CC1.3 *Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.*		CC1.3.1 The Head of Operations reviews its organizational structure, reporting lines, authorities, and responsibilities in terms of information security on an annual basis.		Inspected the organization chart review to determine that Head of Operations reviewed the organizational structure, reporting lines, authorities, and responsibilities in terms of information security on an annual basis.		No exceptions noted
		CC1.3.2 An organizational chart has been defined to appropriately document reporting lines in terms of information security.		Inspected the organizational chart to determine that reporting lines had been appropriately defined for information security.		No exceptions noted
CC1.4 *The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.*		CC1.4.1 Job requirements and responsibilities are documented in job descriptions.		Inspected job descriptions to determine that job requirements and responsibilities were documented.		No exceptions noted

		CC1.4.2 Employees are required to pass a background check as a condition of their employment.		Inspected evidence of completed background checks for a sample of employees to determine that background checks were completed for all employees as a condition of their employment.		No exceptions noted

Trust Services Criteria for the Security Category		***Description of Pequity Controls***		***Service Auditor Test of Controls***		***Result of Test of Controls***
Control Environment						
		CC1.4.3 Contractors are required to read and accept the code of conduct, read and accept an acceptable use agreement and pass a background check.		Inspected policy acknowledgements and evidence of completed background check to determine that contractors were required read and accept the code of conduct, read and accept an acceptable use agreement and pass a background check.		No exceptions noted
CC1.5 *The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.*		CC1.5.1 Security awareness training is provided to all employees on an annual basis.		Inspected evidence of security awareness training completion for a sample of employees to determine that security awareness training was provided.		No exceptions noted
		CC1.5.2 Security awareness training is provided to all contractors on an annual basis.		Inspected evidence of security awareness training completion for a sample of contractors to determine that security awareness training was provided.		No exceptions noted
		CC1.5.3 Managers are required to complete performance appraisals for direct reports at least annually.		Inspected completed performance evaluations for a sample of employees to determine that performance appraisals were completed by managers.		No exceptions noted
Information and Communication						

CC2.1 *The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.*		CC2.1.1 Pequity uses a SOC 2 compliance platform called Drata which objectively and continuously monitors the Pequity control environment and alerts management when internal control and security issues arise.		Inspected the Drata tool configurations to determine that Pequity uses a SOC 2 compliance platform called Drata which objectively and continuously monitors the Pequity control environment and alerts management when internal control and security issues arise.		No exceptions noted
CC2.2 *The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.*		CC2.2.1 Internal personnel have been provided with information on how to report security failures, incidents, concerns, and other complaints to appropriate personnel via the employee handbook, which is posted on the company intranet.		Inspected the employee handbook to determine that it was posted on the company intranet and to determine that it included information on how to report security failures, incidents, concerns, and other complaints to appropriate personnel.		No exceptions noted

Trust Services Criteria for the Security Category		***Description of Pequity Controls***		***Service Auditor Test of Controls***		***Result of Test of Controls***
Information and Communication						
		CC2.2.2 Personnel are required to read and accept the code of conduct upon being hired.		Inspected code of conduct acknowledgements for a sample of employees to determine that the code of conduct was acknowledged upon being hired.		No exceptions noted
		CC2.2.3 Contractors are required to read and accept the code of conduct upon being hired.		Inspected code of conduct acknowledgements for a sample of contractors to determine that the code of conduct was acknowledged upon being hired.		No exceptions noted
		CC2.2.4 Personnel are required to read and accept an acceptable use agreement upon being hired.		Inspected evidence of acceptable use acknowledgements for a sample of employees to determine that employees were required to read and accept acceptable use agreements.		No exceptions noted

		CC2.2.5 Contractors are required to read and accept an acceptable use agreement upon being hired.		Inspected evidence of acceptable use acknowledgements for a sample of contractors to determine that employees were required to read and accept acceptable use agreements.		No exceptions noted
CC2.3 *The entity communicates with external parties regarding matters affecting the functioning of internal control.*		CC2.3.1 Privacy policies are posted on the entity's website to communicate the entity's privacy practices.		Inspected the entity's website to determine that the entity's privacy policies were posted.		No exceptions noted
		CC2.3.2 Pequity maintains a Terms of Service that is available to all external users and internal employees, and the terms detail the company's security and availability commitments regarding the systems.		Inspected the Pequity Terms of Service to determine that it is available to all external users and internal employees, and the terms detail the company's security and availability commitments regarding the systems.		No exceptions noted
Risk Assessment						
CC3.1 *The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.*		CC3.1.1 The entity has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.		Inspected the risk assessment policy to determine that the entity had a defined, formal risk management process that specified risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.		No exceptions noted

Trust Services Criteria for the Security Category		***Description of Pequity Controls***		***Service Auditor Test of Controls***		***Result of Test of Controls***
Risk Assessment						
CC3.2 *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.*		CC3.2.1 A risk assessment is performed on an annual basis to identify and rank potential threats to the system.		Inspected the risk assessment to determine that a risk assessment was completed during the period and identified and ranked potential threats to the system.		No exceptions noted

		CC3.2.2 When identifying risks to include in the risk assessment, the entity considers relevant laws and regulations specific to the types of data they possess (i.e. Protected Health Information, Personally Identifiable Information, etc.).		Inspected the completed risk assessment to determine that the entity considered relevant laws and regulations specific to the types of data they possess, when identifying risks to include in the risk assessment.		No exceptions noted
CC3.3 *The entity considers the potential for fraud in assessing risks to the achievement of objectives.*		CC3.3.1 A risk assessment is performed on an annual basis to identify and rank potential threats to the system.		Inspected the risk assessment to determine that a risk assessment was completed during the period and identified and ranked potential threats to the system.		No exceptions noted
CC3.4 *The entity identifies and assesses changes that could significantly impact the system of internal control.*		CC3.4.1 The Head of Operations reviews its organizational structure, reporting lines, authorities, and responsibilities in terms of information security on an annual basis.		Inspected the organization chart review to determine that Head of Operations reviewed the organizational structure, reporting lines, authorities, and responsibilities in terms of information security on an annual basis.		No exceptions noted
		CC3.4.2 A risk assessment is performed on an annual basis to identify and rank potential threats to the system.		Inspected the risk assessment to determine that a risk assessment was completed during the period and identified and ranked potential threats to the system.		No exceptions noted
Monitoring Activities						
CC4.1 *The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.*		CC4.1.1 Cloud infrastructure is monitored through DigitalOcean monitoring that sends alerts to appropriate personnel.		Inspected cloud infrastructure monitoring configurations and monitoring rulesets from DigitalOcean monitoring to determine that cloud infrastructure was monitored, and alerts would be sent based on predefined rulesets.		No exceptions noted

Trust Services Criteria for the Security Category		***Description of Pequity Controls***		***Service Auditor Test of Controls***		***Result of Test of Controls***
Monitoring Activities						

		CC4.1.2 Monitoring configured to identify web traffic and suspicious activity. When anomalous traffic activity is identified, alerts are automatically created, sent to appropriate personnel and resolved, as necessary.		Inspected DigitalOcean monitoring logs to determine that monitoring was configured to identify web traffic and suspicious activity.		No exceptions noted
CC4.2 *The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including management and executive leadership, as appropriate.*		CC4.2.1 The entity has incident response policies and procedures in place that includes plans for escalating to internal personnel.		Inspected the entity's incident response policies and procedures to determine that the incident response policies and procedures included plans for escalating to internal personnel.		No exceptions noted
		CC4.2.2 Pequity provides a process to external users for reporting security, confidentiality, integrity and availability failures, incidents, concerns, and other complaints.		Inspected the support page to determine that Pequity provides a process to external users for reporting security, confidentiality, integrity and availability failures, incidents, concerns, and other complaints.		No exceptions noted
Control Activities						
CC5.1 *The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.*		CC5.1.1 As part of its annual risk assessment, management linked the identified risks to controls that have been designed and operated to address them. When the need for new controls is identified, management develops the requirements for the new controls and uses the change management process to implement them.		Inspected the risk assessment that was completed during the period to determine that risks were linked to controls and that new were controls were considered for any risks not adequately addressed by existing controls.		No exceptions noted
		CC5.1.2 The entity has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.		Inspected the risk assessment policy to determine that the entity had a defined, formal risk management process that specified risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.		No exceptions noted

Trust Services Criteria for the Security Category	*Description of Pequity Controls*	*Service Auditor Test of Controls*	*Result of Test of Controls*
Control Activities			
CC5.2 *The entity also selects and develops general control activities over technology to support the achievement of objectives.*	CC5.2.1 Web application scans are performed on a quarterly basis to identify vulnerabilities, and management takes action based on the results of the scan.	Inspected the scan results to determine that web application vulnerability scans were performed, and management takes action based on the results of the scan.	No exceptions noted
	CC5.2.2 Web application penetration tests, that include testing for the OWASP top-ten vulnerabilities, are performed by an independent third party on an annual basis and management takes action, as necessary, based on the results of the testing.	Inspected the web application penetration test and remediation report results to determine that a web application penetration test, that included testing for the OWASP top-ten vulnerabilities, was performed by an independent third party. Management takes action, as necessary, based on the results of the testing.	No exceptions noted
CC5.3 *The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.*	CC5.3.1 IT and security policies are defined for protecting against unauthorized access that could compromise the availability, integrity, confidentiality, and privacy of information or systems. IT and security policies are reviewed by appropriate members of management on an annual basis.	Inspected the IT and security policies to determine that IT and security policies were defined for protecting against unauthorized access that could compromise the availability, integrity, confidentiality, and privacy of information or systems.	No exceptions noted
		Inspected management's review of IT and security policies to determine that IT and security policies were reviewed by appropriate members of management on an annual basis.	No exceptions noted
	CC5.3.2 Management has approved Pequity security policies, and all employees agree to these procedures when hired. Management also ensures that security policies are accessible to all employees and contractors.	Inspected Pequity's security policies to determine that they outline requirements for securing the company's operations, services, and systems.	No exceptions noted

				Inspected evidence of security policy acknowledgements for a sample of employees to determine that all employees agree to these procedures when hired.		No exceptions noted

Trust Services Criteria for the Security Category		***Description of Pequity Controls***		***Service Auditor Test of Controls***		***Result of Test of Controls***
Control Activities						
				Inspected the security policy acknowledgement for a sample of contractors to determine that all contractors agree to these procedures when hired.		No exceptions noted
Logical and Physical Access						
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.*		CC6.1.1 Administrator access to DigitalOcean is restricted to appropriate personnel.		Inspected the list of users with administrator access to the DigitalOcean environment to determine that access was restricted to appropriate personnel.		No exceptions noted
		CC6.1.2 Role-based security is in place for internal and external Pequity users.		Inspected Pequity configurations to determine that role-based security was in place for internal and external Pequity users.		No exceptions noted
		CC6.1.3 DigitalOcean roles are configured to restrict permissions to cloud resources to appropriate personnel.		Inspected DigitalOcean role assignments to determine if permissions to cloud resources were restricted to appropriate personnel.		No exceptions noted

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.*		CC6.2.1 Prior to granting newly hired employees' access to system resources, HR must submit a completed access request form.		Inspected access request form samples for new employees hired during the period to determine access requires forms were completed by HR, prior to granting newly hired employees' access to system resources.		No exceptions noted
		CC6.2.2 A termination checklist is completed to ensure that system access, including physical access, for terminated employees has been removed.		Inspected the termination checklist for a sample of employees for the infrastructure provider to determine that access is limited to authorized personnel and removed when appropriate.		N/A- Non- Occurrence (No terminations during the period)

Trust Services Criteria for the Security Category		***Description of Pequity Controls***		***Service Auditor Test of Controls***		***Result of Test of Controls***
Logical and Physical Access						
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.*		CC6.3.1 An administrator must approve new-employee access to the infrastructure provider, and access is restricted to authorized personnel. Access approval and modification to access list are logged. Access is removed when appropriate.		Inspected access lists for the infrastructure provider to determine that access is limited to authorized personnel and removed when appropriate.		No exceptions noted

CC6.4 *The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.*		CC6.4.1 Pequity relies on DigitalOcean physical and environmental controls, as defined and tested within DigitalOcean and AWS SOC 2 efforts.		Not Applicable - Control is Carved Out		The Criterion is carved out and the responsibility of the subservice organization (Digital Ocean and 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.*		CC6.5.1 Procedures are in place to identify data and software stored on equipment to be disposed of and to render such data and software unreadable.		Inspected the Data Deletion Policy to determine that procedures are in place to identify data and software stored on equipment to be disposed of and to render such data and software unreadable.		No exceptions noted
CC6.6 *The entity implements logical access security measures to protect against threats from sources outside its system boundaries.*		CC6.6.1 Inbound and outbound traffic to DigitalOcean is appropriately restricted.		Inspected VPC firewall rules to determine that inbound and outbound traffic to DigitalOcean was appropriately restricted.		No exceptions noted

Trust Services Criteria for the Security Category		***Description of Pequity Controls***		***Service Auditor Test of Controls***		***Result of Test of Controls***
Logical and Physical Access						
		CC6.6.2 DigitalOcean cloud firewalls are in place to protect Pequity from outside threats.		Inspected the DigitalOcean cloud firewalls configurations to determine it was appropriately deployed and was configured to appropriately block malicious traffic.		No exceptions noted

		CC6.6.3 Multi-factor authentication (MFA) is required to access the DigitalOcean Management Console.		Inspected DigitalOcean Management Console configurations to determine that MFA was required in order to access DO.		No exceptions noted
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.*		CC6.7.1 Pequity uses HTTPS to encrypt communications over the internet.		Inspected the Pequity login page and obtained the website certificate to determine that a valid certificate was in place.		No exceptions noted
		CC6.7.2 Customer data at rest is encrypted.		Inspected encryption configurations for data at rest to determine that customer data at rest was encrypted.		No exceptions noted
		CC6.7.3 Full-disk encryption is implemented for all workstations and laptops.		Inspected workstation and laptop encryption settings to determine that full-disk encryption was implemented for all workstations and laptops.		No exceptions noted
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.*		CC6.8.1 Antivirus software is installed on workstations to protect the network against malware.		Inspected antivirus configurations to determine that antivirus software was installed on workstations and servers to protect the network against malware.		No exceptions noted

Trust Services Criteria for the Security Category		***Description of Pequity Controls***		***Service Auditor Test of Controls***		***Result of Test of Controls***
System Operations						

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.*		CC7.1.1 Web application scans are performed on a quarterly basis to identify vulnerabilities, and management takes action based on the results of the scan.		Inspected the scan results to determine that web application vulnerability scans were performed, and management takes action based on the results of the scan.		No exceptions noted
		CC7.1.2 Web application penetration tests, that include testing for the OWASP top-ten vulnerabilities, are performed by an independent third party on an annual basis and management takes action, as necessary, based on the results of scans.		Inspected the web application penetration test and remediation report results to determine that a web application penetration test, that included testing for the OWASP top-ten vulnerabilities, was performed by an independent third party. Management takes action, as necessary, based on the results of the testing.		No exceptions noted
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.*		CC7.2.1 Version control software is used to manage source code, track changes to source code, and roll back changes following an unsuccessful implementation.		Inspected the version control software to determine that version control software was used to manage source code, track changes to source code, and roll back changes following an unsuccessful implementation.		No exceptions noted
		CC7.2.2 Access to the cloud source code version control system is restricted to appropriate personnel.		Inspected the version control tool configurations to determine that access was restricted to appropriate personnel.		No exceptions noted

Trust Services Criteria for the Security Category	*Description of Pequity Controls*	*Service Auditor Test of Controls*	*Result of Test of Controls*
System Operations			
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.*	CC7.3.1 The incident response team follows defined incident response procedures for resolving, and escalating reported security issues.	Inspected a sample of incident response tickets to determine that policies and procedures related to resolving, and escalating reported security issues were in place.	N/A - Non-Occurrence (No security incidents during the period)
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.*	CC7.4.1 The incident response team follows defined incident response procedures for resolving and escalating reported security issues.	Inspected a sample of incident response tickets to determine that policies and procedures related to resolving and escalating reported security issues were in place.	N/A - Non-Occurrence (No security incidents during the period)
CC7.5 *The entity identifies, develops, and implements activities to recover from identified security incidents.*	CC7.5.1 Business and system recovery plans are documented, which provide roles and responsibilities and detailed procedures for recovery of systems to a known state per defined recovery time objectives (RTOs) and recovery point objectives (RPOs). Plans are tested annually.	Inspected business and system recovery plans to determine that business and system recovery plans were documented and included roles and responsibilities and detailed procedures for recovery of systems to a known state per defined RTOs and RPOs.	No exceptions noted
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.*	CC8.1.1 A software development life cycle policy is defined to ensure that appropriate controls are in place over the acquisition, development, and maintenance of technology and its infrastructure.	Inspected the software development life cycle policy to determine that a software development life cycle policy was defined to ensure that appropriate controls were in place over the acquisition, development, and maintenance of technology and its infrastructure.	No exceptions noted

		CC8.1.2 Version control software is used to manage source code, track changes to source code, and roll back changes following an unsuccessful implementation.		Inspected the version control software to determine that version control software was used to manage source code, track changes to source code, and roll back changes following an unsuccessful implementation.		No exceptions noted

Trust Services Criteria for the Security Category		***Description of Pequity Controls***		***Service Auditor Test of Controls***		***Result of Test of Controls***
Change Management						
		CC8.1.3 Access to the cloud source code version control system is restricted to appropriate personnel.		Inspected the list of users with access to the cloud source code version control system to determine that access was restricted to appropriate personnel.		No exceptions noted
		CC8.1.4 Code changes to Pequity are tested prior to implementation.		Inspected code change listing detail to determine that code changes were tested prior to implementation.		No exceptions noted
		CC8.1.5 Pequity releases are approved by appropriate personnel prior to the release being implemented in production.		Inspected code change listing detail to determine that releases were approved by appropriate personnel prior to the release being implemented in production.		No exceptions noted
Risk Mitigation						
CC9.1 *The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.*		CC9.1.1 The entity has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.		Inspected the risk assessment policy to determine that the entity had a defined, formal risk management process that specified risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.		No exceptions noted
		CC9.1.2 A risk assessment is performed on an annual basis to identify and rank potential threats to the system.		Inspected the risk assessment to determine that a risk assessment was completed during the period and identified and ranked potential threats to the system.		No exceptions noted

		CC9.1.3 Pequity has created a business continuity plan to define the criteria for continuing business operations for the organization in the event of a disruption.		Inspected Pequity's Business Continuity Plan to determine that it defined an operational and organizational strategy in the event of a disruption and has been updated in the past year.		No exceptions noted
CC9.2 *The entity assesses and manages risks associated with vendors and business partners.*		CC9.2.1 The Pequity team collects and reviews the SOC reports of its sub- service organizations on an annual basis.		Inspected the written policy governing the use of external service providers to determine that the sub-service organization approval process includes collecting and reviewing the provider's SOC report(s).		No exceptions noted

Trust Services Criteria for the Security Category		***Description of Pequity Controls***		***Service Auditor Test of Controls***		***Result of Test of Controls***
Risk Mitigation						
		CC9.2.2 Pequity has implemented a Vendor Risk Management program with a framework for managing the lifecycle of vendor relationships.		Inspected the vendor review to determine that security documentation, including SOC 2 reports, are collected from sub- service organizations and key vendors.		No exceptions noted

Trust Services Criteria for Availability		***Description of Pequity Controls***		***Service Auditor Test of Controls***		***Result of Test of Controls***
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*		A1.1.1 Cloud infrastructure is monitored through DigitalOcean monitoring that sends alerts to appropriate personnel. Corrective actions are performed, as necessary, in a timely manner		Inspected cloud infrastructure monitoring configurations and monitoring rulesets from DigitalOcean monitoring to determine that cloud infrastructure was monitored, and alerts would be sent based on predefined rulesets.		No exceptions noted

to help meet its objectives.						
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.*		A1.2.1 Pequity relies on DigitalOcean's physical and environmental controls, as defined and tested within the DigitalOcean and AWS SOC 2 reports.		Not Applicable - Control is Carved Out		The Criterion is carved out and the responsibility of the subservice organization (Digital Ocean and AWS).
A1.3 *The entity tests recovery plan procedures supporting system recovery to meet its objectives.*		A1.3.1 Backups are performed daily and retained in accordance with a pre-defined schedule in the Backup Policy.		Inspected the database configuration to determine that backups are made daily using the infrastructure provider's automated backup service.		No exceptions noted

Trust Services Criteria for Confidentiality		***Description of Pequity Controls***		***Service Auditor Test of Controls***		***Result of Test of Controls***
Additional Criteria for Confidentiality						
C1.1 *The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.*		C1.1.1 The entity establishes written policies related to retention periods for the confidential information it maintains.		Inspected the data retention policy to determine that the entity established written policies related to retention periods for the confidential information it maintains.		No exceptions noted
		C1.1.2 The entity has established a data classification policy in order to identify the types of confidential information possessed by the entity and types of protection that are required.		Inspected the data classification policy to determine that the entity had established a data classification policy in order to identify the types of confidential information possessed by the entity and types of protection that were required.		No exceptions noted

C1.2 *The entity disposes of confidential information to meet the entity's objectives related to confidentiality.*		C1.2.1 Formal policies and procedures are in place to guide personnel in the disposal of paper documents containing sensitive data.		Inspected the data disposal policy to determine that formal policies and procedures were in place to guide personnel in the disposal of paper documents containing sensitive data.		No exceptions noted
		C1.2.2 Formal policies and procedures are in place to guide personnel in the disposal of paper documents containing sensitive data.		Inspected the data disposal policy to determine that formal policies and procedures were in place to guide personnel in the disposal of hardware containing sensitive data.		No exceptions noted