AdvicePay, Inc.

Type II System and Organization Controls Report (SOC 2)

Report on a Service Organization's Description of Its System and on the Suitability of the Design and Operating Effectiveness of Its Controls Relevant to Security and Availability Throughout the Period June 1, 2020, to September 30, 2020.

KirkpatrickPrice

4235 Hillsboro Pike
Suite 300
Nashville, TN 37215

TABLE OF CONTENTS

SECTION I:
ASSERTION OF ADVICEPAY, INC. MANAGEMENT

ASSERTION OF ADVICEPAY, INC. MANAGEMENT

We have prepared the accompanying description in section III titled "AdvicePay, Inc.'s Description of Its Payment Processing Gateway Services System" throughout the period June 1, 2020, to September 30, 2020, (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 payment processing gateway services system that may be useful when assessing the risks arising from interactions with AdvicePay, Inc.'s system, particularly information about system controls that AdvicePay, Inc. 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 and availability (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*).

AdvicePay, Inc. uses Amazon Web Services for cloud hosting, Stripe for Internet credit card payment services, and HelloSign for eSignatures. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at AdvicePay, Inc., to achieve AdvicePay, Inc.'s service commitments and system requirements based on the applicable trust services criteria. The description presents AdvicePay, Inc.'s controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of AdvicePay, Inc.'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 AdvicePay, Inc., to achieve AdvicePay, Inc.'s service commitments and system requirements based on the applicable trust services criteria. The description presents AdvicePay, Inc.'s controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of AdvicePay, Inc.'s controls.

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

a. the description presents AdvicePay, Inc.'s payment processing gateway services system that was designed and implemented throughout the period June 1, 2020, to September 30, 2020, in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period June 1, 2020, to September 30, 2020, to provide reasonable assurance that AdvicePay, Inc.'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 organizations and user entities applied the complementary controls assumed in the design of AdvicePay, Inc.'s controls throughout that period.

c. the controls stated in the description operated effectively throughout the period June 1, 2020, to September 30, 2020, to provide reasonable assurance that AdvicePay, Inc.'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 AdvicePay, Inc.'s controls operated effectively throughout that period.

SECTION II:
INDEPENDENT SERVICE AUDITOR'S REPORT

Alan Moore
CEO
AdvicePay Inc.
24 E. Main St.
Bozeman, MT 59715

Scope

We have examined AdvicePay, Inc.'s accompanying description in section III titled "AdvicePay, Inc.'s Description of Its Payment Processing Gateway Services System" throughout the period June 1, 2020, to September 30, 2020, (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 June 1, 2020, to September 30, 2020, to provide reasonable assurance that AdvicePay, Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (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*).

Due to the global pandemic declared by the World Health Organization on March 11, 2020, physical and environmental controls were tested using virtual and remote video technologies.

AdvicePay, Inc. uses Amazon Web Services for cloud hosting, Stripe for Internet credit card payment services, and HelloSign for eSignatures. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at AdvicePay, Inc., to achieve AdvicePay, Inc.'s service commitments and system requirements based on the applicable trust services criteria. The description presents AdvicePay, Inc.'s controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of AdvicePay, Inc.'s controls. The description does not disclose the actual controls at the subservice organizations. 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 AdvicePay, Inc., to achieve AdvicePay, Inc.'s service commitments and system requirements based on the applicable trust services criteria. The description presents AdvicePay, Inc.'s controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of AdvicePay, Inc.'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

AdvicePay, Inc. 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 AdvicePay, Inc.'s service commitments and system requirements were achieved. In section I, AdvicePay, Inc. has provided its assertion titled "Assertion of AdvicePay, Inc. Management" (assertion) about the description and the suitability of the design and operating effectiveness of controls stated therein. AdvicePay, Inc. 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 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 or operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of those tests are presented in section IV, "Trust Services Categories, Criteria, Related Controls, and Tests of Controls," of this report in columns 2, 3, and 4, respectively.

Opinion

In our opinion, in all material respects,

a. the description presents AdvicePay, Inc.'s payment processing gateway services system that was designed and implemented throughout the period June 1, 2020, to September 30, 2020, in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period June 1, 2020, to September 30, 2020, to provide reasonable assurance that AdvicePay, Inc.'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 organizations and user entities applied the complementary controls assumed in the design of AdvicePay, Inc.'s controls throughout that period.

c. the controls stated in the description operated effectively throughout the period June 1, 2020, to September 30, 2020, to provide reasonable assurance that AdvicePay, Inc.'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 AdvicePay, Inc.'s controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in section IV, is intended solely for the information and use of AdvicePay, Inc., user entities of AdvicePay, Inc.'s payment processing gateway services system during some or all of the period June 1, 2020, to September 30, 2020, business partners of AdvicePay, Inc. subject to risks arising from interactions

with the payment processing gateway services 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
- 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.

Joseph Kirkpatrick
CPA, CISSP, CGEIT, CISA, CRISC, QSA
4235 Hillsboro Pike, Suite 300
Nashville, TN 37215

November 13, 2020

SECTION III:
ADVICEPAY, INC.'S DESCRIPTION OF ITS PAYMENT PROCESSING GATEWAY SERVICES SYSTEM

SERVICES PROVIDED

AdvicePay, Inc. (AdvicePay) provides a software-as-a-service (SaaS) platform that allows financial planners to bill clients for its services and to receive payment through the platform. The organization charges the financial planners based on the type of organization and includes a fee per month, per user, and per credit card or Automated Clearing House (ACH) transaction. The product also includes the ability to e-sign documents.

AdvicePay is the first compliant billing solution for financial planners implementing the fee-for-service model that wants to get paid via ACH, debit card, or credit card by its clients. AdvicePay allows advisors to get paid efficiently and compliantly. AdvicePay provides advisors and their clients with an AdvicePay portal to view their billing history, upcoming payments, etc. Advisors can bill clients once or continuously. AdvicePay offers eSignature functionality built into the app and a fee calculator to help advisors determine their fees and tie those to the invoice being sent to a client. AdvicePay also offers customizable settings to both advisors and their clients.

Regulatory Commitments

The Gramm-Leach-Bliley Act (GLBA) is the only industry requirement that impacts AdvicePay operations. The organization designs its security programs and business operations, specifically its privacy and data safeguard rules, to maintain compliance with industry expectations and regulatory commitments.

Contractual Commitments

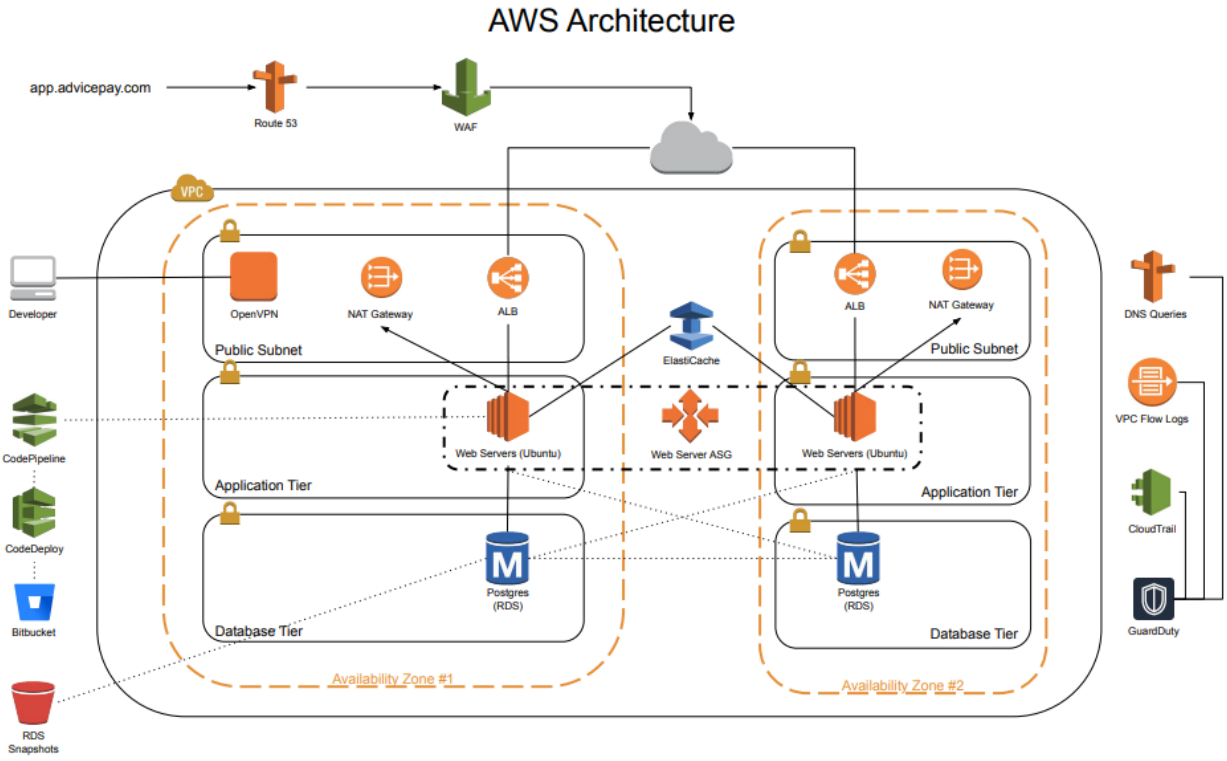
The Standardized AdvicePay SaaS Agreement defines the agreed-upon services between AdvicePay and its clients. Within the contract, terms of service-level agreements (SLAs) for commercial clients are detailed, and information for system uptime and the service level credit for each category is defined. Also included is information on operational security, fees and payments, and non-disclosure agreements (NDAs). The SLAs communicated to commercial clients include best effort technical support with listed response and restoration times.

System Design

AdvicePay designs its payment processing gateway services system to meet its regulatory and contractual commitments. These commitments are based on the services that AdvicePay provides to its clients, the laws and regulations that govern the provision of those services, and the financial, operational, and compliance requirements that AdvicePay has established for its services. AdvicePay establishes operational requirements in its system design that support the achievement of its regulatory and contractual commitments. These requirements are communicated in AdvicePay's system policies and procedures, system design documentation, and contracts with clients.

Infrastructure

The company documents its network design to show how the office location communicates and shares resources from the Amazon Web Services (AWS) cloud environment and how it is protected and segmented using firewalls. To outline the topology of its network, the organization maintains the network diagram below to illustrate its internal infrastructure and describes the connectivity of the production environments. Development Operations, specifically the Lead DevOps, is responsible for maintenance of the diagram. The diagram is reviewed and updated for accuracy annually and upon significant change. The diagram illustrates two orange circles that are the two availability zones in AWS, and the outside perimeter represents services external to the core systems.



The organization uses Stripe, a third-party payment company, to process payments. The organization sends the card data directly to Stripe from the website and does not store, process, or transmit it (other than the procedure call).

The organization maintains an inventory of production systems and end user systems. The AWS inventory is based on EC2, and the inventory shows the current environment.

Software

AdvicePay has documented a list of critical software used for business operations. The inventory is a full list of software that has been approved by management. The list shows the software name,

vendor, description, owner, department, administrator, whether it contains customer data, and the type of system for hosting it.

People

The organization has a traditional hierarchy reporting structure with the CEO having oversight. The Chief Information Security Officer (CISO) reports to the Managing Director and does not have reporting conflicts. The organizational structure is illustrated in the organization chart below.

AdvicePay is governed by a board of directors. The board has full oversight of the business and decision making and has organizational independence. The board acts independently and maintains a committee for the oversight of audits.

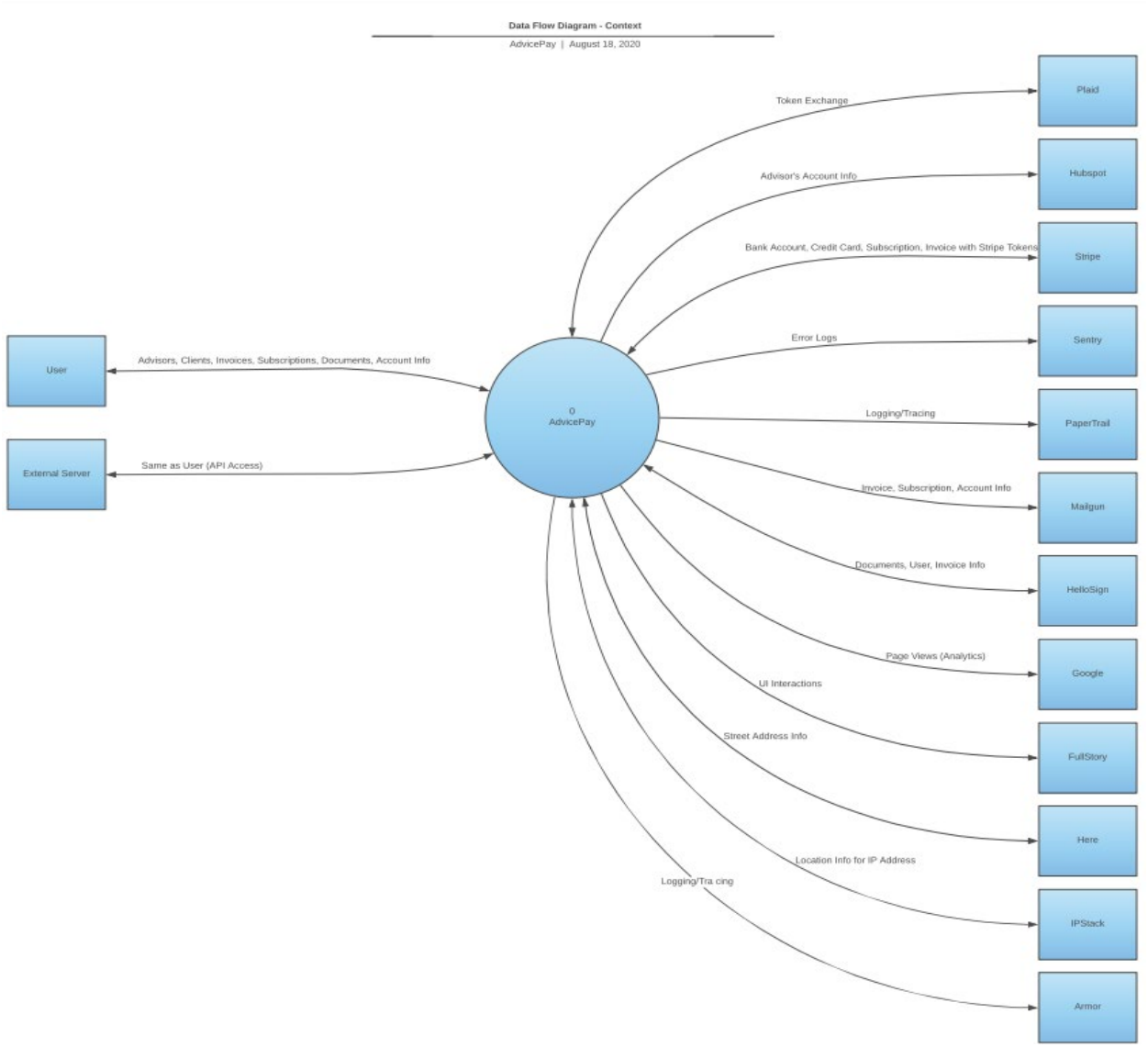
Data

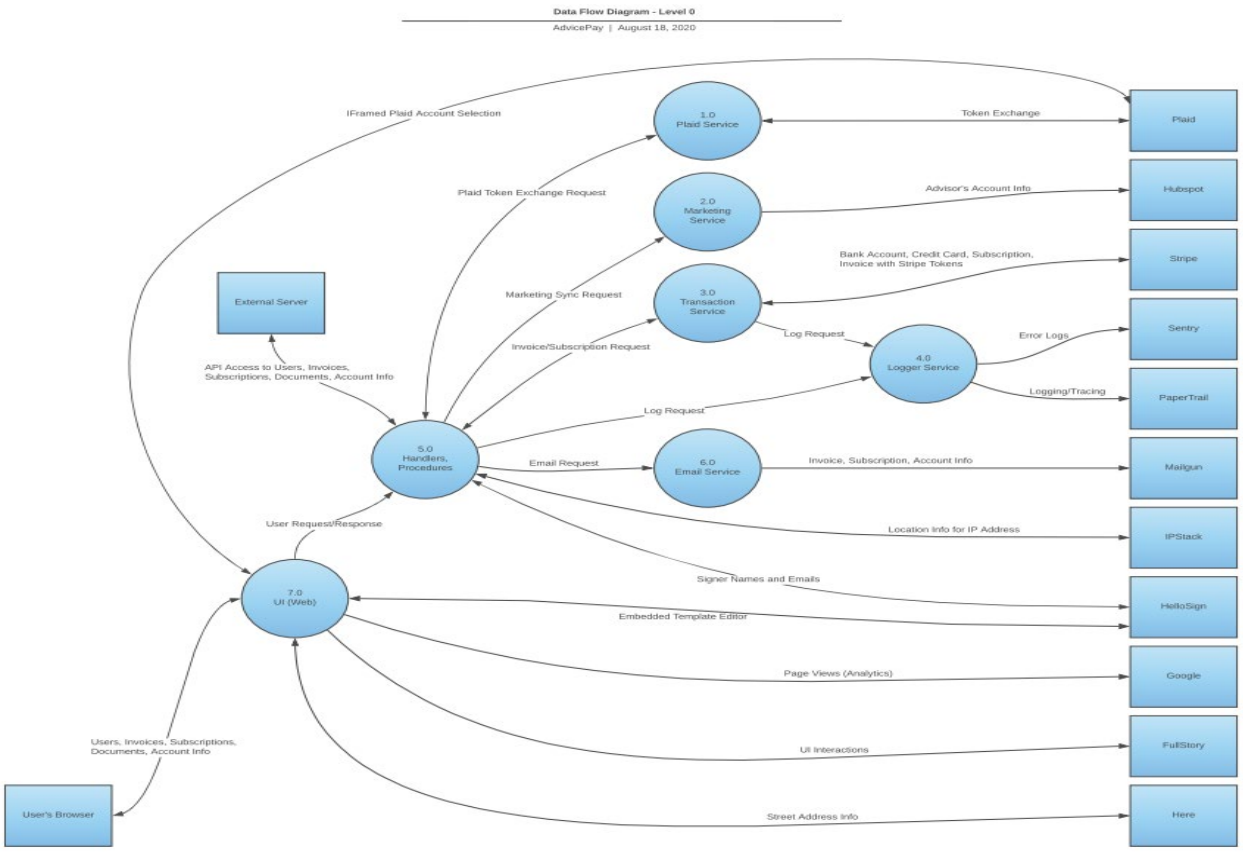
Financial planners can enter limited amounts of data for billing their client and for eSignatures into the AdvicePay application. The organization uses some personally identifiable information such as name, email address, and information related to invoices, subscriptions, fees, etc. Credit card and ACH information is posted directly to Stripe and Plaid, and only a token is returned to be used for future payment processing. Within the AdvicePay application, the only personally identifiable information (PII) data stored is the customer/client name and email address. All other types of information are related to the AdvicePay services and do not contain PII. These other types of information include invoices, subscriptions, fees, user info, etc.

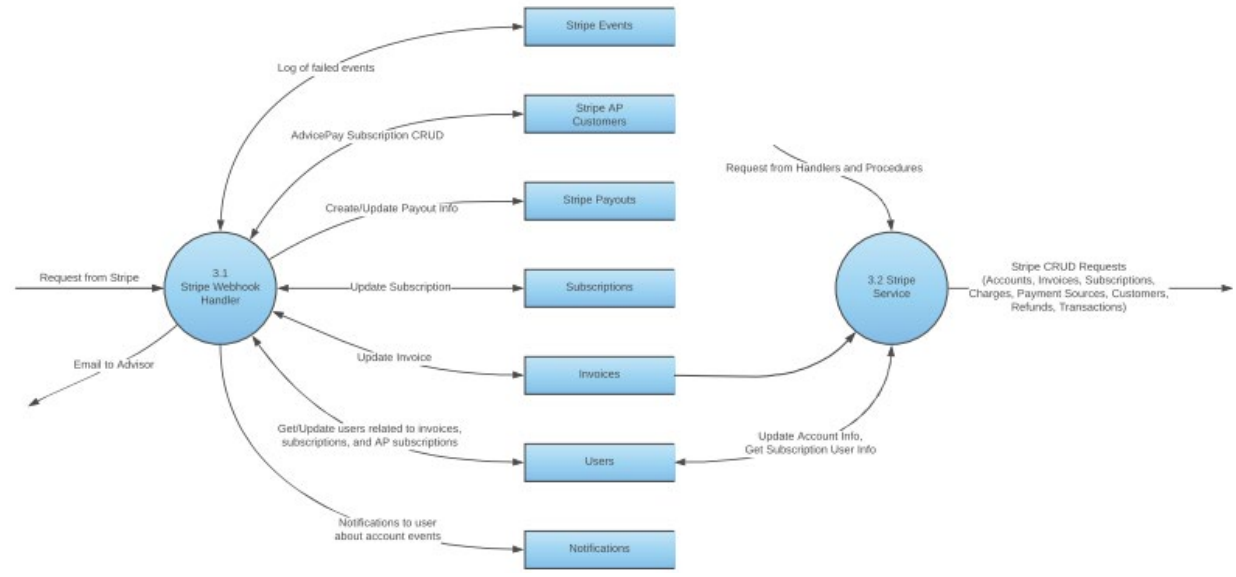
The organization maintains diagrams describing data movement in the environment. The diagrams describe the connections and data movement to services outside of the application including other SaaS solutions. These diagrams are included below.

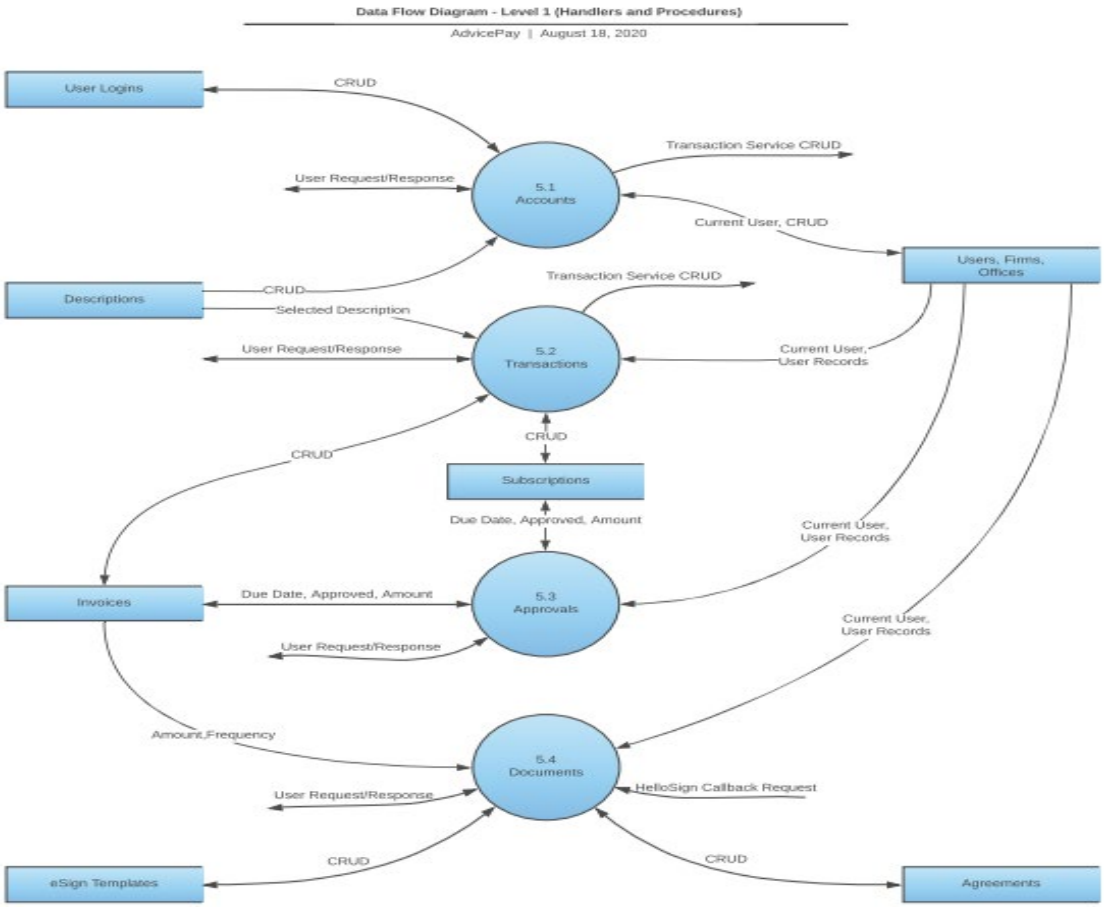
All AdvicePay systems and applications are hosted in the cloud, including Google Drive, Google Gmail, AWS, and a variety of other supporting applications. Passwords are securely stored based on the specific vendor's standards, like Google G Suite, which stores passwords using a hash function on systems that are encrypted.

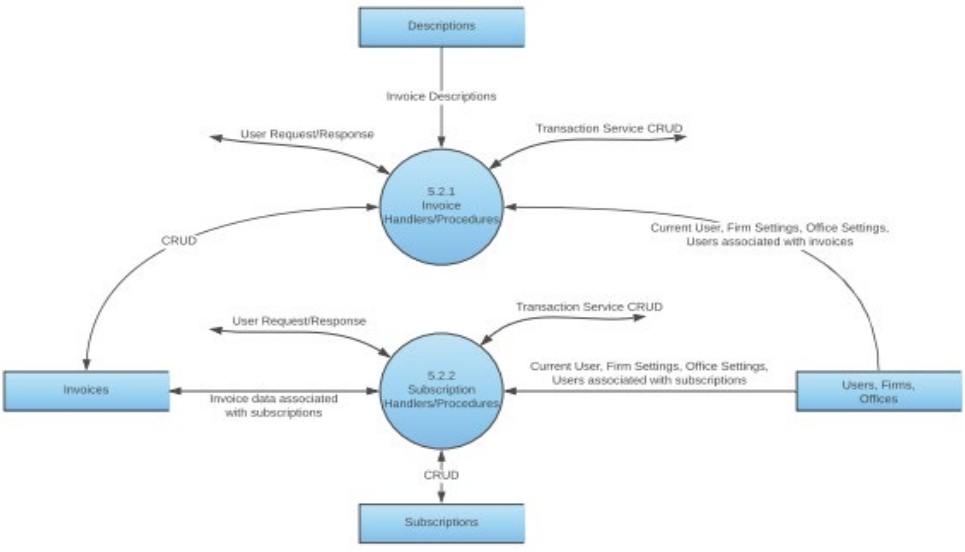
TLS 1.2 is used for data in transit, and the ciphers are automatically negotiated between the client and load balancer. AdvicePay application data is encrypted at rest using AES 256-bit encryption, and AdvicePay application passwords are encrypted using bcrypt with 128-bit salt, all following bcrypt best practices.

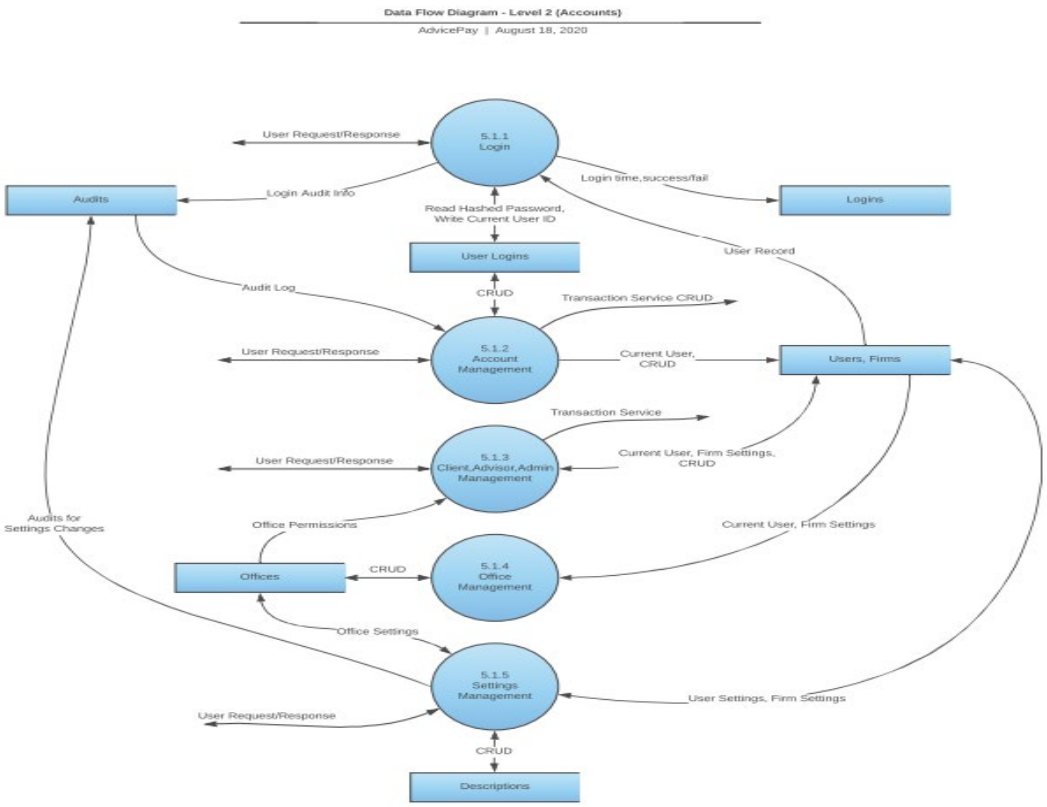


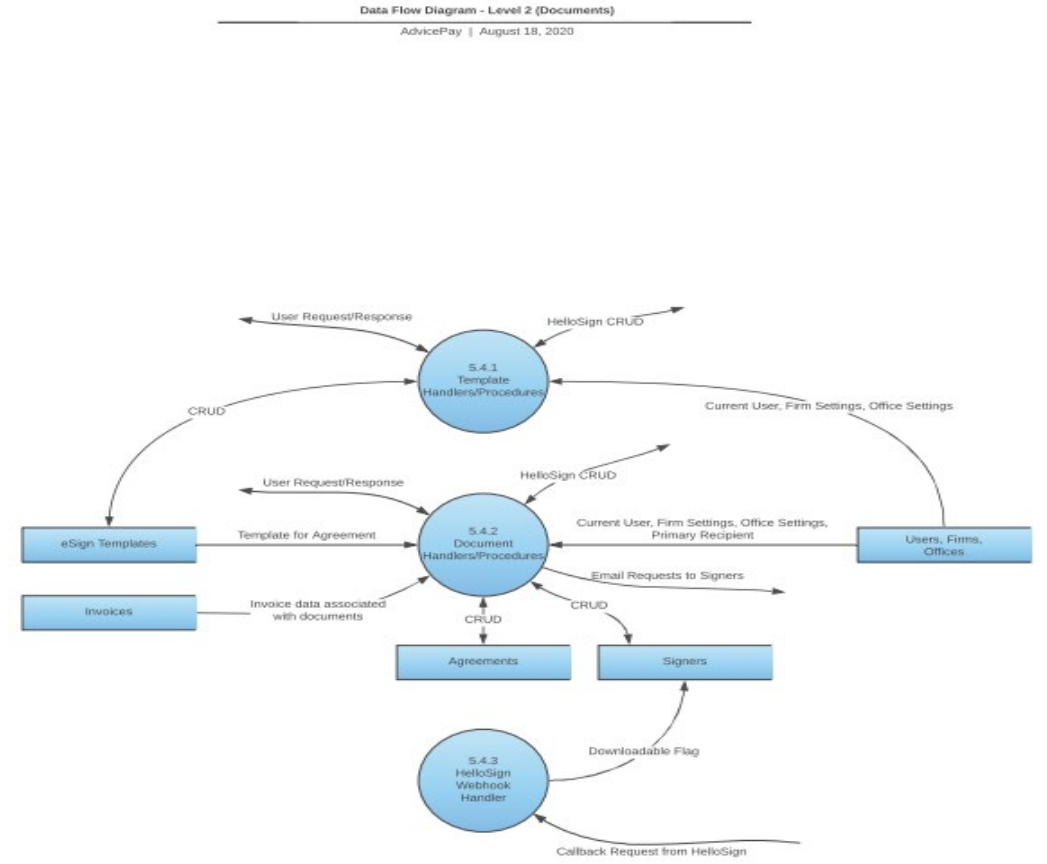

Data Flow Diagram - Level 0
AdvicePay | August 18, 2020
IFramed Plaid Account Selection
1.0 Plaid Service
Token Exchange
Plaid
Plaid Token Exchange Request
2.0 Marketing Service
Advisor's Account Info
Hubspot
Bank Account, Credit Card, Subscription, Invoice with Stripe Tokens
Stripe
External Server
Marketing Sync Request
3.0 Transaction Service
Log Request
4.0 Logger Service
Error Logs
Sentry
Invoice/Subscription Request
API Access to Users, Invoices, Subscriptions, Documents, Account Info
Logging/Tracing
PaperTrail
Log Request
5.0 Handlers, Procedures
Email Request
6.0 Email Service
Invoice, Subscription, Account Info
Mailgun
Location Info for IP Address
IPStack
User Request/Response
Signer Names and Emails
7.0 UI (Web)
Embedded Template Editor
HelloSign
Page Views (Analytics)
Google
Users, Invoices, Subscriptions, Documents, Account Info
UI Interactions
FullStory
User's Browser
Street Address Info
Here


Data Flow Diagram - Level 1 (Transaction Service)
AdvicePay | August 18, 2020
Stripe Events
Log of failed events
Stripe AP Customers
AdvicePay Subscription CRUD
Request from Handlers and Procedures
Stripe Payouts
Create/Update Payout Info
Request from Stripe
3.1 Stripe Webhook Handler
Update Subscription
Subscriptions
3.2 Stripe Service
Stripe CRUD Requests (Accounts, Invoices, Subscriptions, Charges, Payment Sources, Customers, Refunds, Transactions)
Email to Advisor
Update Invoice
Invoices
Get/Update users related to invoices, subscriptions, and AP subscriptions
Update Account Info, Get Subscription User Info
Users
Notifications to user about account events
Notifications


Data Flow Diagram - Level 1 (Handlers and Procedures)
AdvicePay | August 18, 2020
User Logins
CRUD
5.1
Accounts
Transaction Service CRUD
User Request/Response
Current User, CRUD
Users, Firms, Offices
Descriptions
CRUD
Selected Description
Transaction Service CRUD
5.2
Transactions
User Request/Response
Current User, User Records
CRUD
Subscriptions
Due Date, Approved, Amount
Current User, User Records
Invoices
Due Date, Approved, Amount
5.3
Approvals
User Request/Response
Current User, User Records
Amount,Frequency
5.4
Documents
User Request/Response
HelloSign Callback Request
CRUD
CRUD
eSign Templates
Agreements


Data Flow Diagram - Level 2 (Transactions)
AdvicePay | August 18, 2020
Descriptions
Invoice Descriptions
User Request/Response
Transaction Service CRUD
5.2.1
Invoice
Handlers/Procedures
CRUD
Current User, Firm Settings, Office Settings, Users associated with invoices
User Request/Response
Transaction Service CRUD
Invoices
Invoice data associated with subscriptions
5.2.2
Subscription
Handlers/Procedures
Current User, Firm Settings, Office Settings, Users associated with subscriptions
Users, Firms, Offices
CRUD
Subscriptions


Data Flow Diagram - Level 2 (Accounts)
AdvicePay | August 18, 2020
User Request/Response
5.1.1 Login
Audits
Login Audit Info
Login time,success/fail
Logins
Read Hashed Password, Write Current User ID
User Logins
User Record
CRUD
Audit Log
Transaction Service CRUD
User Request/Response
5.1.2 Account Management
Current User, CRUD
Users, Firms
Transaction Service
User Request/Response
5.1.3 Client,Advisor,Admin Management
Current User, Firm Settings, CRUD
Audits for Settings Changes
Office Permissions
Current User, Firm Settings
Offices
CRUD
5.1.4 Office Management
Office Settings
5.1.5 Settings Management
User Settings, Firm Settings
User Request/Response
CRUD
Descriptions


Data Flow Diagram - Level 2 (Documents)
AdvicePay | August 18, 2020
User Request/Response
HelloSign CRUD
5.4.1 Template Handlers/Procedures
CRUD
Current User, Firm Settings, Office Settings
HelloSign CRUD
User Request/Response
eSign Templates
Template for Agreement
5.4.2 Document Handlers/Procedures
Current User, Firm Settings, Office Settings, Primary Recipient
Users, Firms, Offices
Email Requests to Signers
Invoices
Invoice data associated with documents
CRUD
CRUD
Agreements
Signers
Downloadable Flag
5.4.3 HelloSign Webhook Handler
Callback Request from HelloSign

Processes and Procedures

Management has developed and communicated procedures to guide the provision of the organization's services. Changes to procedures are performed annually and authorized by management. These procedures cover the following key security life cycle areas:

- Data classification
- Categorization of information
- Assessment of the business impact resulting from proposed security approaches
- Selection, documentation, and implementation of security controls
- Performance of annual management self-assessments to assess security controls
- Authorization, changes to, and termination of information system access
- Monitoring security controls
- Management of access and roles
- Maintenance and support of the security system and necessary backup and offline storage
- Incident response
- Maintenance of restricted access to system configurations, user functionality, master passwords, powerful utilities, and security devices

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION, AND MONITORING

The security and availability categories and applicable trust services criteria were used to evaluate the suitability of design and operating effectiveness of controls stated in the description. Security and availability criteria and controls designed, implemented, and operated to meet them ensure that the system is protected against unauthorized access (both physical and logical). The controls supporting the applicable trust services security and availability criteria are included in section IV of this report. Although the applicable trust services criteria and related controls are included in section IV, they are an integral part of AdvicePay's description of its payment processing gateway services system.

Control Environment

Management Philosophy

Management's communication within meetings and policies set the tone and direction for the entire organization. Monthly all-hands meetings are used by the CEO to communicate personnel changes, goals and success metrics, projects, and other corporate initiatives. Additionally, the entire Dream Team Handbook is reviewed by the Managing Director with each new hire during their first week. It communicates the organization's integrity and ethics expectations. As there are changes to the policy, they are rolled out to the entire team via Slack and in the company's monthly all-hands meetings. A separate all-team training takes place when larger changes occur.

Security and Availability Management

The organization's security and availability requirements are managed using a combination of documented policies and procedures, management oversight, and network systems and hardware. These management practices are implemented in all areas of the control environment to protect systems, data, and personnel and to ensure compliance with industry best practices and standards.

Security and Availability Policies

All updates made to AdvicePay's policies are made by the Managing Director and CEO. Any proposed changes can be communicated to the Managing Director. The CEO then reviews them for consideration, in which only the CEO may approve such proposed changes. Updates and changes are tracked within the revision log for documentation and reference.

Personnel Security

The organization maintains an employee handbook that provides controls related to personnel security. All employees are required to acknowledge the policy, which is titled the AdvicePay Dream Team Handbook.

The organization has established processes for the hiring and termination of employees. Recruitee is used to manage the search function. An interview and testing process are used to select the most competent potential employee. Management meets to select from the finalists.

Forms are used for recording the steps in the hiring process which includes background checks and departmental notifications. Background checks are conducted before an employment offer is extended. GoodHire is used for executing background checks, and the following are verified:

- Social Security Trace
- National Criminal Records Check
- Sex Offender List
- Domestic Watch List
- County Criminal Court Checks for Counties of Residence for past seven years

Termination procedures are also defined within the Employee Handbook. Team members with performance issues are placed on a performance improvement plan (PIP), documenting the issues, what needs to be improved and by when, and the consequences if the necessary changes do not occur. Violations of the organization's Anti-Harassment, Relationship, and PR/Communication Policies are also grounds for termination, as detailed in the Personal Conduct Policy of the handbook. A separation form, offboarding checklist, additional offboarding checklist for developers, and PIP (coaching/discipline) form are all used to ensure consistency when completing the offboarding process.

The organization communicates training requirements within the Dream Team Handbook and the Technology and Security Operations. Security awareness training for all employees is required at hire and annually, as is the reimbursement program for job-related training.

Physical Security and Environmental Controls

Due to travel restrictions related to COVID-19, the auditor was unable to physically observe security controls in place within the corporate office. Testing was limited to reviews of policies, interviews, and video conference calls with relevant personnel. Interested parties should address concerns with the organization.

AdvicePay, Inc. implements physical access controls for its corporate office facility. AdvicePay rents office space from XY Planning Network (XYPN). XYPN uses an electronic push bar with a proximity security card reader to secure the main entrance to the office. In addition, the wiring closet containing network equipment for wireless access, firewall, and internet are locked in a cage to restrict access. This access is all managed by XYPN's Operation Team.

The office has not been occupied since the start of the pandemic, except for a few XYPN employees, but physical controls that are in place for normal operations include badge access for employees after hours and a visitor log system. The Team visitor access record system by iOFFICE is used to register visitors. There is no video surveillance in the building and no burglar alarms since there are no servers or production systems in the suite.

Regarding environmental controls, the office space has fire suppression included within it and uses a physical security keycard system to restrict entry. All AdvicePay SaaS systems run within AWS and all other systems are cloud-based systems. The only internal infrastructure is a basic network, wireless network, and internet which is rented from XYPN.

Change Management

AdvicePay has an implemented policy in place for change management located within the Technology and Security Operations Policy. The policy covers the AdvicePay application, AWS environment (application systems), Team Member MacBooks, AdvicePay office network, AdvicePay cloud application (where applicable to the degree that AdvicePay has control over these systems). The change management process includes the following:

- Request
- Approval
- Prioritization
- Documentation
- Testing
- Communication
- Implementation
- Rollback
- Provisions for emergency changes

Change requests must be submitted to the appropriate individual for review and approval. If additional approval or review is required, there is an escalation process. All changes must be approved prior to implementation. All change requests are required to be logged whether approved or rejected to document and track the change process. Jira is used for this process. The approval of all change requests and the results should also be documented. This should include change request documentation, change authorization, and the outcome of the change. Final approval of implementation must be made before implementation to ensure testing process, communications, and the rollback plan.

Configuration Management

The organization has documented hardening standards for the production environment. AdvicePay uses "golden" Amazon Machine Images (AMI) for building new instances. Jamf is used to ensure that end user systems are configured consistently. National Institute of Standards and Technology (NIST) and ISO 27001 are used for encryption standards.

AdvicePay's infrastructure is deployed entirely within AWS. The Technology and Security Operations Policy contains the standards for configuring and hardening the AWS environment for hosting the AdvicePay application.

AdvicePay uses the AWS EC2 Virtual Firewall to protect the AdvicePay application EC2 instances from external connections. Security group rules are established within the AWS EC2 Virtual Firewall that control inbound traffic allowed to reach EC2 instances and outbound traffic allowed to leave EC2 instances. Only ports 80 and 443 are allowed into the production network, and all traffic is allowed out.

Application Development

AdvicePay, Inc.'s application suite is developed and maintained by the organization's in-house developers and operations personnel. The roles and responsibilities of developers and operations personnel are defined and appropriately divided to ensure separation of duties. The production

and QA environments are separate. Access to these environments is limited based on job requirements. Roles are defined for Development Operations, Developers, Operations staff, and others. Additionally, all the application server systems are in one subnet, and all the database systems are in another subnet.

AdvicePay uses Git within Bitbucket for version control. Bitbucket Groups are used to control access to the AdvicePay repository, as well as to specific branches within the repository when necessary. The least-privilege model is used when granting access, and only users who need to access the source have any access.

Application Change Management

For application changes, the organization uses its change management policy. Any application change and/or update to the AdvicePay application must be controlled with version control. The final approval of an application change is made after QA testing is completed.

System Monitoring

AdvicePay has implemented multiple processes to monitor the security of its systems. The organization requires annual penetration testing of the external network, annual vulnerability testing of the AdvicePay application and application code, and weekly vulnerability scans are also conducted on application code testing and AWS infrastructure testing. The organization's penetration testing process tests the AdvicePay application and external networks for Open Web Application Security Project (OWASP) vulnerabilities. The following represents the internal testing process of AdvicePay application code:

- Vulnerability test of the AdvicePay application code are performed before each deployment of code to the staging environment
- Golang Security Checker (gosec) and MPM Audit are used to perform vulnerability testing
- Critical and high failures create an exit code in the deployment and sends an email to the development team
- Remediation is performed immediately on all critical and high failures before resubmission to staging
- AdvicePay uses Armor Anywhere to perform routine vulnerability assessments of the AWS infrastructure; Armor Anywhere uses the Rapid7 platform for vulnerability scanning
- Vulnerability scans of the AdvicePay AWS environment are performed each Sunday
- Vulnerability results are delivered to the Armor Management Console reporting on vulnerability and patching with rankings based on the Common Vulnerability Scoring System (CVSS) methodology

AdvicePay remediates all vulnerability findings or performs a risk mitigation if remediation is not possible. AdvicePay uses the following priority scale to determine the remediation process:

- Critical – Vulnerabilities assigned a priority of critical are remediated within 7 days
- High – Vulnerabilities assigned a priority of high are remediated within 7 days. Exception if the vulnerability is mitigated by AWS technical controls, in which case the vulnerability is classified as a priority medium and is remediated within 90 days
- Medium – Vulnerabilities assigned a priority of medium are remediated within 90 days

- Low – Vulnerabilities assigned a priority of low are remediated within 90 days

Constant intrusion detection and prevention system (IDS/IPS) monitoring is conducted using the Armor Anywhere system's IDS/IPS tools along with audit logs for AdvicePay's production system that are exported to Armor's servers. Armor immediately notifies AdvicePay's engineering and security teams of any potential intrusions and vulnerabilities via email. If critical vulnerabilities are detected, immediate corrective action is taken to eliminate them to prevent future intrusion attempts. If legitimate intrusion attempts are encountered, additional filtering rules are written to limit access to the rogue users or systems attempting to access AdvicePay. If an attacker is successful in an intrusion attempt, immediate actions are taken to mitigate data loss/exfiltration, and all affected users are notified as soon as possible after an investigation into the cause and effect of the intrusion.

CloudWatch alarms and auto-scaling groups within AWS are used for capacity determination. The production auto-scaling group has a maximum of three instances available at any given time. Currently, the organization only has a single instance running 99% of the time, and they have never had three instances. The system is designed to scale horizontally, so additional capacity can be easily added if necessary.

The AWS environment uses Armor Anywhere for antivirus and malware protection. Updates are performed automatically and routinely. The system continuously checks for updates, and when an update is available it pulls that update down. Bitdefender is used for antivirus and malware protection on laptops. Bitdefender updates daily.

AdvicePay uses AWS VPC Flow Logs to capture IP traffic going to and from network interfaces. All Flow Log traffic is published to CloudWatch. Logging is retained for 13 months. Logging data is classified as Restricted Distribution per the AdvicePay Information Classification Policy.

Problem Management

AdvicePay, Inc. has developed and implemented a formal incident response process for identifying, reporting, containing, analyzing, and eradicating incidents and breaches. AdvicePay's SIRT (Security Incident Response Team) manages, coordinates, and supports incident response for all AdvicePay security incidents. This entails analyzing and resolving events and incidents that end users report and those that staff members discover through proactive network and system monitoring.

Upon discovery of a security incident, one must immediately report the incident to the CISO and Managing Director. Once the incident has been reported, the CISO or Managing Director is responsible for reporting the incident to AdvicePay Executive Management and completing an incident response report. Customers report security incidents to support@advicepay.com.

Data Backup and Recovery

AdvicePay has established a business continuity plan to maintain or restore operations and ensure availability of information at the required level and in the required time following interruption to, or failure of, critical business processes. The Business Continuity Plan is updated yearly by management to assess the current state, new company needs, and expectations.

AdvicePay uses the AWS Backup services to back up the AdvicePay application environment and data. Backup Schedule Automated snapshot backups are performed nightly at 12:00am MT. All backups of the AWS environment are retained for 30 days. Backup restore requests must be approved by the Product Manager or Managing Director before implementing.

All backups are logged within the AWS Backup system. AdvicePay uses the Backupify G Suite 2.0 SaaS backup application to perform backups of all data associated with G Suite including Google Drive, Google Mail, Google Calendar, and Google Contacts. Backups are performed automatically three times daily based on the following schedule:

- Between 12 AM and 8 AM Eastern Standard Time
- Between 8 AM and 4 PM Eastern Standard Time
- Between 4 PM and 11:59 PM Eastern Standard Time

If necessary, on-demand backups can be performed to back up specific data based on business needs. All backups of AdvicePay G Suite applications are retained for one year. Requests for data restores from backups must be approved by the CISO or Managing Director. Restricted and confidential data are handled based on information classification and handling policies. All backups are logged automatically by Backupify.

System Account Management

Multiple controls have been implemented to regulate and manage all system accounts connected to AdvicePay's systems. All users must be assigned a unique user before being given access to AdvicePay systems, applications, and data. The account creation process is completed by the Managing Director and the CISO. The onboarding checklist guides the account creation process. Accounts are created based on least privilege. The terminations of accounts must take place within 24 hours for voluntary terminations and immediately for involuntary terminations. Change management tickets are used to verify what access was given to ensure that all access is removed. Clients manage their own accounts by self-registering and creating and managing their own users.

Password complexity configurations are defined with the Team Member Security Policy. Passwords must have the following characteristics:

- Contain at least 12 characters
- Cannot contain user's name or user ID
- Be complex
- Contain at least one symbol
- Expire every 180 days (6 months)

Multi-factor authentication (MFA) is required to be used when available. It is required for managing the AWS environment, and Google Authenticator or Authy are used.

Risk Assessment Process

AdvicePay annually performs risk assessments based on the risk register. AdvicePay's Security Risk Management (SRM) program is based on the NIST Risk Register Template. The CISO is

responsible for developing and maintaining AdvicePay's SRM program. The status states the condition of controls for the threat, and confidentiality, integrity, availability, risk likelihood, and risk strategy are analyzed and noted for controls in place or mitigation plans. AdvicePay evaluates risks to determine the appropriate mitigation strategy to assign.

The purpose of the risk mitigation step is to plan the process for controlling, transferring, accepting, or avoiding risks. AdvicePay evaluates risks to determine the appropriate mitigation strategy to assign. AdvicePay acts to control risks by implementing policy, procedures, and technical controls where appropriate. AdvicePay transfers risks to third parties such as AWS. AdvicePay may accept a risk in situations in which it is determined to be a low risk or when there are other factors that reduce the risk. To accept a risk, the CISO creates a risk report to be reviewed and approved by the CEO and the Managing Director. AdvicePay may choose to avoid specific risks in situations in which the level of risk is too high.

Information and Communication Systems

The organization's information security policies are contained within two documents to communicate all expected information security practices to be upheld by its employees. The Technology and Security Policy is intended for the technical staff and the Team Member Security Policy is for all employees and covers information that every employee needs to know. The policies are reviewed annually and comply with all applicable national laws and regulations and contractual obligations. The policies include all necessary topics. The policy is provided to all employees upon hire and required to be acknowledged. The policy is made available to all personnel via the organization's Google Drive.

The organization has a privacy policy for both users of the website and its own employees. One is provided to customers and users of the site and is available on the 'Contact Us' page of the website, while the other is part of the internal security policy and directs employees on the protection of personal client and employee data.

Vendor Management

AdvicePay consistently evaluates, selects, engages, and manages its critical vendors, including AWS, Stripe, and HelloSign, to ensure compliance with its security requirements. The organization uses a standardized AdvicePay SaaS agreement with all critical third-party service providers to define the scope of services and confidentiality expectations. NDAs are also in place for all third parties who have access to AdvicePay's critical data. The organization performs due diligence on all vendors prior to engagements and continues to monitor third-party service delivery once working together.

Monitoring Controls

The company maintains and updates a company scorecard to provide leadership with a report of the state of the company, its key metrics, and the quality of operations and tasks being completed. This Scorecard is updated each week and reviewed in a weekly department head meeting. The scorecard shows number of sprints planned, time on developing features, growth of newsletter list, number of new users, visits to the website, leads, etc.

Changes to the System During the Period

There were no changes that are likely to affect report users' understanding of the payment processing gateway services system during the period from June 1, 2020, through September 30, 2020.

COMPLEMENTARY USER-ENTITY CONTROLS

AdvicePay's services are designed with the assumption that certain controls would be implemented by user organizations. In certain situations, the application of specific controls at the user organization is necessary to achieve control objectives included in this report. AdvicePay's management makes control recommendations to user organizations and provides the means to implement these controls in many instances. AdvicePay also provides best practice guidance to clients regarding control element outside the sphere of AdvicePay responsibility.

This section describes additional controls that should be in operation at user organizations to complement the AdvicePay controls. Client Consideration recommendations include:

- User organizations should implement sound and consistent internal controls regarding general IT system access and system usage appropriateness for all internal user organization components associated with AdvicePay.

- User organizations should practice removal of user accounts for any users who have been terminated and were previously involved in any material functions or activities associated with AdvicePay's services.

- Transactions for user organizations relating to AdvicePay's services should be appropriately authorized, and transactions should be secure, timely, and complete.

- For user organizations sending data to AdvicePay, data should be protected by appropriate methods to ensure confidentiality, privacy, integrity, availability, and non-repudiation.

- User organizations should implement controls requiring additional approval procedures for critical transactions relating to AdvicePay's services.

- User organizations should report to AdvicePay in a timely manner any material changes to their overall control environment that may adversely affect services being performed by AdvicePay.

- User organizations are responsible for notifying AdvicePay in a timely manner of any changes to personnel directly involved with services performed by AdvicePay. These personnel may be involved in financial, technical, or ancillary administrative functions directly associated with services provided by AdvicePay.

- User organizations are responsible for adhering to the terms and conditions stated within their contracts with AdvicePay.

- User organizations are responsible for developing, and if necessary, implementing a business continuity and disaster recovery plan (BCDRP) that will aid in the continuation of services provided by AdvicePay.

The list of user organization control considerations presented above and those presented with certain specified control objectives do not represent a comprehensive set of all the controls that should be employed by user organizations. Other controls may be required at user organizations. Therefore, each client's system of internal controls must be evaluated in conjunction with the internal control structure described in this report.

SECTION IV:
TRUST SERVICES CATEGORIES, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS

Although the applicable trust services criteria and related controls are presented in section IV, "Trust Services Categories, Criteria, Related Controls, and Tests of Controls," they are an integral part of AdvicePay, Inc.'s system description throughout the period June 1, 2020, to September 30, 2020.

Security

The trust services criteria relevant to security address the need for information and systems to be protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the service organization's ability to achieve its service commitments and system requirements.

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 achievement of AdvicePay's service commitments and system requirements. 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

The trust services criteria relevant to availability address the need for information and systems to be available for operation and use to achieve the service organization's service commitments and system requirements.

Availability refers to the accessibility of information used by AdvicePay's systems, as well as the products or services provided to its customers. While the availability objective 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), it does address whether systems include controls to support accessibility for operation, monitoring, and maintenance.

Trust Services Criteria for the Security and Availability Categories			
Control Environment			
Ctrl #	**Description of Controls**	**Service Auditor's Tests of Controls**	**Test Results**
CC1.1	The entity demonstrates a commitment to integrity and ethical values.		
CC1.1.1	The organization has established processes for the hiring and termination of employees.	Reviewed the Hiring Process Checklist, the AP Team Member Offboarding Checklist (dated August 31, 2020), the Developer Offboarding (dated January 14, 2019), the Offboarding Separation Form, and verified that the organization has established processes for the hiring and termination of employees Interviewed the Managing Director and verified the following: • Recruitee is used to manage the search function • An interview and testing process to select the most competent potential employee • Management meets to select from the finalists • Forms are used for recording the steps in the hiring process which includes background checks and departmental notifications Observed the forms used for the hiring of two total employees hired during the audit period and verified that the steps were followed, including background checks, and communications to staff for the creation of accounts and data access Observed the forms used for the termination of one employee terminated during the audit period and verified that the process was followed, and that access was removed	No Relevant Exceptions Noted
CC1.1.2	The organization maintains an employee handbook that all employees are required to acknowledge.	Reviewed the AdvicePay Dream Team Handbook (dated July 2020) and verified that the handbook contains relevant content, including: • Conduct Policy • Background checks	No Relevant Exceptions Noted

		• Revision history • Progressive discipline Interviewed the Managing Director and verified that the handbook is reviewed by upper management and hosted on a Google Drive available to all employees; employees are required to acknowledge the handbook at hire and then annually Observed the Google Drive folder hosting the handbook and verified that all employees have read access Observed the acknowledgements for the two new employees hired during the audit period and 3 of 16 current employees and verified that all have acknowledged the handbook	
CC1.1.3	The Employee Handbook contains a Code of Conduct.	Reviewed the AdvicePay's Dream Team Handbook (dated July 21, 2020) and verified it contains a code of conduct Interviewed the Managing Director and verified that the handbook contains the code of conduct and that employees are required to acknowledge the handbook at hire and then annually thereafter Observed the Google Drive folder hosting the handbook and verified that all employees have read access Observed the acknowledgements for the two new employees hired during the audit period and 3 of 16 current employees and verified that all have acknowledged the handbook, including the code of conduct	No Relevant Exceptions Noted
CC1.1.4	The organization has established processes for the hiring and termination of employees and completes required forms as part of the hiring process.	Reviewed the New Hire Onboarding Checklist, the Offer of Employment, the NDA, Policy Acknowledgement and Laptop Checkout and verified that the organization has established processes for the hiring and termination of employees and	No Relevant Exceptions Noted

		completes the forms as part of the hiring process Interviewed the Managing Director and verified the following: • The forms used for recording the steps in the hiring process which includes background checks and departmental notifications • All employees must sign the NDA, acknowledgements to the Employee Handbook and information security policy • Background checks are performed on all employees prior to starting Observed the forms used for the hiring of all two employees hired during the audit period and verified that the steps were followed, including background checks, and communications to staff for the creation of accounts and data access Observed that the employees had had background checks performed, signed the NDA, and acknowledged the handbook and policies	
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 board had full oversight of the business, decision making, and has organizational independence.	Reviewed the AP Board Rules and Responsibilities document and verified that the roles and responsibilities for the board of directors are defined Reviewed the description of the board of directors and its function and verified that the board acts independently and maintains a committee for the oversight of audits Interviewed the Managing Director and verified that the board has full oversight of the business and decision making and has organizational independence Observed that the board consists of the CEO & Co-Founder, the other Co-	No Relevant Exceptions Noted

		Founder, and a non-executive board member	
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.		
CC1.3.1	The organization has a traditional hierarchy reporting structure with the CEO having oversight.	Reviewed the AP Org Chart (dated August 2020) and verified that the organizational structure shows the relationship of the CISO to management Interviewed the Managing Director regarding the role of the CISO in the organization and verified that the CISO reports to the Managing Director and does not have reporting conflicts Observed the organization chart and verified that the CISO reports to the Managing Director and maintains independence Observed the diagram is up to date Observed the diagram and verified that the organization has a traditional hierarchy reporting structure with the CEO having oversight	No Relevant Exceptions Noted
CC1.3.2	The organization is incorporated in Delaware and operates in Montana as a foreign registered corporation.	Reviewed the Certificate of Incorporation AdvicePay (dated April 28, 2016) and verified that the organization is incorporated in Delaware and operates in Montana as a foreign registered corporation Interviewed the Managing Director and verified that the company was incorporated in Delaware in 2016 but operates in Montana; the board of directors consists of the two founders (one serves as CEO) and one other independent member Reviewed the Secretary of States' websites for Delaware and Montana and verified that the company is incorporated in Delaware and operates in Montana as a foreign corporation	No Relevant Exceptions Noted

CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.		
CC1.4.1	Background checks are conducted before an employment offer is extended.	Reviewed the AdvicePay Dream Team Handbook (dated July 2020) and verified that background checks are conducted before an employment offer is extended and that the background checks include the following: • SSN trace • Criminal Database Search (national and county) • Domestic watchlist search • Sex offender list search Interviewed the Managing Director and verified that background checks are performed on all employees prior to starting and that GoodHire is used for the background checks Observed the two employees hired during the audit period and verified that background checks were performed and included the following: • Social Security Trace • National Criminal Records Check • Sex Offender List • Domestic Watch List • County Criminal Court Checks for Counties of Residence for past seven years	No Relevant Exceptions Noted
CC1.4.2	The Lead Developer reviews blogs for gaining knowledge about configuration management.	Reviewed the blog posts reviewed by the Lead Developer and verified that they provide knowledge about configuration management Interviewed the Lead Developer and verified that the blogs reviewed by him include AWS Security, NIST Cybersecurity Insights, SANS, Cobalt, and Reddit Observed screenshots of each of the blog posts to which the Lead Developer is subscribed and verified his access to the blog posts for security and secure configurations	No Relevant Exceptions Noted

CC1.4.3	The organization requires training upon hire for all employees and annually thereafter.	Reviewed AdvicePay's Dream Team Handbook (dated July 2020) and verified that the company's requirement for training reimbursements and company provided training are detailed Reviewed the Technology and Security Operations document (dated August 11, 2020) and verified that the requirement for new hires to attend policy and security awareness training at hire, and policy-refresher training annually, is documented Reviewed Pluralsight invoices and verified that the organization maintains a subscription for training on coding techniques Interviewed the Managing Director and the CISO and verified that the requirement for security awareness training for all employees at hire and then annually as well as the reimbursement program for job-related training Observed the two new hires and three of 16 current employees and verified that they acknowledged completion of the security awareness training Observed the receipts from Pluralsight for all three application developers and verified that they have subscribed to job competency training for code development	No Relevant Exceptions Noted
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.		
CC1.5.1	All policies require the review of the Managing Director who submits it for approval to the CEO.	Reviewed AdvicePay's Dream Team Handbook (dated July 2020) and the Technology and Security Operations document (dated August 2020) and verified that both documents describe the communication process wherein the Managing Director communicates with the CEO for proposed changes to the Handbook and Policies and the	No Relevant Exceptions Noted

		security policy also details the annual review and update requirements Interviewed the CISO and the Managing Director and verified that the policies are new and that all policies require the review of the Managing Director, who submits it for approval to the CEO; changes are tracked in the tables within the documents Observed the policies and the handbook and verified that the policies are current and contain the history tables described Observed the table and verified that the documents list the CISO, Managing Director, and CEO as participants in the review and update process	
CC1.5.2	The organization has metrics to measure performance and quality.	Reviewed the AP Company Scorecard (dated August 25, 2020) and verified that the organization has metrics to measure performance and quality Interviewed the Managing Director and verified that the Company Scorecard is updated weekly and used to show the state of the company, key metrics, and quality of operations Observed a copy of the company score card and the weekly metrics that it presents Observed the scorecard shows the number of sprints planned, time on developing features, growth of newsletter list, number of new users, visits to the website, leads, etc.	No Relevant Exceptions Noted

Trust Services Criteria for the Security and Availability Categories			
Communication and Information			
Ctrl #	**Description of Controls**	**Service Auditor's Tests of Controls**	**Test Results**
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.		
CC2.1.1	The company maintains and updates a company scorecard to provide leadership with a state of the company, key metrics, and the quality of operations/tasks being completed.	Reviewed the AP Company Scorecard (dated August 25, 2020) and verified that the organization has metrics for performance and quality Interviewed the Managing Director and verified that the Company Scorecard is updated weekly and is used to show the state of the company, key metrics, and quality of operations Observed a copy of the company score card and the weekly metrics that it presents Observed the scorecard shows the number of sprints planned, time on developing features, growth of newsletter list, number of new users, visits to the website, leads, etc.	No Relevant Exceptions Noted
CC2.1.2	The organization stores, transmits, and processes PII data.	Reviewed the AdvicePay Data Flow Diagram (dated August 18, 2020) and determined the types of data used in the application Interviewed the CISO and verified that the organization uses some PII such as name, email address, and information related to invoices, subscriptions, fees, etc.; the credit card and ACH information is posted directly to Stripe and Plaid, and only a token is returned to be used for future payment processing Observed a demonstration of the system and verified that the financial planners enter their client's name and billing information Observed that the platform makes calls to Stripe for payment processing	No Relevant Exceptions Noted

		Observed that the financial planner can enter limited amounts of data for billing their client and for eSignatures	
CC2.1.3	The organization maintains diagrams describing data movement in the environment.	Reviewed the Data Flow Diagram (dated August 18, 2020) and verified that the organization has diagrams describing data movement in the environment Interviewed the Lead Developer regarding data flow within the environment and verified that the diagram describes the connections and data movement to services outside of the application, including other SaaS solutions Observed the network diagram and compared it to the description provided by the Lead Developer and to the product demonstration and verified that the diagram accurately represents the AdvicePay data flow process	No Relevant 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	The organization communicates training requirements within the Dream Team Handbook and the Technology and Security Operations.	Reviewed AdvicePay's Dream Team Handbook (dated July 2020) and verified that the company's requirement for training reimbursements and company-provided training are detailed Reviewed the Technology and Security Operations document (dated August 11, 2020) and verified that the requirement for new hires to attend policy and security awareness training at hire, and policy-refresher training annually, is documented Reviewed Pluralsight invoices and verified that the organization maintains a subscription for training on coding techniques Interviewed the Managing Director and the CISO and verified that the requirement for security awareness	No Relevant Exceptions Noted

		training for all employees at hire and then annually as well as the reimbursement program for job-related training Observed the two new hires and 3 of 16 current employees and verified that they acknowledged completion of security awareness training Observed the receipts from Pluralsight for all three application developers and verified that they have subscribed to job competency training for code development	
CC2.2.2	When reporting a security incident, employees are instructed to contact the CISO or Managing Director.	Reviewed the Team Member Security Policy (dated June 6, 2020) and verified that employees are instructed to contact the CISO or Managing Director when reporting a breach or complaint Reviewed the organization's Privacy Policy posted on the company website and verified that the privacy policy has contact information for emailing the Help Desk and physical/mailing address Interviewed the CISO and verified that the policy states that if a breach is suspected, the employee should contact the CISO or Managing Director and verified that the privacy policy posted on the website has the contact information for the Help Desk Observed the policy and website and verified that employees are instructed to contact the CISO or Managing Director and clients would contact the Help Desk and that the privacy policy provides Help Desk contact information	No Relevant Exceptions Noted
CC2.2.3	The organization uses contracts and its website to communicate services to its clients.	Reviewed the Standardized AdvicePay SaaS Agreement (dated August 31, 2020) and verified that it contains the following:	No Relevant Exceptions Noted

		• Terms for SLAs for commercial clients • Information for system uptime and the service level credit for each category • Information on operational security • Fees and payments • Non-disclosure Reviewed three executed contracts and verified that they match the template provided Interviewed the Managing Director and verified that the SLAs communicated to commercial clients include best effort technical support with listed response time and restoration times Observed the Security and Compliance page on the company website and verified information about security is presented on the website	
CC2.2.4	Company policies are hosted on a Google Drive available to all employees.	Reviewed the Technology and Security Operations (dated August 11, 2020) and verified the Chief Information Security Officer is responsible for communicating the information security policy to personnel Interviewed the Managing Director and the CISO and verified that the handbook and policies are hosted on a Google Drive available to all employees and distributed to customers and vendors as requested Observed the Google Drive folder hosting the handbook and verified that all employees have read access	No Relevant Exceptions Noted
CC2.2.5	Monthly all-hands meetings occur to communicate the tone and direction of the company to its employees.	Reviewed the AP All-Hands Team Slides (dated June 6, 2020, July 7, 2020, August 8, 2020) and verified that monthly all-hands meetings communicate the tone and direction of the company to its employees	No Relevant Exceptions Noted

		Interviewed the Managing Director and verified that the monthly all-hands meeting that the CEO uses to communicate personnel changes, goals and success metrics, projects, and other corporate initiatives Observed the contents of the slides from the all-hands meetings from three of four months during the audit period and verified the inclusion of personnel changes, projects, goals and progress toward them, and initiatives including the SOC2 audit	
CC2.2.6	The organization maintains an incident response plan.	Reviewed the Technology and Security Operations (dated August 11, 2020) and verified that the organization has an incident response plan in place that includes the following steps: • Incident classification track • Responsibilities for the SIRT • Incident notification • Lessons learned Interviewed the CISO and verified that the Incident Response Plan is included in the policy and it discusses the SIRT role, incident classifications, tracking and correlation, and contacts Observed the Incident Response Plan and verified that it contains information on the SIRT, reporting, assessment, incident classification and criticality, tracking, notifications, and lessons learned	No Relevant Exceptions Noted
CC2.2.7	The organization has documented descriptions for key staff with security responsibilities assigned.	Reviewed the organization's job descriptions and verified that the organization has documented descriptions for key staff with assigned security responsibilities Interviewed the Managing Director and the CISO and verified that the CISO has primary responsibility for information security	No Relevant Exceptions Noted

		Observed the job descriptions and verified that the CISO has responsibility for policies, security, third-party vendor review, working with development for application security, disaster recovery, and security training Observed that the Senior Manager of Customer Experience has oversight of QA testing and maintaining the knowledge base	
CC2.2.8	Annual training is required for personnel with incident response responsibilities.	Reviewed the Incident Report Form (dated August 7, 2020) and verified that the organization has had tabletop testing and training for incident response Interviewed the CISO and verified that the annual training for incident response includes tabletop drills to enforce the understanding of roles of the SIRT Observed the documentation and verified that the organization has performed a tabletop test for an incident response drill and the simulation was for a client's former employee exporting data and that the report contained the steps to resolve the incident; the lesson learned were recorded	No Relevant Exceptions Noted
CC2.2.9	Information security responsibilities are documented for all employees.	Reviewed the Technology and Security Operations (dated August 11, 2020) and verified security responsibilities are defined for the CEO, Information Security Steering Committee, Managing Director, CISO, SIRT, DevOps, Developers, Operations, and Team Members verified that the scope is provided for each of the policies Reviewed the Team Member Security Policy (dated June 9, 2020) and verified that the scope of the policy is defined	No Relevant Exceptions Noted

		Interviewed the CISO and verified that the information security policy is hosted on a Google Drive available to all employees and that employees are required to acknowledge the policy at hire and annually Observed the Google Drive folder hosting the policy and verified that all employees have read access Observed the acknowledgements the two new employees hired during the audit period and 3 of 16 current employees and verified that all have acknowledged the security policy	
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.		
CC2.3.1	The Lead Developer reviews blog posts from AWS Security, NIST Cybersecurity Insights, SANS, Cobalt, and Reddit to stay knowledgeable about system configurations.	Reviewed the blog posts reviewed by the Lead Developer and verified that they provide knowledge about configuration management Interviewed the Lead Developer and verified that the blogs reviewed by him include AWS Security, NIST Cybersecurity Insights, SANS, Cobalt, and Reddit Observed screenshots of each of the blog posts to which the Lead Developer is subscribed and verified his access to the blog posts for security and secure configurations	No Relevant Exceptions Noted
CC2.3.2	When reporting a security incident, clients would contact the help desk.	Reviewed the Team Member Security Policy (dated June 6, 2020) and verified that employees are instructed to contact the CISO or Managing Director when reporting a breach or complaint Reviewed the organization's Privacy Policy posted on the company website and verified that the privacy policy has Help Desk's email and physical/mailing address Interviewed the CISO and verified that the policy states that if a breach is suspected, the employee should	No Relevant Exceptions Noted

		contact the CISO or Managing Director and verified that the privacy policy posted on the website has the contact information for the Help Desk Observed the policy and website and verified that employees are instructed to contact the CISO or Managing Director and clients would contact the Help Desk and that the privacy policy provides Help Desk contact information	
CC2.3.3	Distribution of the Information Security Policy to customers and vendors occurs on a requested basis.	Reviewed the Technology and Security Operations (dated August 11, 2020) and verified the Chief Information Security Officer is responsible for communicating the information security policy to personnel Interviewed the Managing Director and the CISO and verified that the handbook and policies are hosted on a Google Drive available to all employees and distributed to customers and vendors as requested Observed the Google Drive folder hosting the handbook and verified that all employees have read access	No Relevant Exceptions Noted
CC2.3.4	The SIRT should only communicate incident details with other parties who have a business reason to know them	Reviewed the Technology and Security Operations (dated August 11, 2020) and verified that the organization has an incident response plan in place that includes the following steps: • Incident classification track • Responsibilities for the SIRT • Incident notification • Lessons learned Interviewed the CISO and verified that the Incident Response Plan is included in the policy and it discusses the SIRT role, incident classifications, tracking and correlation, and contacts Observed the Incident Response Plan and verified it contains information on	No Relevant Exceptions Noted

		the SIRT, reporting, assessment, incident classification and criticality, tracking, notifications, and lessons learned	
CC2.3.5	The organization maintains a knowledgebase of articles to instruct its clients on best practices when using its services.	Reviewed the organization's website and verified that the organization has many help articles for clients at different service levels Interviewed the Managing Director and the CISO and verified that the organization maintains a knowledgebase with 300 articles for using the product and that the availability of the articles is based on account levels: Advisor users, Essential and Professional Advisor users, and Enterprise users Observed that the organization has documentation for the use of the product form onboarding and creating an account to the full functionality of the product	No Relevant Exceptions Noted

Trust Services Criteria for the Security and Availability Categories			
Risk Assessment			
Ctrl #	**Description of Controls**	**Service Auditor's Tests of Controls**	**Test Results**
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.		
CC3.1.1	The organization is governed by GLBA and has designed its security programs accordingly.	Interviewed the CISO and verified that the organization is governed by GLBA because their clients are involved in personal investing; therefore, the organization has implemented controls that reflect the intent of the act in their security program, specifically Privacy and Safeguard rules that involve security and encryption of data Observed by verifying controls throughout the assessment that the organization has privacy policies and controls as well as security and encryption of data as described	No Relevant Exceptions Noted
CC3.1.2	The organization performs a formal risk assessment.	Reviewed the AP Risk Assessment (dated March 10, 2020) and verified that the organization performs a formal risk assessment Reviewed the Technology and Security Operations Policy (dated August 11, 2020) and verified that the organization performs risk assessments based on the risk register annually and the SRM program is based on the NIST Risk Register Template Interviewed the CISO and verified that the annual risk assessment process and the company's decision to base the risk assessment on the NIST template; also verified how remediation efforts are assigned to staff Observed the results of the risk assessment in the risk register and verified that it is based on the NIST framework with mappings to other frameworks as well	No Relevant Exceptions Noted

		Observed the STATUS column in the risk assessment and verified it states the condition of controls for the threat, and confidentiality, integrity, availability, risk likelihood, and risk strategy are analyzed and noted for controls in place or mitigation plans	
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	Risk analysis strategies are documented and used for performing the company's formal risk assessment.	Reviewed the AP Risk Assessment (dated March 10, 2020) and verified that the organization performs a formal risk assessment Reviewed the Technology and Security Operations Policy (dated August 11, 2020) and verified that the organization performs risk assessments based on the risk register annually and the SRM program is based on the NIST Risk Register Template Interviewed the CISO and verified the annual risk assessment process and the company's decision to base the risk assessment on the NIST template; also verified how remediation efforts are assigned to staff Observed the results of the risk assessment in the risk register and verified that it is based on the NIST framework with mappings to other frameworks as well Observed the status states the condition of controls for the threat, and confidentiality, integrity, availability, risk likelihood, and risk strategy are analyzed and noted for controls in place or mitigation plans	No Relevant Exceptions Noted
CC3.2.2	The process of risk mitigation includes mitigating, accepting, or transferring risks.	Reviewed the AP Risk Assessment (dated March 10, 2020) and verified that the organization has performed and identified remediation needed Reviewed the Technology and Security Operations Policy (dated August 11, 2020) and verified that the	No Relevant Exceptions Noted

		policy provides directions for risk mitigation Reviewed the Risk Assessment of Data Loss Prevention (DLP) and verified that the analysis of accepted risks identified Interviewed the CISO and verified that the process of risk mitigation includes mitigating, accepting, or transferring risks and the documented decisions for each finding Observed the documentation provided for the description of actions to be taken for findings in the risk assessment including the mitigation of some risks and the acceptance of others Observed that video surveillance DLP, monitored security systems, and unlocked front door during office hours were accepted risks	
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.		
CC3.3.1	AdvicePay's SRM program is based on the NIST Risk Register Template.	Reviewed the AP Risk Assessment (dated March 10, 2020) and verified that the organization performs a formal risk assessment Reviewed the Technology and Security Operations Policy (dated August 11, 2020) and verified that the organization performs risk assessments based on the risk register annually and the SRM program is based on the NIST Risk Register Template Interviewed the CISO and verified that the annual risk assessment process and the company's decision to base the risk assessment on the NIST template; also verified how remediation efforts are assigned to staff Observed the results of the risk assessment in the risk register and	No Relevant Exceptions Noted

		verified that it is based on the NIST framework with mappings to other frameworks as well Observed that the status states the condition of controls for the threat, and confidentiality, integrity, availability, risk likelihood, and risk strategy are analyzed and noted for controls in place or mitigation plans	
CC3.3.2	AdvicePay evaluates risks to determine the appropriate mitigation strategy to assign.	Reviewed the AP Risk Assessment (dated March 10, 2020) and verified that the organization has performed and identified remediation needed Reviewed the Technology and Security Operations Policy (dated August 11, 2020) and verified that the policy provides directions for risk mitigation Reviewed the Risk Assessment of DLP and verified the analysis of accept risks identified Interviewed the CISO and verified that the process of risk mitigation includes mitigating, accepting, or transferring risks and the documented decisions for each finding Observed the documentation provided for the description of actions to be taken for findings in the risk assessment including the mitigation of some risks and the acceptance of others Observed that video surveillance DLP, monitored security systems, and unlocked front door during office hours were accepted risks	No Relevant Exceptions Noted
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.		
CC3.4.1	AdvicePay evaluates risks associated with environment and operational changes on an ongoing basis.	Reviewed the AP Risk Assessment (dated March 10, 2020) and verified that the organization performs a formal risk assessment	No Relevant Exceptions Noted

		Reviewed the Technology and Security Operations Policy (dated August 11, 2020) and verified that the organization performs risk assessments based on the risk register annually and the SRM program is based on the NIST Risk Register Template Interviewed the CISO and verified the annual risk assessment process and the company's decision to base the risk assessment on the NIST template; also verified how remediation efforts are assigned to staff Observed the results of the risk assessment in the risk register and verified that it is based on the NIST framework with mappings to other frameworks as well Observed the status states the condition of controls for the threat, and confidentiality, integrity, availability, risk likelihood, and risk strategy are analyzed and noted for controls in place or mitigation plans	

Trust Services Criteria for the Security and Availability Categories			
Monitoring Activities			
Ctrl #	**Description of Controls**	**Service Auditor's Tests of Controls**	**Test Results**
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	AdvicePay annually performs risk assessments based on the risk register.	Reviewed the AP Risk Assessment (dated March 10, 2020) and verified that the organization performs a formal risk assessment Reviewed the Technology and Security Operations Policy (dated August 11, 2020) and verified that the organization performs risk assessments based on the risk register annually and that the SRM program is based on the NIST Risk Register Template Interviewed the CISO and verified the annual risk assessment process and the company's decision to base the risk assessment on the NIST template; also verified how remediation efforts are assigned to staff Observed the results of the risk assessment in the risk register and verified that it is based on the NIST framework with mappings to other frameworks as well Observed the status states the condition of controls for the threat, and confidentiality, integrity, availability, risk likelihood, and risk strategy are analyzed and noted for controls in place or mitigation plans	No Relevant Exceptions Noted
CC4.1.2	The organization's internal controls are evaluated at least annually through regulatory and information security audits.	Reviewed the AdvicePay 2019 SOC 2 Type I Report (dated March 31, 2019) and verified that the organization performs independent audits Interviewed the CISO and verified that the organization engages in annual audits	No Relevant Exceptions Noted

		Observed the SOC 2 Type I audit report and the audit was performed and resulted in an unqualified opinion	
CC4.1.3	The organization performs security processes to detect control failures.	Interviewed the CISO and verified that the organization uses pre-established policies to determine organizational processes *Exception: The organization does not have recurring processes in place to detect control failures.*	Exception Noted
CC4.2	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.		
CC4.2.1	The CISO is responsible for developing and maintaining AdvicePay's SRM program.	Reviewed the AP Risk Assessment (dated March 10, 2020) and verified that the organization performs a formal risk assessment Reviewed the Technology and Security Operations Policy (dated August 11, 2020) and verified that the organization performs risk assessments based on the risk register annually and that the SRM program is based on the NIST Risk Register Template Interviewed the CISO and verified the annual risk assessment process and the company's decision to base the risk assessment on the NIST template; also verified how remediation efforts are assigned to staff Observed the results of the risk assessment in the risk register and verified that it is based on the NIST framework with mappings to other frameworks as well Observed the status states the condition of controls for the threat, and confidentiality, integrity, availability, risk likelihood, and risk strategy are analyzed and noted for controls in place or mitigation plans	No Relevant Exceptions Noted

Trust Services Criteria for the Security and Availability Categories			
Control Activities			
Ctrl #	**Description of Controls**	**Service Auditor's Tests of Controls**	**Test Results**
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	The organization's information security policies are contained within two documents.	Reviewed the Technology and Security Operations Policy (dated August 11, 2020) and verified that the policy contains relevant content including • Revision history • Date of last review • Policy maintenance • Best-practices guidelines Reviewed the Team Member Security Policy (dated June 18, 2020) and verified that the policy contains • Revision History • Date of last update • Policy information for all employees Reviewed the CISO's job description and verified that the role of the CISO in managing policies Interviewed the CISO and verified that the organization's information security policies are contained within two documents: the Technology and Security Policy is intended for the technical staff, and the Team Member Security Policy is for all employees and covers information that every employee needs to know Observed the Google Drive folder hosting the policy and verified that all employees have read access Observed the job description of the CISO and verified he is responsible for maintaining and updating all security documents	No Relevant Exceptions Noted

CC5.1.2	Roles are defined for Development Operations, Developers, Operations staff, and others and rights to the development systems are limited based on role.	Reviewed the Technology and Security Operations (dated August 11, 2020) verified that the roles are defined for Development Operations, Developers, Operations staff, and others Interviewed the Lead Developer and verified that the organization has three developers and the Lead Developer serving in the Development Operations role and verified that any of the three can move code to production but that the act is logged Observed permissions on the production systems and verified that only the three developers can merge code Observed that the rights to the development systems are limited based on role and verified access to Bitbucket is limited to four people	No Relevant Exceptions Noted
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.		
CC5.2.1	The Technology and Security Policy is intended for the technical staff and provides best practices guidelines for technology.	Reviewed the Technology and Security Operations Policy (dated August 11, 2020) and verified that the policy contains relevant content including • Revision history • Date of last review • Policy maintenance • Best practices guidelines Reviewed the Team Member Security Policy (dated June 18, 2020) and verified that the policy contains • Revision History • Date of last update • Policy information for all employees Reviewed the CISO's job description and verified the role of the CISO in managing policies	No Relevant Exceptions Noted

		Interviewed the CISO and verified that the organization's information security policies are contained within two documents: the Technology and Security Policy is intended for the technical staff, and the Team Member Security Policy is for all employees and covers information that every employee needs to know Observed the Google Drive folder hosting the policy and verified that all employees have read access Observed the job description of the CISO and verified that he is responsible for maintaining and updating all security documents	
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	All policies are required to be reviewed annually by the Managing Director and approved by the CEO.	Reviewed AdvicePay's Dream Team Handbook (dated July 2020) and the Technology and Security Operations document (dated August 2020) and verified both documents describe the communication process wherein the Managing Director communicates with the CEO for proposed changes to the Handbook and Policies, and the security policy also details the annual review and update requirements Interviewed the CISO and the Managing Director and verified that the policies are new and that all policies require the review of the Managing Director, who submits it for approval to the CEO; changes are tracked in the tables within the documents Observed the policies and the handbook and verified that the policies are current and contain the history tables described Observed the table and verified that the documents list the CISO, Managing Director, and CEO as	No Relevant Exceptions Noted

		participants in the review and update process	
CC5.3.2	The AP Company Scorecard, used to measure performance and quality, is updated each week and reviewed in a weekly department head meeting.	Reviewed the AP Company Scorecard (dated August 25, 2020) and verified that the organization has metrics to measure performance and quality Interviewed the Managing Director and verified that the Company Scorecard is updated weekly and used to show the state of the company, key metrics, and quality of operations Observed a copy of the company score card and the weekly metrics it presents Observed the scorecard shows the number of sprints planned, time on developing features, growth of newsletter list, number of new users, visits to the website, leads, etc.	No Relevant Exceptions Noted
CC5.3.3	The organization has requirements for testing of the business continuity and disaster recovery plans annually.	Reviewed the AdvicePay Business Continuity Plan.pdf (dated August 12, 2020) and verified that the organization has requirements for testing of the business continuity and disaster recovery plans annually and the disaster recovery team tests the disaster recovery plan quarterly Reviewed the Business Recovery Plan Tabletop Test (dated September 30, 2020) and verified that the company tested the disaster recovery response Interviewed the CISO and the Lead Developer and verified that the organization's first disaster recovery test was a tabletop exercise Observed the results of the tabletop test and verified that the scenario of regional failover and a multi-region failover Observed that the test showed that the failover would take approximately 20 to 30 minutes, well below the SLAs committed to the commercial clients	No Relevant Exceptions Noted

CC5.3.4	All AdvicePay policies are required to be reviewed annually.	Reviewed the Technology and Security Operations (dated August 11, 2020) and verified the following: • Policies are reviewed annually by the Information Security Steering Committee • The policy describes the communication to the Managing Director, who then communicates with the CEO for proposed changes to the Handbook and Policies for the CEO's approval • The security policy details the annual review and update requirements Interviewed the CISO and the Managing Director and verified that the policies are new and that all policies require the review of the Managing Director, who submits it for review and approval to the CEO; changes are tracked in the tables within the documents Observed the policies and handbook and verified that the policies are current and contain the history tables described Observed the table and verified that the documents list the CISO, Managing Director, and CEO as participants in the review and update process	No Relevant Exceptions Noted

Trust Services Criteria for the Security and Availability Categories			
Logical and Physical Access Controls			
Ctrl #	**Description of Controls**	**Service Auditor's Tests of Controls**	**Test Results**
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	All users must be assigned a unique user before being given access to any AdvicePay systems, applications, and data.	Reviewed the Technology and Security Operations (dated August 11, 2020) and verified that shared usernames are prohibited except for the demo server Interviewed the CISO and the Lead Developer and verified that shared accounts are not allowed on any platform except for the system used for sales demonstrations Observed the user accounts on Google applications, AWS, and Bitbucket and verified that there are no shared accounts or group account names	No Relevant Exceptions Noted
CC6.1.2	The documents used in the onboarding process ensure security when granting system access to new employees.	Reviewed the New Hire Onboarding Checklist, the Offer of Employment, the NDA, Policy Acknowledgement and Laptop Checkout and verified that the organization has established processes for the hiring and termination of employees and completes the forms as part of the hiring process Interviewed the Managing Director and verified the following: • The forms used for recording the steps in the hiring process include background checks and departmental notifications • All employees must sign the NDA, acknowledgements to the Employee Handbook and information security policy • Background checks are performed on all employees prior to starting Observed the forms used for the hiring of the two employees hired during the	No Relevant Exceptions Noted

		audit period and verified that the steps were followed, including background checks, and communications to staff for the creation of accounts and data access Observed that the employees had background checks performed and had signed the NDA and acknowledged the handbook and policies	
CC6.1.3	The organization has a privacy policy for both users of the website and tis own employees.	Reviewed the AdvicePay Privacy Policy (dated July 2, 2020) and verified that the organization has a privacy policy for users of the website and system Reviewed the Team Member Security Policy (dated June 9, 2020) and verified that the organization has a privacy policy directed at employees for the protection of private employee and customer data Interviewed the CISO and verified that the organization has two privacy policies: one is provided to customers and users of the site and is available on the 'Contact Us' page of the website, while the other is part of the internal security policy and directs employees on the protection of client and employee personal data Observed the organization's privacy policies and verified that the customer-facing privacy policy discusses the collection and use of personal data and descriptions of consumer rights and that it is available on the organization's website Observed that the employee privacy policy provides direction for employees on the protection of customer and employee personal information	No Relevant Exceptions Noted
CC6.1.4	AdvicePay uses Git within Bitbucket for source code version control.	Interviewed the Lead Developer and verified the use of Bitbucket as the source code repository and that access	No Relevant Exceptions Noted

		is based on role and is tightly controlled Observed a demonstration of the Bitbucket system and verified that the user list included only four members of staff	
CC6.1.5	Password complexity configurations are defined with the Team Member Security Policy.	Reviewed the Team Member Security Policy (dated June 9, 2020) and verified that the passwords must have the following characteristics: • Contain at least 12 characters • Cannot contain user's name or user ID • Are complex • Contain at least one symbol • Expire every 180 days (6 months) Reviewed the Jamf Security Settings to confirm the password settings in Jamf Interviewed the CISO and verified that the company has MacBooks and does not have a domain to enforce passwords but that Jamf is used to maintain laptop configurations including password complexity Observed the Jamf settings and verified that passwords are required, must be at least 12 characters, complex, and contain at least one symbol Observed that passwords must be changed every 6 months and cannot reuse the past 20 passwords Observed that screensaver activates after 10 minutes	No Relevant 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	The account creation process is to be completed by the Managing Director and the CISO.	Reviewed the Technology and Security Operations (dated August 11, 2020) and verified that the account	No Relevant Exceptions Noted

		creation process is completed by the Managing Director and the CISO Reviewed the New Hire Onboarding Checklist and verified the checklist is used by the CISO and Managing Director to grant user access Interviewed the CISO and verified that accounts are created based on least privilege and approval from the hiring manager Observed the tickets for the two new employees hired during the audit period and verified their accounts are created in G Suite and other SaaS systems; appropriate access has been granted to the AdvicePay application platform	
CC6.2.2	The terminations of accounts must take place within 24 hours for voluntary terminations and immediately for involuntary terminations.	Reviewed the Technology and Security Operations (dated August 11, 2020) and verified that the terminations of accounts must take place within 24 hours for voluntary terminations and immediately for involuntary terminations Reviewed the AP Team Member Offboarding Checklist and verified that the checklist is used to remove access for terminated employees Interviewed the CISO and verified that change management tickets are used to verify which access was given to make sure that all access is removed Observed the one terminated employee's form and verified that the termination form was completed and observed user lists to verify access to AdvicePay platform and Google authentication was removed	No Relevant Exceptions Noted
CC6.2.3	Change management tickets are used to verify which access was given to make sure that all access is removed.	Reviewed the Technology and Security Operations (dated August 11, 2020) and verified that terminations of accounts must take place within 24 hours for voluntary terminations and	No Relevant Exceptions Noted

		immediately for involuntary terminations Reviewed the AP Team Member Offboarding Checklist and verified that the checklist is used to remove access for terminated employees Interviewed the CISO and verified that change management tickets are used to verify which access was given to make sure that all access is removed Observed the one terminated employee's form and verified that the termination form was completed and observed user lists to verify that access to AdvicePay platform and Google authentication was removed	
CC6.2.4	Accounts are created based on least privilege and approval from the hiring manager.	Reviewed the Technology and Security Operations (dated August 11, 2020) and verified that the account creation process is completed by the Managing Director and the CISO Reviewed the New Hire Onboarding Checklist and verified the checklist is used by the CISO and Managing Director to grant user access Interviewed the CISO and verified that accounts are created based on least privilege and approval from the hiring manager Observed the tickets for the two new employees hired during the audit period and verified their accounts are created in G Suite and other SaaS systems; appropriate access has been granted to the AdvicePay application platform	No Relevant Exceptions Noted
CC6.2.5	Clients manage their own accounts by self-registering and creating and managing their own users.	Reviewed How to Manually Close an Advisor Account – AdvicePay Help Desk document (dated October 8, 2019) and verified that clients are able to deregister their own accounts	No Relevant Exceptions Noted

		Interviewed the CISO and the Business Development Associate and verified that the process for clients to self-register their own accounts and to manage their own user accounts Observed a demonstration of the platform by the Business Development Associate and verified that clients manage their own accounts by self-registering and creating and managing their own users Observed documentation and verified that users can close their own advisor accounts	
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	Access given to restricted and confidential data is based on a need to know basis.	Reviewed the Technology and Security Operations (dated August 11, 2020) and verified that access changes for users outside of the new hire and termination process must be approved by the Managing Director Reviewed the Team Member Security Policy (dated June 9, 2020) and verified that access given to restricted and confidential data is need-based Interviewed the CISO and verified that access to data is based on role and need and that access requests must be approved by the Managing Director and tracked in change tickets Observed the policies and verified access is need-based Observed the two new employees and verified that their access is based on role, which provided no access to the production system	No Relevant 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	AdvicePay, Inc. implements physical access controls for its corporate office facility.	Reviewed the Team Member Security Policy (dated June 9, 2020) and verified the following: • The front door is locked to the XYPN office space during no-working hours and is secured by badge reader • The back door is always locked and has no access from the outside, it is egress only Interviewed the CISO and verified that the office has not been occupied since the start of the pandemic except for a few XYPN employees (sister company) but verified the following for normal operations: • Employees are given a badge for after hour access • The Teem visitor access record system by iOFFICE is used to register visitors • There is no video surveillance in the building and no burglar alarms since there are no servers or production systems in the suite Observed a remote walkthrough by the CISO using Webex and verified that the following was in place: • Badge reader access on the front door • The office was unoccupied because of the COVID pandemic except one XYPN employee • The office has a visitor recording system • The closet hosting the switches was unlocked but the metal cabinet hosting the systems was key-locked Reviewed door logs for three days and verified that access is recorded and had little activity because of the pandemic	No Relevant Exceptions Noted
CC6.4.2	Visitors are required to sign in with the iPad at the front desk.	Reviewed the Team Member Security Policy (dated June 9, 2020) and verified visitors are required to sign in with the iPad at the front desk	No Relevant Exceptions Noted

		Interviewed the CISO and verified that visitors to the XYPN offices are required to sign in using the iPad kiosk at the front desk Observed the kiosk system at the front desk used to sign in visitors records first and last name, time in and out, host, host email, host phone number, and visit type (purpose)	
CC6.4.3	AdvicePay uses badge access for granting access to its facility after hours.	Reviewed the Team Member Security Policy (dated June 9, 2020) and verified the following: • The front door is locked to the XYPN office space during no-working hours and is secured by badge reader • The back door is always locked and has no access from the outside, it is egress only Interviewed the CISO and verified that the office has not been occupied since the start of the pandemic except for a few XYPN employees (sister company) but verified that the following for normal operations: • Employees are given a badge for after hour access • The Teem visitor access record system by iOFFICE is used to register visitors • There is no video surveillance in the building and no burglar alarms since there are no servers or production systems in the suite Observed a remote walkthrough by the CISO using Webex and verified that the following was in place: • Badge reader access on the front door • The office was unoccupied because of the COVID pandemic except one XYPN employee • The office has a visitor recording system	No Relevant Exceptions Noted

		• The closet hosting the switches was unlocked but the metal cabinet hosting the systems was key-locked Reviewed door logs for three days and verified that access is recorded and had little activity because of the pandemic	
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	The organization provides physical asset security as long as necessary for all types of data and software.	Reviewed the Team Member Security Policy (dated June 9, 2020) and verified the following: • The front door is locked to the XYPN office space during no working hours and is secured by badge reader • The back door is always locked and has no access from the outside, it is egress only Interviewed the CISO and verified that the office has not been occupied since the start of the pandemic except for a few XYPN employees (sister company) but verified the following for normal operations: • Employees are given a badge for after-hour access • The Team visitor access record system by iOFFICE is used to register visitors • There is no video surveillance in the building and no burglar alarms since there are no servers or production systems in the suite Observed a remote walkthrough by the CISO using Webex and verified that the following was in place: • Badge reader access on the front door • The office was unoccupied because of the COVID pandemic except one XYPN employee • The office has a visitor recording system	No Relevant Exceptions Noted

		• The closet hosting the switches was unlocked but the metal cabinet hosting the systems was key-locked Reviewed door logs for three days and verified that access is recorded and had little activity because of the pandemic	
CC6.5.2	The Data Classification Policy mandates the wiping or physical destruction of restricted and confidential data before disposal.	Reviewed the Team Member Security Policy (dated June 9, 2020) and verified that the data classification policy mandates the wiping or physical destruction of restricted and confidential data before disposal Interviewed the CISO and verified that drives are wiped or destroyed before discarding but the company has not had to destroy any yet and the organization has a shredder for disposal of documents Observed during remote walkthrough of the office that a shredder is available for employees to use to shred confidential documents	No Relevant Exceptions Noted
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.		
CC6.6.1	Bitbucket Groups are used to control access to the AdvicePay repository, as well as to specific branches within the repository when necessary.	Interviewed the Lead Developer and verified that the use of Bitbucket as the source code repository and that access is based on role and is tightly controlled Observed a demonstration of the Bitbucket system and verified that the user list included only four members of staff	No Relevant Exceptions Noted
CC6.6.2	Application passwords are required to be encrypted.	Reviewed the Technology and Security Operations (dated August 11, 2020) and verified that the requirement for application passwords to be encrypted with bcrypt using 128-bit salt Interviewed the Lead Developer and the CISO and verified that the use of bcrypt to hash user passwords	No Relevant Exceptions Noted

		Observed the code for the bcrypt implementation and verified that it is used to create hashes of passwords in the application	
CC6.6.3	MFA is required to be used when available.	Reviewed the Technology and Security Operations (dated August 11, 2020) and verified that the requirement for MFA to be used when available Interviewed the CISO and the Lead Developer and verified that MFA is used whenever possible but is required for managing the AWS environment, and Google Authenticator or Authy is used Observed a demonstration of the Lead Developer logging into the AWS console and the use of MFA Observed the login settings for users and verified MFA is required	No Relevant Exceptions Noted
CC6.6.4	Firewall ports filter the information allowed into the production network.	Reviewed the Technology and Security Operations (dated August 11, 2020) and verified only ports 80 and 443 are allowed into the production network and all traffic is allowed out Reviewed the Firewall Configuration Screen Shot and verified that the ports allowed to and from the AWS environment Interviewed the Lead Developer and the CISO and verified that only ports 80 and 443 are allowed to the AWS environments and all ports are allowed for egress Observed screenshots of the AWS firewall configuration and verified that only ports 80 and 443 are allowed for ingress traffic Observed that no egress filtering is applied	No Relevant Exceptions Noted

CC6.6.5	TLS1.2 encryption is required to be used for data in transit.	Reviewed the Technology and Security Operations (dated August 11, 2020) and verified that the requirement to use TLS1.2 encryption for data in transit Interviewed the CISO and the Lead Developer and verified that data in transit is set to TLS1.2 and nothing lower is allowed Tested three URLs provided of the company's website and verified that TLS1.2 is used, and no deprecated protocols were found to be in use	No Relevant 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	NIST and ISO 27001 are used for encryption standards.	Reviewed the Technology and Security Operations (dated August 11, 2020) and verified that the requirement to use TLS1.2 encryption for data in transit Interviewed the CISO and the Lead Developer and verified that NIST and ISO 27001 are used for encryption standards Tested the three URLs provided and verified that TLS1.2 is used, and no deprecated protocols were found to be in use in alignment with NIST	No Relevant Exceptions Noted
CC6.7.2	The organization requires separate development, test, and public demo environments.	Reviewed the Software Development Life Cycle (dated May 1, 2020) and verified that the requirement for separate development, test, and public demo environments Reviewed the AdvicePay AWS Environments (dated September 8, 2020) and verified that the organization has a network diagram showing the production, demo, staging, and preview environments Interviewed the Lead Developer and verified that the separation of the environments as all the application	Exception Noted

		server systems are in one subnet and all the database systems are in another subnet Observed the network diagram and interviewed the Lead Developer to verify that all application servers are in one subnet and all database servers are in another subnet Observed there is no segmentation between development/staging and production application servers and no segmentation between development/staging and production database servers *Exception: Proper segmentation is not implemented between development/staging environments and production environments.*	
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	The organization requires the use of antivirus software for its production servers and end user systems.	Reviewed the Technology and Security Operations (dated August 11, 2020) and verified that Bitdefender is updated daily Interviewed the CISO and the Lead Developer and verified that Armor Antivirus (AV) is installed on production servers and that Bitdefender is used on MacBooks for malware protection Observed the implementation and console for Jamf and verified that all systems comply with Bitdefender on end user systems Observed the Armor implementation on production servers and verified that Armor is running on the production systems	No Relevant Exceptions Noted

Trust Services Criteria for the Security and Availability Categories			
System Operations			
Ctrl #	**Description of Controls**	**Service Auditor's Tests of Controls**	**Test Results**
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	AdvicePay requires annual penetration testing and weekly vulnerability scans.	Reviewed the Software Development Life Cycle (dated May 1, 2020) and verified that security is implemented throughout the development process and is validated within the operations/maintenance phase Reviewed the Technology and Security Operations (dated August 11, 2020) and verified the requirement for annual penetration testing of the external network, annual vulnerability scans of the application and application code, and weekly vulnerability scans of internal application code testing and internal AWS infrastructure testing Reviewed the Maverick Security Assessment (dated May 12, 2020) and verified a web application penetration test was performed Reviewed Vulnerability Scans and verified that vulnerability scans are performed weekly and annually Interviewed the CISO and verified that the annual penetration test includes applications and infrastructure and that the vulnerability scans are performed by Armor Anywhere before each release Observed the penetration test and verified that application, including OWASP vulnerabilities, and network testing is included Observed the schedules of the vulnerability scans and the outputs from them and verified that the	No Relevant Exceptions Noted

		remediations of findings include the retesting of the penetration testing with the testing performed from March 30 – April 6, 2020 and the retest completed by May 12 Observed that all findings on the penetration test were remediated	
CC7.1.2	AdvicePay remediates all vulnerability findings or performs a risk mitigation if remediation is not possible.	Reviewed the Technology and Security Operations (dated August 11, 2020) and verified the requirement for annual penetration testing of the external network, annual vulnerability scans of the application and application code, and weekly vulnerability scans of internal application code testing and internal AWS infrastructure testing Reviewed Vulnerability Scans and verified that vulnerability scans are performed weekly and annually Interviewed the CISO and verified that the annual penetration test includes applications and infrastructure and that the vulnerability scans are performed by Armor Anywhere before each release Observed the penetration test and verified that application, including OWASP vulnerabilities, and network testing is included Observed the schedules of the vulnerability scans and the outputs from them and verified that the remediations of findings include the retesting of the penetration testing with the testing performed from March 30 – April 6, 2020 and the retest completed by May 12 Observed that all findings on the penetration test were remediated	No Relevant Exceptions Noted
CC7.1.3	All change requests are tracked in Jira and must be approved by the product owner.	Reviewed the Technology and Security Operations Policy (dated August 11, 2020) and verified that the	No Relevant Exceptions Noted

		change management process includes the following: • Request • Approval • Prioritization • Documentation • Testing • Communication • Implementation • Rollback • Provisions for emergency changes Interviewed the Lead Developer and verified that the changes are tracked in Jira and must be approved by the product owner; verified the process from approval to completion and the necessity of a rollback plan Observed three Jira tickets from the audit period and verified that all were approved by the product owner or lead developer Observed that all changes have a risk determination, issue type classification, assignment to a sprint, testing, and backout plans if applicable	
CC7.1.4	The organization's penetration test includes application, including OWASP vulnerabilities, and network testing.	Reviewed the Technology and Security Operations (dated August 11, 2020) and verified the requirement for annual penetration testing of the external network, annual vulnerability scans of the application and application code, and weekly vulnerability scans of internal application code testing and internal AWS infrastructure testing Reviewed Vulnerability Scans and verified that vulnerability scans are performed weekly and annually Interviewed the CISO and verified that the annual penetration test includes applications and infrastructure and the vulnerability scans are performed by Armor Anywhere before each release	No Relevant Exceptions Noted

		Observed the penetration test and verified that application, including OWASP vulnerabilities, and network testing is included Observed the schedules of the vulnerability scans and the outputs from them and verified that the remediations of findings include the retesting of the penetration testing with the testing performed from March 30 – April 6, 2020 and the retest completed by May 12 Observed that all findings on the penetration test were remediated	
CC7.1.5	End user systems are configured consistently.	Reviewed the Technology and Security Operations Policy (dated August 11, 2020) and verified that the organization has documented hardening standards for the production environment Interviewed the Lead Developer and verified that the process of using the "golden" AMI for building new instances and the process for updating that image Interviewed the CISO and verified that the use of Jamf for ensuring end user systems are configured consistently Observed a demonstration of the production environment and the AMI update process and verified configuration images for end user MacBook systems and the Jamf configuration process	No Relevant 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	The SIRT is responsible for managing, coordinating, and supporting AdvicePay's incident response procedures.	Reviewed the Technology and Security Operations (dated August 11, 2020) and verified that the organization has an incident response plan in place that includes the following steps:	No Relevant Exceptions Noted

		• Incident classification track • Responsibilities for the SIRT • Incident notification • Lessons learned Interviewed the CISO and verified that the Incident Response Plan is included in the policy and it discusses the SIRT role, incident classifications, tracking and correlation, and contacts Observed the Incident Response Plan and verified it contains information on the SIRT, reporting, assessment, classification of incident and criticality, tracking, notifications, and lessons learned	
CC7.2.2	IDS/IPS tools are provided by a third-party provider.	Reviewed the Technology and Security Operations (dated August 11, 2020) and verified that Armor is used for intrusion detection and prevention Interviewed the CISO and verified the use of Armor for server-based IPS monitoring and the use of GuardDuty at the perimeter and application level firewalls that send logs to CloudWatch Observed notifications in GuardDuty of two port probes and verified that IPS is working and alerting staff of issues	No Relevant Exceptions Noted
CC7.2.3	Constant IDS/IPS monitoring is implemented using Armor Anywhere as well as audit logs and for file integrity monitoring.	Reviewed the Technology and Security Operations (dated August 11, 2020) and verified that constant IDS and IPS monitoring is implemented by using Armor Anywhere as well as audit logs and for file integrity monitoring Interviewed the CISO and verified the use of Armor for server-based IPS monitoring and verified the use of GuardDuty at the perimeter and application level firewalls that send logs to CloudWatch Observed notifications in GuardDuty of two port probes and verified that	No Relevant Exceptions Noted

		IPS is working and alerting staff to issues Observed Armor alerts for File Integrity Monitoring for 8 days of 88 workdays in the audit period and verified that Armor is operational and alerting staff	
CC7.2.4	A third-party service provider is used for logging the production environment.	Interviewed the Lead Developer and verified that the use of Armor Anywhere for logging of the production environment Observed the logging capabilities for the systems in the AWS production environment in Armor and verified that systems are sending log information to Armor Anywhere	No Relevant Exceptions Noted
CC7.2.5	The organization responds to reported security incidents according to its predetermined procedure.	Reviewed the Incident Report (dated June 30, 2020) and verified that the organization responded to a potential security concern Interviewed the CISO and verified the incident report and the suspected email phishing attempt; the email was a legitimate email from a vendor Observed the incident response ticket and verified that the incident was reported, researched, and determined not to be a threat or breach Observed follow-up actions were taken and no lessons learned were recorded and no update to the Incident Response Plan was necessary	No Relevant Exceptions Noted
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 SIRT evaluates the criticality of reported security incidents.	Reviewed the Technology and Security Operations (dated August 11, 2020) and verified that the organization has an incident response plan in place that includes the following steps: • Incident classification track • Responsibilities for the SIRT	No Relevant Exceptions Noted

		• Incident notification • Lessons learned Interviewed the CISO and verified that the Incident Response Plan is included in the policy and it discusses the SIRT role, incident classifications, tracking and correlation, and contacts Observed the Incident Response Plan and verified it contains information on the SIRT, reporting, assessment, classification of incident and criticality, tracking, notifications, and lessons learned	
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 Plan includes procedures for dealing with lessons learned.	Reviewed the Technology and Security Operations (dated August 11, 2020) and verified that the organization has an incident response plan in place that includes the following steps: • Incident classification track • Responsibilities for the SIRT • Incident notification • Lessons learned Interviewed the CISO and verified that the Incident Response Plan is included in the policy and it discusses the SIRT role, incident classifications, tracking and correlation, and contacts Observed the Incident Response Plan and verified it contains information on the SIRT, reporting, assessment, classification of incident and criticality, tracking, notifications, and lessons learned	No Relevant Exceptions Noted
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.		
CC7.5.1	Incident recovery procedures are defined within the Technology and Security Operations document.	Reviewed the Technology and Security Operations (dated August 11, 2020) and verified that the organization has an incident response	No Relevant Exceptions Noted

		plan in place that includes the following steps: • Incident classification track • Responsibilities for the SIRT • Incident notification • Lessons learned Interviewed the CISO and verified that the Incident Response Plan is included in the policy and it discusses the SIRT role, incident classifications, tracking and correlation, and contacts Observed the Incident Response Plan and verified it contains information on the SIRT, reporting, assessment, classification of incident and criticality, tracking, notifications, and lessons learned	
CC7.5.2	Critical patches must be applied immediately.	Reviewed the Patch Management Policy (dated May 29, 2020) and verified the following: • Laptops are managed by Jamf and are set to receive automatic OS updates • Critical patches must be applied immediately • The AWS environment is updated weekly Interviewed the Lead Developer and the CISO and verified that Jamf is used to install patches on laptops and that the update process for the production systems includes installing patches in the staging environment and testing prior to installing the patches in the production environment Observed that the Jamf settings and verified that patching on MacBooks is current Observed that patching of the systems in the staging environment was current and the production systems were patched as of two weeks prior showing that patches were tested in the staging environment for two weeks	No Relevant Exceptions Noted

Trust Services Criteria for the Security and Availability Categories			
Change Management			
Ctrl #	**Description of Controls**	**Service Auditor's Tests of Controls**	**Test Results**
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	The Technology and Security Operations Policy defines information security responsibilities for all employees.	Reviewed the Technology and Security Operations (dated August 11, 2020) and verified that security responsibilities are defined for the CEO, Information Security Steering Committee, Managing Director, CISO, SIRT, DevOps, Developers, Operations, and Team Members verified that the scope is provided for each of the policies Reviewed the Team Member Security Policy (dated June 9, 2020) and verified that the scope of the policy is defined Interviewed the CISO and verified that the information security policy is hosted on a Google Drive available to all employees and that employees are required to acknowledge the policy at hire and then annually Observed the Google Drive folder hosting the policy and verified that all employees have read access Observed the acknowledgements the two new employees hired during the audit period and 3 of 16 current employees and verified that all have acknowledged the security policy	No Relevant Exceptions Noted
CC8.1.2	AdvicePay has an implemented policy in place for change management located within the Technology and Security Operations Policy.	Reviewed the Technology and Security Operations Policy (dated August 11, 2020) and verified that the change management process includes: • Request • Approval • Prioritization • Documentation • Testing	No Relevant Exceptions Noted

		• Communication • Implementation • Rollback • Provisions for emergency changes Interviewed the Lead Developer and verified that the changes are tracked in Jira and must be approved by the product owner; verified that the process from approval to completion and the necessity of a rollback plan Observed three Jira tickets from the audit period and verified that all were approved by the product owner or lead developer Observed all changes have a risk determination, issue type classification, assignment to a sprint, testing, and backout plans if applicable	
CC8.1.3	The organization has documented hardening standards for the production environment.	Reviewed the Technology and Security Operations Policy (dated August 11, 2020) and verified that the organization has documented hardening standards for the production environment Interviewed the Lead Developer and verified that the process of using the "golden" AMI for building new instances and the process for updating that image Interviewed the CISO and verified that the use of Jamf for ensuring end user systems are configured consistently Observed a demonstration of the production environment and the AMI update process and verified configuration images for end user MacBook systems and the Jamf configuration process	No Relevant Exceptions Noted
CC8.1.4	The hardening standards are based on SANS and AWS guidance.	Reviewed the Technology and Security Operations (dated August 11, 2020) and verified that the organization has hardening standards for production systems	No Relevant Exceptions Noted

		Interviewed the Lead Developer and verified that the hardening standards are based on SANS and AWS guidance Observed the configuration standards and verified that they match best practices for production systems	
CC8.1.5	The organization has processes for updating the configuration for images.	Reviewed the Technology and Security Operations (dated August 11, 2020) and verified that the organization has processes for updating the configuration for images Interviewed the Lead Developer and verified that the updating process for AMI images includes launching an EC2 image from the golden image and updating it; verified that it is then tested as a production candidate image in the staging environment Observed a demonstration of the staging environment and the process for updating images	No Relevant Exceptions Noted

Trust Services Criteria for the Security and Availability Categories			
Risk Mitigation			
Ctrl #	**Description of Controls**	**Service Auditor's Tests of Controls**	**Test Results**
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.		
CC9.1.1	The organization analyzes risks from potential business disruptions with its annual risk assessment.	Reviewed the AP Risk Assessment (dated March 10, 2020) and verified that the organization performs a formal risk assessment Reviewed the Technology and Security Operations Policy (dated August 11, 2020) and verified that the organization performs risk assessments based on the risk register annually and the SRM program is based on the NIST Risk Register Template Interviewed the CISO and verified the annual risk assessment process and the company's decision to base the risk assessment on the NIST template; also verified how remediation efforts are assigned to staff Observed the results of the risk assessment in the risk register and verified that it is based on the NIST framework with mappings to other frameworks as well Observed that the status states the condition of controls for the threat, and confidentiality, integrity, availability, risk likelihood, and risk strategy are analyzed and noted for controls in place or mitigation plans	No Relevant Exceptions Noted
CC9.2	The entity assesses and manages risks associated with vendors and business partners.		
CC9.2.1	Vendors are reviewed upon renewal and annually.	Reviewed the Technology and Security Operations (dated August 11, 2020) and verified that vendors are reviewed upon renewal and annually Reviewed the Vendor Security Review document and verified that the organization maintains a list of vendors with columns used to record	No Relevant Exceptions Noted

		the information collected during the vendor review process Observed the record of vendors' review is in progress and verified that the organization collected audit reports if available and compliance information for GDPR, ISO, and privacy information, along with notes of findings Observed that the organization has collected and reviewed SOC 2 reports for vendors that have them	
CC9.2.2	The organization performs due diligence on all vendors and reviews them against set criteria.	Reviewed the Technology and Security Operations (dated August 11, 2020) and verified that the organization reviews vendors based on the following criteria: • Financial stability • Business maturity • Services offered • Quality of service and support • Security documentation • SOC assessment Reviewed the Vendor Security Review and verified that the organization maintains a list of vendors with columns used to record the information collected during the due diligence and review process Observed the record for all new vendors onboarded during the audit period and verified that the companies were SaaS providers Observed the organization collected audit reports if available and compliance information for GDPR, ISO, and privacy information, along with notes of findings	No Relevant Exceptions Noted
CC9.2.3	The organization maintains a list of service providers.	Reviewed the Third-Party Vendors Google Docs list and verified that the organization maintains a list of service providers	No Relevant Exceptions Noted

		Interviewed the CISO and verified that the service organizations and the services each provide Observed list of service providers	
CC9.2.4	Clients and vendors are required to sign NDAs prior to sharing any sort of information.	Reviewed the Pacific Advisors & AdvicePay Mutual NDA (dated June 29, 2020) and verified that NDAs are signed with clients and vendors prior to engaging in information sharing Interviewed the CISO and verified that clients and vendors are required to sign NDAs prior to sharing any sort of information Observed an executed copy of an NDA and verified that they are used to protect confidential information from being disclosed Observed the agreement contains restrictions on use, ownership, disclosures required by law, indefinite duration, and disposal	No Relevant Exceptions Noted
CC9.2.5	The Standardized AdvicePay SaaS Agreement details agreed upon services with AdvicePay's clients.	Reviewed the Standardized AdvicePay SaaS Agreement (dated August 2020) and verified the following: • The SLAs terms for commercial clients are detailed in Schedule C of the contract • Schedule B contains information for system uptime and the service level credit for each category Reviewed the AdvicePay Terms of Service and verified that the Terms of service for individual accounts do not guarantee SLAs Interviewed the Managing Director and verified that the SLAs communicated to commercial clients include best effort technical support with listed response time and restoration time Observed the contracts for SLA commitments and observed monitoring	No Relevant Exceptions Noted

		solutions to verify unavailability of systems would be known by technical staff within minutes Observed disaster recovery and backup and restore processes to verify that restoration of services can be met	

Additional Criteria for Availability			
Ctrl #	**Description of Controls**	**Service Auditor's Tests of Controls**	**Test Results**
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.		
A1.1.1	CloudWatch alarms and auto-scaling groups within AWS are used for capacity determination.	Interviewed the Lead Developer and verified that the use of CloudWatch for capacity monitoring of the AWS environment, that auto-scaling is enabled and automatically implements more systems as necessary, and the use of Uptime Robot to monitor the availability of the site Observed a demonstration of the monitoring configuration of CloudWatch and the graphical interface showing system capacity for system capacity Observed the dashboard for Uptime Robot and verified its use for monitoring the availability of the site	No Relevant Exceptions Noted
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.		
A1.2.1	The facilities are equipped with environmental safeguards that protect the company assets and monitor for fire, water, and intrusion-related incidents.	Reviewed the Team Member Security Policy – 2020 June (dated June 9, 2020) and verified that the policies for physical access to the company's offices include requirements for hours of access, security card use, and egress only for the back door Interviewed the CISO and verified that the offices have locked doors equipped with badge readers, water-based sprinklers, and smoke detectors; there are no servers in the office as everything is hosted at AWS Observed during a video walkthrough of the office that the doors were locked with badge reader on the front door and no latch on the back door (egress only)	No Relevant Exceptions Noted

		Observed water-based sprinklers and smoke detectors Observed that the computer closet was key-locked and contained no servers	
A1.2.2	The organization has a disaster recovery plan for the cloud environment and for the protection of business processes.	Reviewed the Business Recovery Plan (dated September 30, 2020) and verified that the organization has a disaster recovery plan for the cloud environment Reviewed the AdvicePay Business Continuity Plan (dated August 12, 2020) and verified that the organization has a business continuity plan for the protection of business processes Reviewed the Business Impact Analysis (dated August 12, 2020) and verified that the organization has performed a business impact analysis to determine the availability requirements of critical assets Interviewed the CISO and the Lead Developer and verified that the AWS environment is backed up, and is replicated to another availability zone in the same region and then replicated to another region for disaster recovery purposes Observed a presentation of the disaster recovery process and the replication between availability zones and to another region and verified data is redundant between zones and little effort would be required to make the new region active as the data and applications are already present	No Relevant Exceptions Noted
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.		
A1.3.1	AdvicePay uses the AWS Backup services to perform backups of the AdvicePay application environment and data.	Reviewed the Technology and Security Operations (dated August 11, 2020) and verified the requirement for backups in the AWS and Google environments	No Relevant Exceptions Noted

		Interviewed the CISO and the Lead Developer and verified that the replication process for AWS occurs between the two availability zones and to another region Observed a demonstration of the replication processes used for backing up the environments Observed that the environments are continuously replicated between AWS USEast1a and USEast1b and then to the west region for disaster recovery	
A1.3.2	The organization performs a business impact analysis to determine the availability requirements of critical assets.	Reviewed the Business Recovery Plan (dated September 30, 2020) and verified that the organization has a disaster recovery plan for the cloud environment Reviewed the AdvicePay Business Continuity Plan (dated August 12, 2020) and verified that the organization has a business continuity plan for the protection of business processes Reviewed the Business Impact Analysis (dated August 12, 2020) and verified that the organization has performed a business impact analysis to determine the availability requirements of critical assets Interviewed the CISO and the Lead Developer and verified that the AWS environment is backed up and is replicated to another availability zone in the same region and then replicated to another region for disaster recovery purposes Observed a presentation of the disaster recovery process and the replication between availability zones and to another region and verified data is redundant between zones and little effort would be required to make the new region active as the data and applications are already present	No Relevant Exceptions Noted