AdvicePay

AdvicePay Security Overview

Have Questions?

Contact us at support@advicepay.com

About AdvicePay

AdvicePay is a privately owned company headquartered in Bozeman, MT. We are incorporated in Delaware and registered to do business in Montana. AdvicePay is a cloud-based SaaS established by well-known financial advisors Michael Kitces and Alan Moore. AdvicePay is a fee-for-service business solution built specifically for Financial Advisors who expect efficiency, compliance, and security in their billing and payment processes. Financial advisors benefit from invoicing and payment workflows designed exclusively to support their businesses, including up-to-date compliance and data security management. Users can issue agreements for client e-signature, accept ACH and credit cards, bill hourly or one-time fees, or establish recurring retainer or subscription billing compliantly – all through the AdvicePay system.

How We Protect Data for You and Your Clients

Have Confidence in a Secure System

We've designed the AdvicePay system to maximize data security at every level of our payment processing. AdvicePay utilizes multiple third-party vendors to provide services as applicable to the AdvicePay application. AdvicePay engages with the Stripe payment processing platform, a U.S.-based payment processor that manages billions of dollars each year. Stripe has been audited by a Payment Card Industry (PCI)-certified auditor and is certified to PCI DSS Service Provider Level 1. This is the most stringent level of certification available in the payments industry. Stripe annually performs a SOC 2 Type II audit for compliance.

For additional information on Stripe's security see: Security at Stripe

In addition to Stripe, AdvicePay also integrates with the following other third party vendors:

- Plaid for ACH transactions - How We Handle Data
- DocuSign for document signature - Security
- HelloSign for document signature - Security
- FTNI for Online Check Deposit

Infrastructure Hosting - AWS

AdvicePay Infrastructure is hosted to maximize compliance and security. AdvicePay's physical infrastructure is hosted and managed within Amazon's secure data centers and utilizes Amazon Web Services (AWS). Amazon continually manages risk and undergoes recurring assessments to ensure compliance with data security industry standards.

Amazon's data center operations have been accredited under:

- ISO 27001, ISO 27017, ISO 27018
- SOC 1/SSAE 16/ISAE 3402, SOC 2, SOC 3
- PCI DSS Level 1
- FISMA Moderate
- Sarbanes-Oxley (SOX)
- SEC Rule 17a-4(f)

For additional information on AWS compliance see: AWS Security and Compliance

Payment Information

Payment Information is never stored in our database. AdvicePay submits payment requests to Stripe securely via tokenization. Customer information is never stored directly on any AdvicePay servers. This approach enables information to remain securely stored in one place, guarding against compromise.

Fraud Prevention

AdvicePay employs adaptive machine learning to detect and prevent fraud by using Radar, a data aggregator used to identify potential fraud indicators across all of Stripe's 100,000+ businesses. These proactive steps work to improve fraud detection and reduce the risk of improper use of the platform.

Information Security

AdvicePay ensures the security and confidentiality of Customer Confidential Information and Consumer Confidential Information while also protecting AdvicePay's proprietary and confidential information. AdvicePay takes the appropriate measures as applicable to meet the standards and framework of the ISO 27001 and NIST 800-53 Cybersecurity Framework. The highlighted sections below provide a high level overview of the AdvicePay policies and procedures that safeguard AdvicePay's information security environment.

Auditing

In order to measure an information system's level of security through confidentiality, integrity, and availability, the system must collect audit data that provides key insights into system performance and activities. This audit data is collected in the form of system logs. Logging from critical systems, applications, and services provides information that can serve as a starting point for metrics and incident investigations. All AdvicePay systems are logged using AWS auditing mechanisms and aggregated into a SIEM for monitoring and reporting. AdvicePay retains all logs for an extended period for the purposes of review, investigation, and compliance.

Encryption

AdvicePay uses HTTPS with TLS 1.2 exclusively to ensure confidentiality and data integrity. HTTPS is the secure version of HTTP, the protocol over which data is sent between your browser and the website to which you are connecting. You can be confident all interactions between client and advisor browsers and the AdvicePay website are encrypted using the secure HTTPS protocols.

AdvicePay application data is securely stored in AWS RDS instances. The data is encrypted at rest using AES 256-bit encryption at all times. AdvicePay backs up data using the AWS Backup service and all backups are encrypted using AES 256-bit encryption.

Vulnerability Assessments

Internally AdvicePay performs routine vulnerability assessments of the AdvicePay application code and vulnerability assessment of the AWS infrastructure. Vulnerability tests of the Application application code are performed on an ongoing basis before each deployment of code. Vulnerability assessments of the AWS infrastructure are performed on a weekly basis.

AdvicePay engages a third-party testing company to perform testing on an annual basis. The scope of the third party testing includes the following:

- Penetration testing of the external network
- Vulnerability testing of the AdvicePay application
- Vulnerability testing of the AdvicePay application code

IDS/IPS and Malware Protection

AdvicePay engages with a third party cloud security platform that provides SIEM services to strengthen our AWS security posture. The services integrate with our AWS environment providing the ability to detect, prevent, and report security threats through IDS and IPS services as well as malware protection services. This cloud security platform provides log management, automated monitoring of logs, reporting, and retention of logs for security and compliance purposes.

Incident Management

AdvicePay's Incident Management program is designed to respond, manage, and resolve incidents that cause a disruption or reduction in service. AdvicePay's Incident Response Team (IRT) manages, coordinates, and supports the incident response process. The Incident Response Team is responsible for carrying out the Incident Management process including the following:

- Incident Identification and Reporting
- Incident Analysis and Assessment
- Incident Notification and Escalation
- Resolution and Recovery
- Postmortems and Lessons Learned
- Training and Testing

Incident Reporting -- You See Something Say Something

While AdvicePay is constantly monitoring for incidents, it is always important that if we see something that we say something. If you see any issue while using the AdvicePay services that may be an incident please contact us. These potential incidents include but are not limited to:

- Privacy Issues
- Security Incidents
- Fraud Incidents

Business Resiliency

AdvicePay is dedicated to providing continuity of the AdvicePay services in the event of incidents and disasters. AdvicePay has established a Business Continuity Plan and Business Recovery Plan (BRP). Additionally AdvicePay has designed both backup processes and failover processes to complement our Business Recovery Plan in order to protect data and ensure our ability to recover quickly.

Business Continuity Plan

AdvicePay recognizes that it is critical for our organization to be able to provide continuous, uninterrupted services to our customers and our customer's clients. Any inability to provide services for an extended period of time could have a severe economic impact to AdvicePay and our customers. AdvicePay has created a Business Continuity Plan (BCP) that defines AdvicePay's critical business units (departments), scope of the BCP, and ranking of business units based on criticality. The Recovery Point Objectives, Recovery Time Objectives, and criticality of business units is evaluated through our annual Business Impact Analysis.

The scope of the Business Continuity Plan is a structured plan that includes the following key components:

- BCP Plan Detail
  - BCP Team Responsibilities
  - Succession Plan and Key Personnel
  - BCP/DR Strategy
- BCP and BRP Response Scenarios
- Recovery Time Objectives and Recovery Point Objectives
- Business Continuity Plan and Business Recovery Plan Administration
  - Communications
  - Authorization
  - Annual Testing of the BCP
  - Quarterly Testing of the BRP
  - Documentation
  - Distribution
  - Training

Business Recovery Plan

AdvicePay recognizes that it is critical for our organization to be able to provide continuous, uninterrupted services to our customers and our customer's clients. Any inability to provide services for an extended period of time could have a severe economic impact to AdvicePay and our customers. The AdvicePay Business Recovery Plan (BRP) defines the process for technology recovery.

The scope of the BRP covers AdvicePay's technology recovery. Included in the technology recovery are the AdvicePay application systems that are maintained within AWS and AdvicePay's laptop computers used by Team Members.

The BRP plan provides detailed processes to perform:

- AWS Zone Failover Process
- AWS Region Failover Process
- Laptop Recovery Process

Backup and Restore Policy

The backup and restore policy covers the backup and restoration of data associated with the AdvicePay AWS environment including the following:

- Backup Schedule - Nightly
- Backup Retention - 30 days
- Restore Requests Approval Process
- Logging of Backups

Privacy

Your data privacy and preferences concerning the collection of your information is important to AdvicePay. The AdvicePay Privacy Policy describes our privacy practices that apply to AdvicePay website visitors and individuals who register to use the AdvicePay services. If you have any questions about the AdvicePay Privacy Policy, please contact us.

AdvicePay Compliance

SOC 2 Type II

AdvicePay performs an annual SOC 2 Type II audit that is performed and delivered by CPA firm, KirkpatrickPrice. The audit specifically tests AdvicePay's reporting controls that relate to security and availability. This attestation provides evidence that AdvicePay has a strong commitment to security and to delivering high-quality services to its clients by demonstrating that they have the necessary internal controls and processes in place.

The successful completion of the SOC 2 Type II examination and audit highlights AdvicePay's continued commitment to deliver best-in-class solutions and safeguards to protect and secure our customers' data. This Attestation of Compliance is widely known as the industry benchmark for SaaS businesses and the most stringent examinations of an organization's security controls, policies, and procedures, and we are proud to exceed customer expectations when it comes to protecting their data.

PCI SAQ A

As a merchant service provider, AdvicePay performs a PCI Self Assessment Questionnaire (PCI SAQ A) on an annual basis as required by our partner Stripe. The PCI SAQ A is a validation tool that assists in evaluating and attesting to the PCI Data Security Standard (DSS) of compliance. AdvicePay partners with Stripe who performs all card holder data functions. Stripe is a certified PCI DSS Level 1 payment processor. AdvicePay as a merchant service provider does not perform any cardholder data functions including storage, processing, or transmission of card data.