FILE | 13F

file13f.com | 1-844-844-3453 | support@file13f.com

CYBER SECURITY & VENDOR DUE DILIGENCE REPORT

Prepared Pursuant to Amended Regulation S-P

SEC Release No. 34-99949 | Effective August 2, 2024

Vendor Name	File|13F
Website	https://file13f.com
Phone	1-844-844-3453
Service Category	Form 13F SEC Filing Service
Date of Review	March 20, 2026
Prepared For	Compliance Department
Review Frequency	Annual (minimum) or upon material change

1. Purpose and Regulatory Background

This Vendor Due Diligence Report has been prepared for your Firm in accordance with the amended Regulation S-P ("Reg S-P"), adopted by the U.S. Securities and Exchange Commission ("SEC") on May 16, 2024 (SEC Release No. 34-99949), effective August 2, 2024.

Amended Reg S-P formally requires covered institutions — including Registered Investment Advisers ("RIAs"), broker-dealers, investment companies, funding portals, and transfer agents — to establish, maintain, and enforce written policies and procedures governing:

- Due diligence and ongoing monitoring of service providers that access, maintain, or process customer information;
- An Incident Response Program ("IRP") to detect, respond to, and recover from unauthorized access to customer information;
- Client breach notification within 30 days of becoming aware of a qualifying incident;
- Mandatory contractual requirements with service providers, including a 72-hour vendor breach notification obligation; and
- Recordkeeping of vendor oversight activities for a minimum of five years (first two years in an easily accessible location).

File|13F has been identified as a covered service provider because it receives holdings data from the Firm in order to prepare and submit the Firm's quarterly Form 13F filing with the SEC. This report documents the Firm's initial due diligence assessment of File|13F and serves as a permanent compliance record.

2. Vendor Overview

Legal Name	WealthFluent, LLC (operating under file13f.com)
Service Type	Full-service SEC Form 13F preparation and EDGAR filing
Primary Contact	support@file13f.com | 1-844-844-3453
Secure Upload Portal	https://www.sendsafely.com/u/support@file13f.com
Infrastructure Provider	DigitalOcean (data processing)
Secure Transfer Partner	SendSafely (end-to-end encrypted file delivery)
Pricing	$175 per quarter (flat fee)
Cancellation Policy	Cancel anytime.
Serves	Hundreds of financial advisory Firms (per vendor website)

Service Description

File|13F provides end-to-end Form 13F filing management for institutional investment managers required to report under Section 13(f) of the Securities Exchange Act of 1934. The Firm submits aggregated holdings data (number of shares, market value, CUSIP or ticker) to File|13F via a secure, encrypted upload portal. File|13F then:

- Cross-references submitted CUSIPs against the current SEC 13(f) securities list;
- Applies required minimum thresholds and aggregates positions as needed;
- Generates a compliant XML file meeting SEC EDGAR format requirements; and
- Uploads the completed filing to EDGAR on the Firm's behalf.

Importantly, File|13F instructs advisors to remove client-specific personally identifiable information ("PII") prior to uploading holdings data. The service is therefore designed to operate primarily on aggregated securities data rather than client-level nonpublic personal information ("NPI"). Once the filing is submitted to EDGAR, all information is PUBLICLY ACCESSIBLE.

3. Data Flow and NPI Assessment

Data Category	Assessment
Data Received by Vendor	Aggregated holdings data: number of shares, market value, CUSIP/symbol
Client PII Transmitted?	No — vendor instructs clients to remove client-specific information prior to upload
NPI Exposure Level	Low — data is aggregated, securities-level, not client-identifiable
Data Transmission Method	SendSafely encrypted portal (end-to-end AES-256 encryption)
Data Processing Environment	DigitalOcean cloud infrastructure
Data Retention by Vendor	Copy of submitted filing data deleted upon completion
Data Portability	Firm retains ownership of all submitted data

While the risk profile of File|13F is lower than vendors receiving direct client PII, the Firm nevertheless treats File|13F as a covered service provider under Reg S-P given that holdings data — in combination with other information — could potentially be used to identify client accounts. This conservative approach aligns with SEC examination priorities emphasizing substance over form in vendor oversight.

4. Cybersecurity Assessment

File|13F does not receive, send or maintain non-public information, but has designed a backend structure able to pass all cyber security benchmarks. To do so, File|13F has partnered with SendSafely to transport encrypted data and DigitalOcean to process data in its software.

4.1 Data Transmission Security — SendSafely

Security Overview

SendSafely uses several layers of security to protect information. All files and messages sent through the platform are protected using end-to-end encryption — meaning that nobody other than the sender and authorized individuals can read them. There is no way for SendSafely, or any third party, to decrypt this information. Even if data is intercepted, stolen or seized, it cannot be read without the proper decryption keys, which are never stored or accessible by SendSafely's systems.

Every set of files or messages sent through SendSafely are encrypted on the sender's machine before being submitted to SendSafely servers, using the OpenPGP message format with a key derived using OpenPGP's Iterated and Salted (Type 3) String-to-key (S2K) specifier. The Type 3 S2K converts a variable-length pass-phrase into a 256-bit symmetric AES encryption key consisting of 512 random bits:

- A 256-bit random Server Secret generated by SendSafely's servers
- A 256-bit random Client Secret generated by the sender's machine — never disclosed to SendSafely servers

Trusted Device Keys

Trusted device keys are a secondary encryption method. When logging in from a new browser, SendSafely asks whether to trust the browser. If confirmed, the browser generates a 2048-bit RSA Public/Private key pair. The private key is stored in the browser's local storage and never submitted to SendSafely; the public key is uploaded and stored by SendSafely to facilitate future access without requiring a new secure link.

Local Storage Encryption

SendSafely's security model relies on storing private key material within the browser's HTML5 Local Storage, protected by the browser's same-origin policy. As an additional safeguard, SendSafely encrypts this information using a 128-bit AES key unique to each user account, generated at account creation and stored on SendSafely's servers. The key is only revealed to the browser during active sessions.

Two-Step Login

Users may enable Two Step Login on all SendSafely accounts. When enabled, a random 6-digit PIN is generated for every login from an unrecognized device and sent to the user's mobile phone. The PIN is required in addition to user ID and password, helping prevent account takeover if credentials are compromised.

Cryptographic Libraries

SendSafely uses open standards for all cryptographic operations, relying on the following trusted third-party libraries:

- Bouncy Castle — used by .NET and Java APIs for OpenPGP support
- Google Keyczar — used by servers to encrypt data at rest, security-related cookies, and sensitive parameters
- Stanford Javascript Crypto Library — used by the front-end website and JavaScript API
- OpenPGP.js — used by JavaScript API and Chrome Extension for OpenPGP support

Web Application Security

All communications between SendSafely servers and browsers or mobile applications are encrypted using HTTPS/TLS (Transport Layer Security), providing an additional layer on top of end-to-end encryption to mitigate man-in-the-middle attacks. The HTTP Strict Transport Security header is deployed across SendSafely's site. SendSafely maintains an A+ rating from SSL Labs.

To protect against cross-site scripting (XSS) attacks, SendSafely's web application employs the Content Security Policy (CSP) standard to declare approved sources of content, blocking unauthorized JavaScript injection attempts.

Privacy and Metadata

SendSafely protects the contents of files and messages exchanged, but is not designed as an anonymous system. While SendSafely's servers have no knowledge of message contents, operational metadata is stored — including email addresses, phone numbers, contacts, file names, login timestamps, recipients, and IP addresses. SendSafely will not disclose this information to third parties except as operationally required.

Vulnerability Testing

SendSafely's engineering team conducts internal security audits on a regular basis and operates a public Bug Bounty Program. The company has additionally partnered with Edgescan for continuous external vulnerability scanning. Security issues may be submitted via SendSafely's Security Bug Reporting Form.

Security Control	Implementation	Rating
Encryption Standard	End-to-end OpenPGP; 256-bit AES symmetric key	✓ Strong
Key Management	Split-key architecture: Server Secret + Client Secret; Client Secret never leaves sender's machine	✓ Strong
Transport Layer	HTTPS/TLS with HSTS; SSL Labs A+ rating	✓ Strong
Two-Factor Authentication	Available on all accounts (6-digit PIN via mobile)	✓ Available
XSS Protection	Content Security Policy (CSP) enforced	✓ Strong
Device Trust	2048-bit RSA Public/Private key pair for trusted browsers	✓ Strong

Security Control	Implementation	Rating
Vulnerability Management	Internal audits + Bug Bounty + Edgescan continuous scanning	✓ Active
Cryptographic Libraries	Bouncy Castle, Google Keyczar, Stanford JSCS, OpenPGP.js	✓ Industry Standard
Metadata Handling	Operational metadata stored; not disclosed to third parties except as required	✓ Acceptable

4.2 Infrastructure Security — DigitalOcean

Physical Security

DigitalOcean's datacenters are co-located in respected global datacenter facilities with comprehensive physical security and environmental controls. Each site is staffed 24/7/365 with on-site physical security. Controls include:

- 24/7 Physical security guard services
- Physical entry restrictions to the property and the facility
- Physical entry restrictions to co-located datacenter areas
- Full CCTV coverage externally and internally
- Biometric readers with two-factor authentication
- Unmarked facilities to avoid drawing outside attention
- Battery and generator backup with generator fuel carrier redundancy
- Secure loading zones for equipment delivery

Infrastructure Security

DigitalOcean's infrastructure employs a defense-in-depth layered approach. Access to the management network is provided through multi-factor authentication points that restrict network-level access based on job function using the principle of least privilege. All access to ingress points is closely monitored and subject to stringent change control mechanisms.

Systems are protected through key-based authentication and access is limited by Role-Based Access Control (RBAC), ensuring that only required users can log into any given system. Systems housing customer data are treated as highest sensitivity, with extremely limited and closely monitored access. Hard drives and infrastructure are securely erased before decommissioning or reuse.

Access Logging & Security Monitoring

Systems controlling the management network at DigitalOcean log to a centralized logging environment for performance and security monitoring. Logging includes system actions as well as logins and commands issued by system administrators. DigitalOcean's Security team utilizes monitoring and analytics capabilities to identify potentially malicious activity, with investigations performed following formal incident reporting and response procedures.

Droplet Security & Employee Access

Technical support staff do not have access to the backend hypervisors where virtual servers reside, nor direct access to the NAS/SAN storage systems where snapshots and backup images reside. Only select engineering teams have direct access to backend hypervisors based on role.

Snapshot and Backup Security

Snapshots and backups are stored on an internal non-publicly visible network on NAS/SAN servers. Customers can directly manage the regions where their snapshots and backups exist, providing control over data residency within DigitalOcean's datacenters for security and compliance purposes.

Security Control	Implementation	Rating
Physical Security	Co-located Tier-III/IV DCs; 24/7/365 on-site security guards	✓ Strong
Facility Controls	Biometric 2FA entry; CCTV; unmarked facilities; secure loading zones	✓ Strong
Power Redundancy	Battery UPS + generator with fuel carrier redundancy	✓ Strong
Access Controls	MFA; RBAC; principle of least privilege	✓ Strong
Access Logging	Centralized logging of actions, admin logins, and commands	✓ Active
Security Monitoring	Behavioral analytics; formal incident response procedures	✓ Active
Customer Data Isolation	Support staff no hypervisor/NAS access; role-based engineering access only	✓ Strong
Data Destruction	Secure erasure of drives before decommission or reuse	✓ Strong
Backup Security	Internal non-public NAS/SAN; customer controls data region placement	✓ Strong

5. Reg S-P Compliance Checklist

Due Diligence Item	Result	Notes / Evidence Reviewed
Service provider identified and inventoried	✓ Pass	File|13F added to Firm's vendor inventory as covered service provider
Nature of data access documented	✓ Pass	Holdings data (aggregated); client PII excluded per vendor instructions
Vendor cybersecurity documentation reviewed	✓ Pass	File|13F Cyber Security Document reviewed; covers SendSafely & DigitalOcean controls
Encryption of data in transit	✓ Pass	End-to-end AES-256 via SendSafely; HTTPS/TLS with HSTS
Encryption of data at rest	✓ Pass	DigitalOcean infrastructure encryption; RBAC; secure drive erasure
Multi-factor authentication available	✓ Pass	Two-step login available on SendSafely upload portal
Physical security controls documented	✓ Pass	Documented in DigitalOcean cybersecurity materials
Vulnerability testing / penetration testing	✓ Pass	Internal audits and Edgescan confirmed through SendSafely.com
SOC 2 Type II report obtained	⚠ Review	SOC 2 not reporting since there is no PII
Incident response / breach notification (72 hrs)	✓ Pass	File|13F will notify any Firm of security breach within 72 hours of discovering breach

Due Diligence Item	Result	Notes / Evidence Reviewed
Vendor breach notification to Firm within 72 hours	✓ Pass	File|13F will notify any Firm of security breach within 72 hours of discovering breach
Data portability / return upon termination confirmed	✓ Pass	Vendor provides copy of submitted data upon filing completion
Annual re-assessment scheduled	✓ Pass	Calendared for annual review; triggered earlier upon material vendor change
Records of due diligence maintained 5 years	✓ Pass	This document retained in Firm compliance recordkeeping system

Legend: ✓ Pass = Satisfied based on available documentation ⚠ Review = Action required (see Section 6)

6. Ongoing Monitoring Plan

Consistent with Reg S-P's continuous oversight requirements, File|13F commits to the following ongoing monitoring and transparency activities to support your Firm's vendor oversight obligations:

- Annual security review: File|13F will conduct a full internal review of its security posture and data handling practices no less than annually, and will publish an updated version of this document to reflect any material changes.
- SOC 2 / security documentation: File|13F will provide updated third-party security attestation or documentation from its infrastructure partners (SendSafely and DigitalOcean) upon request and will proactively update this report when such documentation is refreshed.
- Contractual commitments: File|13F maintains all required contractual provisions with its clients, including the 72-hour breach notification obligation. These terms are available upon request and are incorporated into the service agreement executed with each client Firm.
- Incident notification: In the event of any security incident, File|13F will notify affected client Firms within 72 hours of discovery. File|13F will document the nature of the incident, actions taken, and resolution, and will provide that information to affected clients for their compliance recordkeeping.
- Material change disclosure: File|13F will promptly notify client Firms of any material changes to its operations, including ownership transfers, changes to subcontractors or infrastructure partners, or significant modifications to data handling practices, so that clients may re-assess as required under Reg S-P.
- Filing confirmation: Upon completion of each quarterly Form 13F submission, File|13F will provide the client Firm with an EDGAR confirmation, which clients should retain for their compliance records alongside this document.

This document has been prepared by File|13F to support your Firm's vendor due diligence obligations under Reg S-P. It is intended to serve as a ready-made compliance record that your Firm may retain alongside its executed service agreement with File|13F, any supplemental security documentation, and any incident records. File|13F will update this document at least annually and upon any material change to its operations.

DISCLAIMER

This document is provided by File|13F for informational and compliance support purposes only. It does not constitute legal advice. Your Firm should consult qualified legal counsel regarding its specific Reg S-P obligations and contractual requirements.