Filevine

How Filevine Approaches Security

WHITEPAPER

filevine.com

Table of Contents

INTRODUCTION

Partners in Safeguarding Legal Data

Filevine is committed to helping clients comply with their ethical duty to protect client information. Our team of experienced security professionals is dedicated to protecting your information, so you can better serve your clients and manage your practice with confidence.

As cyber threats proliferate, data security has become a growing concern for legal professionals. ABA Model Rule 1.6(1) charges all lawyers with the responsibility to "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."

THE CANADIAN BAR ASSOCIATION

ABA AMERICANBARASSOCIATION

The ABA Standing Committee on Ethics and Professional Responsibility has further stated that lawyers must "understand technologies that are being used to deliver legal services to their clients [and] use and maintain those technologies in a manner that will reasonably safeguard property and information that has been entrusted to the lawyer." Furthermore, ABA Formal Opinion 477R requires lawyers to secure communication of protected client information.

With security in mind, this paper aims to describe the sophisticated security controls Filevine utilizes to protect your client's information. This document is intended to give you a detailed but not exhaustive look into Filevine's security

landscape. We do not know for sure who is reading this paper so we have a few other security mechanisms in place as well that we will not describe, just as a precaution. This whitepaper explores some of the greatest security threats legal professionals face today and describes several of the powerful techniques we employ to safeguard your data.

It All Starts With Our Team

Information security, privacy and compliance are of utmost importance to Filevine; and it all starts with our trusted team members and outstanding leadership supporting this mission.

One of the most effective ways to safeguard data is to have security experts who are familiar with the threats facing the legal vertical and experienced in protecting law firms and their highly confidential data. The Filevine security team has both, and the team maintains recognized security certifications in many disciplines. These certifications include but are not limited to the following:

CIPP/US, CISA, CISSP, CITP, G2700, GAWN, GCCC, GCIH, GCPM, GISP, GLEG, GNFA, GPEN, GSLC, GSNA, GSOC, GSM, GWAPT, GXPN, MCTS, SEC+, Splunk Certified Power User, & Others.

GCPM

GSNA

GISP

GLEG

GCCC

GSLC

GAWN

GWAPT

GCIH

GXPN

GPEN

GNFA

GSOC

G2700

CISA

CIPP/US

CISSP

Filevine security team members have also taught classes on **CompTIA Sec+, Pentest+, CYSA+, CND, and CEH, Instant Response, Information Assurance, Digital Forensics, Network Security, and Cyber Defense.**

Pentest+ **CYSA+** **CompTIA Sec+** **CND** **CEH**

To ensure customer data is treated as confidential and private information, Filevine employees sign Mutual Non Disclosure Agreements (MNDA), are screened to ensure they pass criminal and financial background checks, and are obligated to review and comply with the terms and conditions contained in our employee handbook, annually.

For the Department of Justice, Criminal Justice Information System (CJIS), or other high security clientele, in addition to the standard employment screening process, Filevine also ensures our employees are fingerprinted, and pass individual State and Federal Bureau of Investigations (FBI) screening processes before being granted access to support these customers and their environments.

The cyber security landscape is changing every day and Filevine is well positioned to aid law firms and other professionals with highly advanced compliance, privacy and security programs to protect your data. We can help your business manage many potentially damaging risks today. This whitepaper will cover the three most common risks business face along with additional security measures we've found are vital to protect our customers.

CHAPTER 1

Risk 1: Ransomeware and Business Email Compromise (BEC)

One of the most common cyber-attacks currently facing lawyers is ransomware.

These attacks often begin with a phony email (or phish) as part of a BEC attack which fools a firm employee into opening an email with a URL link, infected document, attachment or simply an unexpected login screen requesting the user's username and password to open the file or access the link. Once the link is clicked, credentials entered or document opened, the malware then launches a ransomware program infecting the computer.

With access to one computer, the attack can spread throughout the network by exploiting vulnerabilities in older versions of Server Message Block (SMBv1), which provides access to local files, network file shares, printers, and backups. This attack allows a cybercriminal to encrypt the entire system so users cannot access the computers and demand ransom to restore access to the users.

More recent versions of ransomware look for all system backups of the victim's data so the attackers can encrypt those files as well, forcing the victim to pay the ransom to continue operations. These new ransomware variants also make a copy of the victim's files and send them to the cloud so the attackers can try to use the firm's data to target other victims or for other monetary gains.

Ransomware attacks against lawyers and businesses are on the rise, targeting firms of all sizes and geographic locations. This often results in the loss of all access to records and client data—sometimes permanently. Firm operations often screech to a halt, sometimes for months, as managers scramble to recover data. In the meantime, bad press and client dissatisfaction grows.

If ransomware were not impactful enough on its own, BEC also often involves theft of client information from compromised email accounts of partners, paralegals and administrative staff alike. Once the bad guys have access to your email, they often set up auto-forwarding rules to systematically download confidential client information from your mailbox and they patiently wait, looking for opportunities to steal money from the firm.

These adversaries look for upcoming financial transactions and they often attempt to steal money from the firm or clients by changing wiring instructions for business transactions orchestrated by the firm in the ninth hour. These transactions often occur over long weekends or holidays. Filevine helps reduce the likelihood and impact of security attacks with our layered approach to information security.

HOW FILEVINE HELPS PROTECT YOU

1 . Built on AWS's Trusted Platform

Filevine is the Legal Work Platform built on AWS—which is considered to be one of the most reliable, highly available and secure global infrastructures available.

This is the same platform used by government agencies, the Department of Defense, and some of the world's largest businesses and financial institutions (for example: Dow Jones, Capital One, GE, Johnson & Johnson, NASA, Disney, Netflix, BBC, Adobe, Turner Broadcasting, Facebook, Twitter, and millions of others).

Filevine leverages AWS's FIPS 197, FIPS 199 and FIPS 140-2 encryption within the AWS IaaS and PaaS platforms to ensure confidentiality

and that your data is highly available and protected. AWS's platform meets security, privacy, and compliance requirements for numerous compliance regimes including the following:

1	Cloud Security Alliance (CSA) Controls
2	International Organization for Standardization (ISO)
3	ISO 9001, ISO 27001, ISO 27017, ISO 27018
4	American Institute of Certified Public Accountants (AICPA) SOC 1, 2, 3
5	Criminal Justice Information Services (CJIS)
6	Department of Defense Data Processing (DoD SRG)
7	Federal Risk and Authorization Management Program (FedRAMP)
8	Federal Information Security Management (FISMA)
9	Health Insurance Portability Accountability Act (HIPAA)
10	Health Information Trust Alliance Common Security Framework (HITRUST CSF)[2]

Filevine believes in defense-in-depth, leveraging HA systems, database backup practices, redundant data centers, and best-in-class computing practices to provide firm protection from ransomware events and other disasters. Defense-in-depth means that Filevine does not rely on a single security control or even two to protect a security risk area. Typically, multiple security layers are designed-in to protect the Filevine platform.

Similarly, Filevine leverages Azure for our Lead Docket platform and Google Cloud Platform (GCP) for our Outlaw platform. These state of the art cloud service providers have similar levels of protections, redundancies and performance to AWS. So whichever Filevine product you are using, you can be reassured the corresponding platforms are secure and performing optimally so your teams are productive and your client's data is safe.

Azure's platform meets security, privacy, and compliance requirements for numerous compliance regimes including the following:

1	Cloud Security Alliance (CSA) Controls
2	International Organization for Standardization (ISO)
3	ISO 27001, ISO 27017, ISO 27018
4	American Institute of Certified Public Accountants (AICPA) SOC 1, 2, 3
5	Federal Risk and Authorization Management Program (FedRAMP)
6	Federal Information Security Management (FISMA)
7	Health Insurance Portability Accountability Act (HIPAA)
8	Health Information Trust Alliance Common Security Framework (HITRUST CSF)[3]

Google Cloud

Google's Cloud Platform (GCP) meets security, privacy, and compliance requirements for numerous compliance regimes including the following:

1	Cloud Security Alliance (CSA) Controls
2	International Organization for Standardization (ISO)
3	ISO 27001, ISO 27017, ISO 27018, ISO 27701
4	American Institute of Certified Public Accountants (AICPA) SOC 1, 2, 3
5	Federal Risk and Authorization Management Program (FedRAMP)
6	Federal Information Security Management (FISMA)
7	Health Insurance Portability Accountability Act (HIPAA)
8	Health Information Trust Alliance Common Security Framework (HiTECH CSF)

CHAPTER 2

Risk 2: Reused / Weak Passwords

verizon

The Verizon 2023 Data Breach Investigation Report[6] found that poor password practices were the root cause of many breaches, especially Business Email Compromises (BECs), one of the most common threats against businesses.

In the report, 70% of the BECs breaches appeared to occur because these credentials (username and password combination) consisted of compromised, weak, or reused passwords.

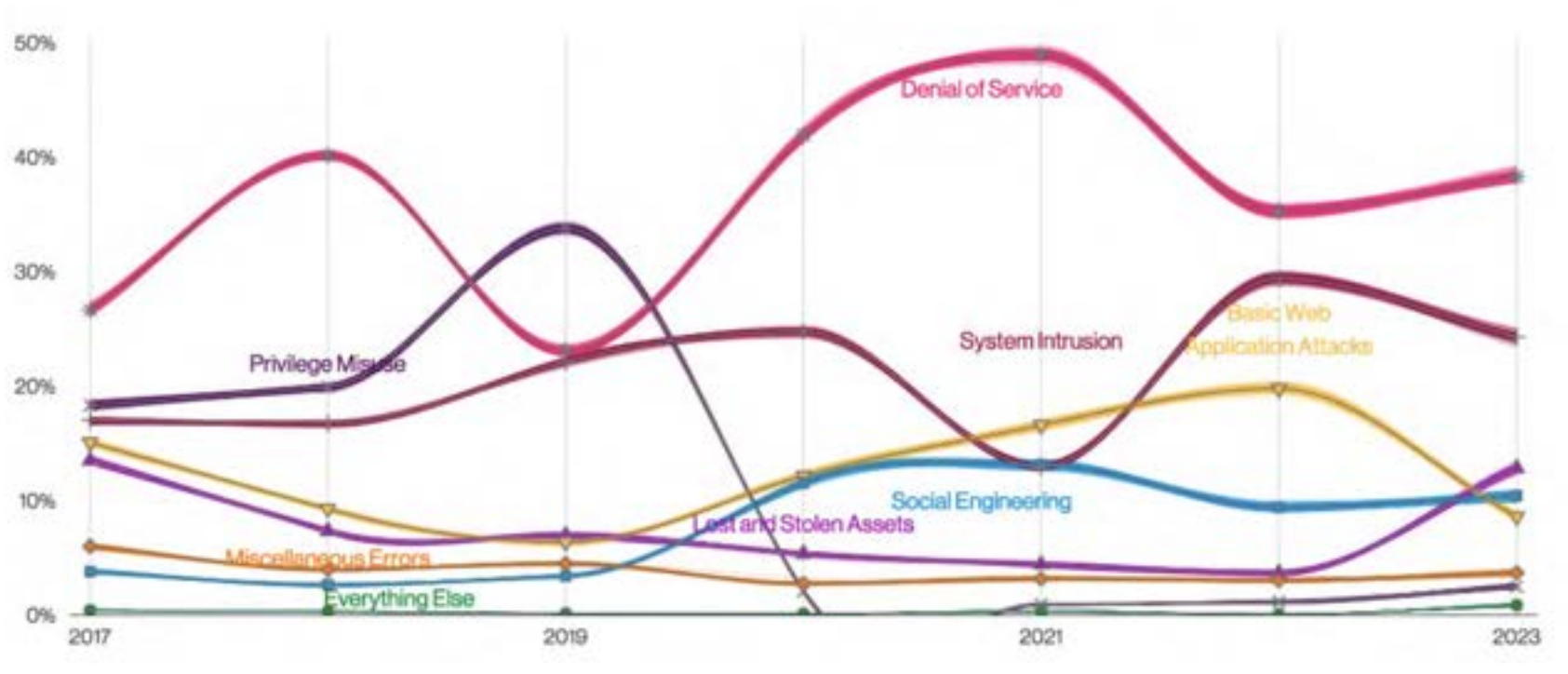


Figure 25. Patterns over time in incidents

Figure 25 from Verizon 2023 Data Breach Investigation Report[6]

Data breaches can result in tremendous financial and reputational costs to firms and individuals. When large data breaches occur, the criminal underground often hoard these breached credentials in large databases spanning many years and many successful attacks. The hackers often sell or share these credentials with other hackers further increasing the risk of data loss from a weak or reused password.

Using historical information, and human tendencies to reuse passwords we have memorized, cybercriminals can often discover trends or patterns over time, allowing them to potentially guess the credentials for other cloud systems we use.

HOW FILEVINE HELPS PROTECT YOU

1 . Identity and Access Management (IAM)

Filevine has invested heavily in a best-in-class IAM system to manage multiple security controls related to passwords. These security layers ensure Filevine employee's passwords and access are protected with multiple controls and sophisticated protection.

These layers include but are not limited to role-based access controls (RBAC), enforcement of strong passwords, two-factor authentication (2FA), password session time-outs, and account expiration for frequent, unsuccessful login attempts.

2 . Role-Based Access Control (RBAC)

This allows Filevine administrators and firm administrators to easily manage access to their confidential information. Access is granted or restricted based on predefined job roles inside the organization.

If an individual changes roles, their access changes as well. This makes it easier to authenticate, authorize, and audit access to systems and data. Firms can also delegate or provide limited access to clients or outside counsel without compromising security. Together, these features give Filevine customers greater control over who has access to information.

3 . Strong Passwords

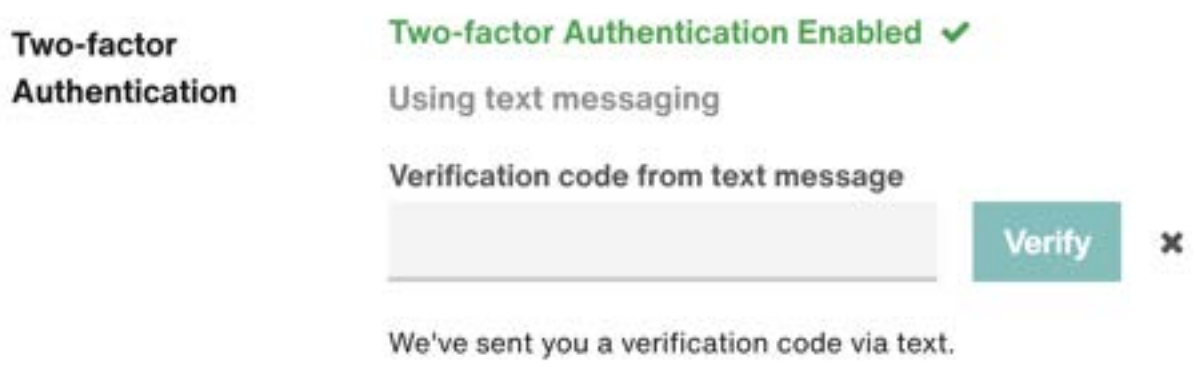
When you create a Filevine user account or update your account's passwords, Filevine requires a complex password of at least eight (8) characters and at least one (1) non-alpha character. Passwords are salted and one-way hashed in storage.

Much more complex and lengthy passwords are supported. Filevine administrative accounts used to administer the platform have even stronger password requirements to ensure access to the platform is secure. Filevine also supports and encourages the use of strong passphrases for clients utilizing the platform.

4 . Two-Factor Authentication (2FA)

Filevine administrative accounts utilize 2FA to provide an additional level of authentication, dramatically reducing the risk of hacking and data theft.

2FA is a combination of something you know, such as a password, and something you have, such as a soft token, hard token, or some other one-time password (OTP) technology such as Google or Microsoft authenticator. Due to this extra level of security for Filevine users, it's much less likely that the theft of a device or password will result in unauthorized access to data. Filevine has further enhanced the platform by allowing customers to enable this same 2FA feature so their users are equally protected from password re-use or theft.



Filevine is currently refactoring and deploying a new universal IAM platform for our applications, including Filevine, Vinesign, Leaddocket and Outlaw. This IAM platform is intended to provide support for federated IAM access and to allow additional enforcement of 2FA across the FV ecosystem, ultimately leading to a unified login experience.

5 . Failed Login Attempts

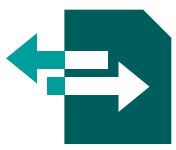
When Filevine user accounts cross the configured threshold for failed login attempts, the accounts are automatically locked, and a predetermined timed lockout is enabled to prevent additional failed attempts to access the account.

This practice reduces the likelihood of unauthorized access by someone who has identified a valid username but is attempting to brute force or guess the password.

2 . Redundant Data Backup

Filevine's AWS infrastructure automatically backs up client data. These backups are automated in multiple availability zones made up of multiple data centers, respectively.

To provide an added layer of security, backup data is encrypted using AES 256 to protect it at rest. Even in the most dire situations, should a firm employee introduce malware into your system, your data in the Filevine system should not be impacted. We regularly test our ability to restore these backups to ensure prompt recovery of your data in the event of a disaster.



3 . Disaster Recovery (DR) and High Availability (HA)

A fire, flood, or ransomware event can damage files and servers or lead to lost productivity and billables. Filevine ensures that no matter what happens to your physical office, as long as you can get an internet connection, you can immediately access your Filevine files and operate your practice remotely.

Filevine utilizes multiple AWS regions in the United States and Canada. Each AWS region is made up of multiple data centers often located in different states. These redundant data centers utilize redundant server clusters and redundant hardware and software systems within each data center.

AWS ensures that the Filevine platform has redundant switching, routing, and power for the supporting infrastructure systems to keep the platform up and to keep you productive. These investments make Filevine a central part of your firm's Disaster Recovery (DR) and Business Continuity Plans (BCP). High Availability (HA) systems help to ensure that no single point of failure can disrupt the platform.

Furthermore, our HA computing environment spans multiple availability zones with local system redundancy, to ensure that should part of the system fail—such as operating systems, web services, databases or file storage—there is a redundant system available to pick up the load.[3]

Documents stored in Filevine are replicated in near-real-time within the AWS region to each of the data centers in the region, and then every 15 minutes, these files are backed up to a different AWS region and replicated within that region. These backup practices add cost to the platform, but it ensures that under standard conditions, multiple copies of each revision of each document is saved to make sure you do not lose your work product.

4. Up-to-Date Server Software

Filevine regularly patches with the latest security updates to protect against new and emerging security threats.

We routinely refresh our server infrastructure through automated infrastructure-as-code (IaC) deployments to ensure pristine, predictively configured, patched and hardened Center for Internet Security (CIS) benchmarked AMI server images are deployed into production.

5. Physical Data Security

Filevine leverages AWS data centers to ensure they are secure, offsite locations with redundant power supply and cooling systems. This provides added stability and redundancy to keep the Filevine systems online, accessible, and secure.

Physical access points to server rooms are recorded by closed-circuit television cameras and access is monitored and controlled by professional security staff. AWS data centers undergo rigorous SSAE 18 and ISO 27001 standards, SOC 2 Type I, II and III certifications to ensure the confidentiality, availability, and integrity of customer data. These audits review more than 2600 requirements throughout the year.[4]

These data centers contain multiple layers of security defenses including but not limited to perimeter fencing and barricades, sally ports, multi-factor authentication, access controls, man-traps, security guards, video surveillance, motion sensors, security feeds, intrusion detection technology, and other security measures.

Physical access to Filevine office locations is authorized via electronically managed access control systems and access devices. Filevine facilities are locked at all times and access is granted with the authorized security application from previously authorized devices, ensuring that Filevine personnel or approved visitors who enter the building(s) are authorized.

Filevine offices also are protected with security cameras, motion sensors, magnetic locks, alarm systems and we utilize an external security monitoring company to provide around-the-clock alerting and response for security events.

6 . Media Destruction Practices

AWS complies with media destruction and retention policies consistent with NIST 800-88.

AWS media storage devices are classified as Critical and are managed as high impact throughout their lifecycle. AWS does not release media from its control until it has been securely decommissioned.(5)

7 . Disk Encryption and Sanitization Practices

Filevine laptops and removable media should not be used to store customer data.

In the event that business purposes necessitate storage of customer data on portable devices, these devices are encrypted utilizing whole disk encryption. Furthermore, these devices are forensically wiped when repurposed and then

again before being recycled. The recycling provider physically destroys the hard drives on laptops that are rotated out of service. The recycling service provides an attestation of destruction when needed.

8 . Additional Clouds and Trusted Service Providers

Filevine also leverages Azure and Google Cloud Platforms (GCP) to provide similar services to AWS for the Filevine portfolio of products.

These other providers also go through extensive vetting and they also comply with similar security controls to ensure they are also best in class service providers.

CHAPTER 3

Risk 3: Website Security

The Verizon 2023 Data Breach Investigation Report[6] shows that web application attacks are among the most common attacks for almost every kind of business reviewed in the report.

Many SaaS platforms, websites and web applications are targeted by hackers in an attempt to gain unauthorized access to large quantities of sensitive information.

To prevent these attacks from being successful, Filevine has continued to follow a defense-in-depth approach to protect this important information. This approach includes utilizing web application firewalls, writing secure code, testing the code, protecting the code from attack, vulnerability scanning, internal penetration testing, and hiring external penetration testing experts to reduce the likelihood we missed anything obvious.

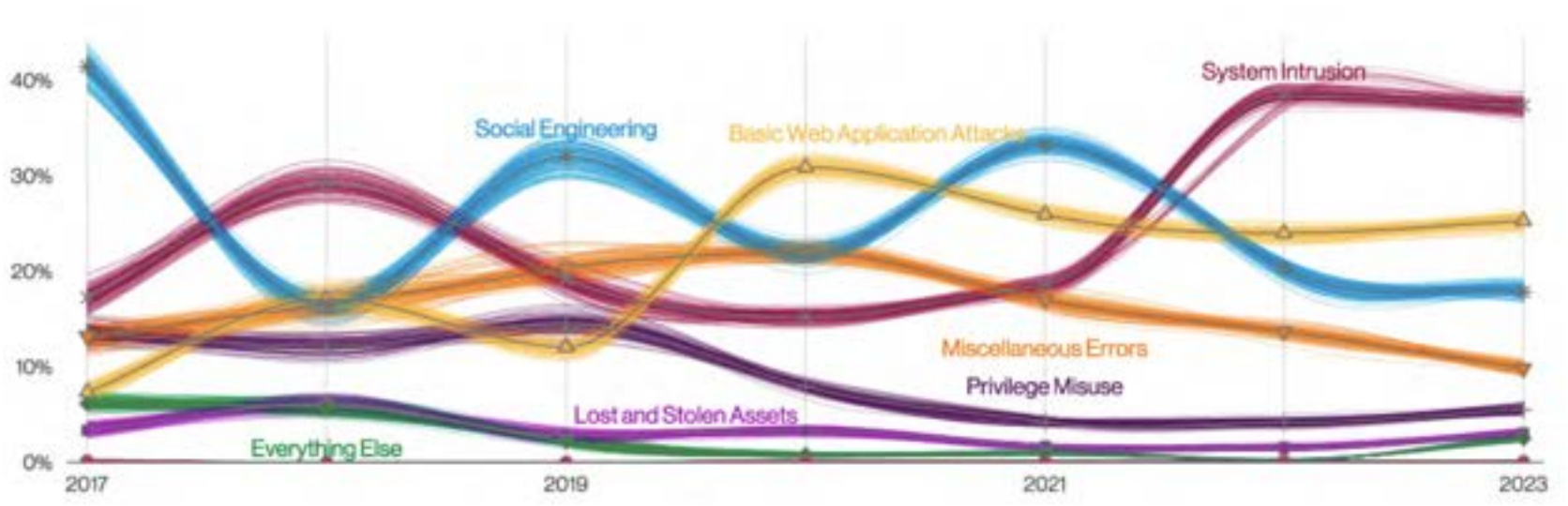


Figure 26. Patterns over time in breaches

Figure 26 from Verizon 2023 Data Breach Investigation Report[6]

HOW FILEVINE HELPS PROTECT YOU

1. Web Application Firewalls (WAF)

Filevine utilizes industry recognized WAF technology in blocking mode, to protect our platform against common web exploits such as SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF) and other OWASP Top 10 type attacks.[7]

The OWASP Top 10 are the most common security flaws that hackers try to exploit to gain unauthorized access to the site. Filevine leverages AWS Shield, Azure WAF on Application Gateway and GCP Cloud Armor AWF services to protect our respective platforms.

AWS SHIELD

AZURE WAF

GCP CLOUD ARMOR AWF

2. Managed Distributed Denial of Service (DDoS) Protections

In addition to these WAF services these same providers include managed DDoS protections to ensure our operating platform has always-on detection and automatic in-line mitigation that minimizes platform latency and potential downtime.

DDoS protection defends against common transport layer attacks targeting web platforms.

3. Secure Software Development Lifecycle (SDLC)

Filevine is adopting a secure SDLC methodology aligned with the OWASP Top 10.

Filevine developers attend annual training on OWASP Top 10 practices and software Architects perform peer code reviews on code so significant risks are often identified before going into production.

Filevine has invested in dynamic application security testing (DAST) and static application security testing (SAST) tools to reduce the likelihood of security defects making their way into production code. WAF, vulnerability scanning, and penetration testing are also utilized in a defense-in-depth approach to protect the Filevine platform.

4 . Separate Development, QA, Pre-Production & Production Environments

Filevine follows industry best practices by utilizing distinct and separate development lanes of the product for testing and performance testing.

Pre-Production environments do not, by policy, contain production data. Pre-Production data is masked or fabricated, unless required by the customer to use production data for testing purposes. Pre-Production data is destroyed shortly after a customer goes live on the platform.

5 . Code Escrow

Filevine utilizes best-in-class, third-party source code repositories which essentially hold our source code in escrow should anything happen to Filevine.

Although this is unlikely, customers can be reassured that the source code will be protected and accessible via a trusted third-party provider should the unthinkable happen.

6 . Penetration Testing

Filevine utilizes industry-recognized security experts to annually test the Filevine platform to ensure our websites, web applications, APIs, and related services are safe and secure.

We strategically use different white hat hackers to ensure we are getting a fresh approach to testing the platform. When findings do arise, we prioritize and resolve these issues programmatically.

7 . Enterprise Encryption

Filevine utilizes industry-recognized encryption to protect client data at rest and in transit throughout our product portfolio. Filevine utilizes the AWS Key Management Service (AWS KMS) to protect client documents with encryption at rest. This service supports Perfect Forward Secrecy (PFS) such as Ephemeral Diffie- Hellman (DHE) or Elliptic Curve Ephemeral Diffie-Hellman (ECDHE).[8]

At Rest Encryption
Filevine encrypts client data at-rest using FIPS 140-2 compliance AES 256 encryption, which should render any data, in the unlikely event it was stolen, unreadable by the attacker.

In Transit Data Encryption
Filevine supports encryption of client data in transit using TLS 1.2 or TLS 1.3, allowing for data to flow securely between the client's browser and the Filevine platform. TLS 1.0 and 1.1 are not enabled.

8 . Server-Side Verification

Application data is examined server-side to ensure that data coming from the customer is only properly formed data.

The server performs input validation and other checks to prevent unauthorized access or the injection of harmful data.

8 . Secured Data Sources

Your most critical information, such as your client database, should not be accessible to anyone on the internet. Filevine restricts access to critical resources from an authorized list of Filevine's web servers and IP addresses.

This means that when a user sends a request to the web server to access client data, the web server then sends that request to the backend data sources. If the computer that originally sent the request is not from that whitelist, the datasource will reject it. This provides an additional layer of security for the client data.

9 . Restricted Access to Production Data

Unauthorized and unnecessary access to your data is controlled within Filevine. We are guided by the principle of least privilege. We restrict access to the production Filevine environment to a limited number of Filevine administrators with a legitimate business need for authorized troubleshooting and break/fix purposes.

If a customer requests Filevine's support within their Filevine tenant, the customer is responsible to grant access to Filevine support representatives and then to revoke access to Filevine support representatives within their Filevine application tenant when the support issue is resolved.

10 . Secure Document Download and Folder Sharing

Each time an authorized Filevine user requests to download a document from Filevine, the system will check that user's permissions to ensure that they are authorized to download that specific document. After confirming, Filevine generates a unique URL for each download.

This unique URL is configurable to limit access based on the client's time specification to ensure that documents are not shared for longer than the client expects. Filevine allows customers to grant permissions to their guest users so

CHAPTER 4

Filevine Security Program Practices

As mentioned previously, the security landscape is constantly changing and new threats emerge daily. Filevine strives to take reasonable and proactive steps to protect our platform while understanding that information security is a shared responsibility.

We each have responsibilities to ensure we are only allowing users who are authorized to view or upload information into our platforms at the same time as managing user permissions and roles.

To further support the defense-in-depth security approach, Filevine has invested heavily in information security tools and practices and has adopted many security controls to better protect client data and to earnestly comply with our client's compliance, privacy and data protection requirements.

For more details, the Filevine information security team can be reached via email at security@filevine.com

HOW FILEVINE HELPS PROTECT YOU

1. Operational Security

Filevine maintains a Business Continuity Plan (BCP) and a Data Security Incident Response Plan, among other policies and procedures.

Our team of data security, compliance, and legal professionals recently completed our SOC2 Type II audit in Q3, 2022. In addition to SOC2, Filevine has also passed several Criminal Justice Information System (CJIS) security audits and customer requirements to meet FBI security obligations. Furthermore, Filevine has adopted the CIS 18 Critical Security controls and has successfully completed an external HIPAA Security controls audit ensuring that administrative, physical and technical safeguards are being utilized.

2. Vulnerability Management (VM)

Filevine utilizes enterprise grade vulnerability management tools to ensure the Filevine platform, websites and infrastructure are regularly scanned (usually weekly) for missing patches, application misconfigurations or other common security vulnerabilities.

Critical and High risk vulnerabilities or security findings are identified and remediated frequently, often within our standard patching cycle (usually within 30-45 days) to provide sufficient time to test the impact of the fix or patch in pre-production lanes before being released into production environments.

Moderate and Low risk vulnerabilities are reviewed and prioritized by the business for remediation against similarly impactful feature enhancements and functionality.

3 . Next Generation Endpoint Protection (NGEP)

Filevine utilizes multiple enterprise-grade, next generation, endpoint protection products to provide a high level of security to Filevine endpoints.

These services include advanced malware detection, threat intelligence, predictive machine learning models and anti-virus (AV) into a unified extended detection and response (XDR) platform. NGEP and XDR are used in tandem to significantly reduce the likelihood that malicious software can launch or propagate.

4 . Anti-Virus (AV)

In addition to the AV software used to protect Filevine laptops, and servers, Filevine utilizes two industry recognized anti-virus scanners to inspect documents and attachments uploaded into the Filevine platform.

These AV engines are designed to protect against malicious attachments uploaded into the Filevine project via email, SMS or documents uploaded via file folder sharing. These AV engines support scanning of very large files up to 16 GBs.

5 . Network Time Protocol (NTP)

Where possible, Filevine utilizes universal NTP servers to ensure time sources are consistent within disparate clouds and allow effective log correlation and aggregation to support Incident Response, monitoring and alerting efforts.

6 . Mobile Device Management (MDM)

Filevine utilizes enterprise grade MDM to manage, inventory, patch, encrypt and secure our Macintosh and Windows computers.

MDM enables Filevine to ensure configuration and security policies are technically enforced to protect the devices used to build and support Filevine systems and platforms.

7 . Intrusion Detection and Intrusion Prevention (IDS & IPS)

Filevine utilizes enterprise grade IDS to monitor network traffic within our VPC environments.

This monitoring is further augmented with blocking and prevention tools at the network, host and system levels to increase the security posture of the platform and our users' computing environments.

8 . Incident Response (IR) Team

Filevine has a trained and experienced team of incident handlers with multiple security certifications and years of experience managing incidents.

This team is very familiar with industry recognized tactics, techniques, and procedures (TTPs) to ensure security incidents are resolved in a timely and efficient manner. The team reviews numerous security alerts, events of interest (EoIs), significant events, and other incident types as we work through the IR process. Our IR team is aligning efforts to defend our platform by adopting

recently updated security best practices identified in the Mitre D3FEND "knowledge graph of cybersecurity countermeasures".[9] The D3FEND matrix identifies five risk reduction categories with associated countermeasures proven to reduce the likelihood and impact of security attacks. These categories include:

MITRE | D3FEND™

Harden | Detect | Isolate | Deceive | Evict

9. Enterprise Logging & Security Incident & Event Management (SIEM)

Filevine utilizes multiple, best-in-class solutions to support enterprise logging and IR efforts.

Filevine has deployed enterprise logging and SIEM technologies to increase visibility, aggregate, organize and prioritize network and system events to allow our teams to respond to alerts and potential threats in a timely manner.

We maintain in-house Security Operation staff to triage security alerts and we have aligned our security program with the MITRE ATT&CK Matrix framework, best practices for detection and response using the fourteen tactical domains and 215 techniques.[10] These tactics include the following:

MITRE | ATT&CK®

1	Reconnaissance	8	Credential Access
2	Resource Development	9	Discovery
3	Initial Access	10	Lateral Movement
4	Execution	11	Collection
5	Persistence	12	Command and Control
6	Privilege Escalation	13	Exfiltration
7	Defense Evasion	14	Impact

they can download documents. Filevine users can also determine how long download links will be valid. Furthermore, documents shared with Filevine secure links can be individually password protected and secured as well.

11. Secure Document Upload

Filevine utilizes the web standard cross-origin resource sharing (CORS) to ensure uploads originate only from Filevine and cannot be uploaded from other browsers or web pages.

File uploads can be performed by Org Admins and authorized Filevine users who have been granted the corresponding permissions. All files are encrypted "in transit," and with AES 256 for "at rest" storage.

12. Document Backup and Recovery Testing

Filevine understands how important documents and work products are to our customers. As a result, Filevine utilizes a belt and suspenders model for document and database backup.

Documents stored in AWS S3 benefit from the standard 11 nines of durability, as well as cross region backup to a separate and distinct S3 high availability zone every 15 minutes. This approach offers high availability within the region and high availability across other regions in the event of a disaster.

Similarly, high availability database clusters are also backed up to other regions for fault tolerance. These backups, together, are tested annually, or more often as part of our Incident Response process or our standard SOC 2 Type II testing.

13. Status Monitoring

Filevine regularly reviews the status of the Filevine platform. We have provided a status webpage to ensure customers are apprised of potential issues.

The site can be reached here: https://status.filevine.com/. Customers may also subscribe to the notification service to receive near real-time alerts.

View of status.filevine.com

14 . User Controlled Defenses

Filevine has implemented multiple features in the platform to allow customers to block SPAM email messages, text messages, malicious senders, domains, and other unwanted messages from entering the platform.

Additional layers of protection are continuously being added to verify incoming messages are from members of the project or Org within the Filevine platform and other security related features.

With these investments to address three of the most common cybersecurity risk areas for our customers, Filevine is well-positioned as a leader in the case management platform vertical, delivering a robust, secure, and compliant legal core platform to our clients.

While our IR team has not fully adopted these tactics and techniques from the Mitre ATT&CK and D3FEND frameworks, we are constantly improving our IR processes and implementing these techniques as we diligently strive to prevent, identify and stop potential attacks before they cause harm or disruption.

10 . Credit Card Security

Filevine does not store customer credit card information on its servers and it is not intended to be a credit card storage system. However, the Outlaw and Vinesign self-service products and the upcoming Filevine Payments module do allow for credit card payments via the Stripe API.

4.0

Stripe is a PCI Data Security Standard (PCI DSS) Level 1 service provider. This is the most stringent level of certification available in the payments industry to ensure companies that process, store or transmit credit card information maintain a secure environment. See Security at Stripe[11] for more information.

Filevine has completed our PCI DSS 4.0 SAQ - Type A for 2023 and will continue to monitor and assess PCI compliance as applicable, annually.

11 . Enterprise Security Awareness & Phishing Training

Filevine provides ongoing security awareness training to its workforce to keep pace with evolving cyber threats.

We have implemented a best-in-class security awareness training platform, formalized our awareness program and created curriculum including but not limited to the following:

1	Annual security awareness training campaigns
2	Monthly phishing campaigns with remediation training
3	Additional remediation training for repeat offenders
4	OWASP Top 10 training for developers
5	Product specific training and awareness

12 . Risk Assessments (RA)

Filevine performs an annual risk assessment on Filevine systems. The RA report is used to identify risks in its areas of responsibility and to implement appropriate changes to mitigate risks prioritized by the business.

Filevine reevaluates the risk assessment and risk assessment process annually or when otherwise necessary to both update the previous results and to identify new areas of concern. The risk assessment process consists of the following phases:

Identifying
The identification phase includes listing out risks (including threats and vulnerabilities) that exist in the environment. This phase provides a basis for all other risk management activities.

Assessing
The assessment phase considers the potential impact(s) of identified risks to the business and its likelihood of occurrence.

Mitigating
The mitigation phase includes putting controls, processes, and other physical and virtual safeguards in place to prevent and detect identified and assessed risks.

Reporting
The reporting phase results in risk reports provided to managers with the necessary data to make effective business decisions and to comply with internal policies and applicable regulations.

Monitoring
The monitoring phase includes Filevine management performing monitoring activities to evaluate whether processes, initiatives, functions and/or activities are mitigating the risk as designed.

13 . Third-Party Risk Management (3PRM)

Similar to the Filevine Risk Assessment process, Filevine performs 3PRM risk assessments whenever Filevine contracts with a third party. This process includes input from business stakeholders including the Legal, Finance, and Information Security teams.

Vendor and supplier risk is managed with a best-in-class third-party risk management platform as well as using industry standard security questionnaires, audit report reviews and in-depth and sometimes on-site technical interviews. Our 3PRM process is intended to be thorough and to identify key business risks to Filevine stakeholders so they can make educated and informed decisions when selecting business partners with whom to work.

14 . Filevine Security Council

As stated previously, Filevine's Executive team, Board of Directors and employees are very committed to information security, privacy, compliance and protecting customer data. This top-down approach is demonstrated through quarterly business reviews (QBRs) and the establishment of the Filevine Security Council.

The charter of this committee clearly states their responsibilities are,

"To manage the risk of securing Filevine's intellectual property and customer data in accordance with required regulations, contractual obligations, and industry best practices for a company of Filevine's size by prioritizing risk remediation projects, accepting residual risk, and avoiding material security breaches."

This Council is authoritative and governs the affairs of Filevine's information

security program. Business and security risks are discussed in monthly meetings designed to bring appropriate stakeholders together to raise awareness and when needed, to take action to manage these risks appropriately or to marshall support for new security features or investments.

15 . Cyber Security Insurance

Filevine has made significant investments in cyber security insurance in the unlikely event of an unforeseen business impacting security event.

This insurance provides up to $10MM in protection to ensure Filevine can continue to conduct business as usual, while attending to any unexpected financial demands or losses as a result of the incident.

CHAPTER 5

Privacy Program Considerations

Filevine endeavors to comply with state, federal and international privacy requirements. Filevine has appointed a Data Privacy/Data Protection Officer (DPO) to lead privacy efforts.

Filevine has established a privacy program, including privacy by design initiatives and privacy assessments for numerous privacy regimes:

1	California data security regulations, Cal. Civ. Code §1798.81.5
2	California Consumer Privacy Act of 2018 and subsequent regulations (“CCPA/CPRA”)
3	Connecticut data security regulations, C.G.S.A § 36a-701b
4	Data protection agreement (DPO) implications
5	Family Educational Rights and Privacy Act (FERPA) privacy implications
6	General Data Protection Regulation (GDPR) privacy implications
7	Protection of Personal Information of Residents of the Commonwealth of Massachusetts, 201 CMR 17.00
8	New York SHIELD Act, N.Y. Gen. Bus. Law § 899-bb.
9	Oregon data security regulations, O.R.S. 646A.600 et. seq.,
10	Rhode Island Identity Theft Protection Act, RIGL § 11-49.3-1 et seq.
11	Social Security Administration (SSA) privacy implications.
12	Standard Contractual Clauses (SCC) requirements.
13	New York SHIELD Act, N.Y. Gen. Bus. Law § 899-bb.

In many instances, Filevine has retained expert external legal and privacy counsel to augment the internal general counsel and DPO feedback on privacy risks. Filevine strives to be informed of privacy implications and to do the right thing concerning privacy for our

customers and our customers' customers.

Filevine has standard Terms and Conditions and a Privacy Policy to provide additional guidance on how we protect and manage customer data, use cookies and any client data entrusted to us.

Filevine enters into Data Protection/Data Processing agreements and Standard Contractual Clauses whenever required by customers to ensure the confidentiality of customer data.

GDPR and CCPA implications regarding cookies, consent, right to be forgotten actions and many other considerations are also addressed in the Privacy Policy.

You can also reach Filevine's Privacy team via email: privacy@filevine.com

CHAPTER 6

Compliance Program Considerations

Filevine uses best-in-class cloud service providers that individually have their own compliance and security programs. Filevine utilizes different cloud platforms to operate distinct Filevine products so if one cloud experiences slowness or security issues, the other Filevine products should not be affected significantly.

These cloud platform partners independently ensure their security and compliance posture and they have dozens of compliance attestations. These can be found here: AWS (security and compliance), GCP (security and compliance), and Microsoft Azure (security and compliance).

At the same time, Filevine endeavors to comply with contractual, state, federal and international compliance requirements with respect to our use of these cloud partners.

Filevine has a dedicated compliance team which conducts audits year round to assess our security program's effectiveness and the effectiveness of our trusted partners. Filevine has established a Privacy program and privacy assessments have been completed for numerous privacy regimes:

1. Written Information Security Policies and Procedures (WISP)

To support Filevine's Compliance and Information Security programs, we have created a detailed set of information security policies and procedures to help govern the secure operations of our platform.

These security policies govern how we manage the confidentiality, integrity, and availability triad (CIA) as well as the two other Trust Services Criteria for processing integrity and availability. These security policies and procedures are aligned with NIST 800-53 / Cyber Security Framework (CSF) Moderate standards and include but are not limited to the following:

1	Acceptable Encryption	12	Internal Audit
2	Acceptable Use	13	Internal Control
3	Access Control	14	Mobile Device Encryption
4	Change Control & Configuration Management	15	Network Security
5	Code of Corporate Ethics	16	Passwords
6	Customer Support and SLA	17	Product/Services Scope
7	Data Retention and Destruction	18	Removable Media
8	Incident Response	19	Risk Assessment
9	Information Security Program Management	20	Software Development Life Cycle
10	Information	21	System & Communication Security
11	Sensitivity	22	Vendor Management

These policies and procedures are documented in our Information Security Management System (ISMS) and they are reviewed and updated annually or as required.

2 . HIPAA / HITECH Compliance

Filevine should not be considered as a “covered entity” as described in the HIPAA Security Rule and subsequent legislation.

However, in some cases, Filevine does operate as a business associate (BA) and more often than not, as a sub-business associate (SBA) for our customers helping their clients with medical cases. In that capacity, Filevine may enter into business associate agreements (BAAs) with those customers.

To further this point, Filevine does not collect health or electronic personal health information (ePHI) records from our customers. Records stored in the Filevine platform are encrypted, removing our visibility into the nature of these documents. It is our understanding that some customers may collect, process or store health records in Filevine. As a result we endeavor to comply with the Technical, Physical and Administrative safeguards contemplated in the HIPAA Security Rule. As applicable, Filevine endeavors to comply with the following safeguards:

Administrative Safeguards[13]

Security Management Process
A covered entity must identify and analyze potential risks to ePHI, and it must implement security measures that reduce risks and vulnerabilities to a reasonable and appropriate level.

Security Personnel
A covered entity must designate a security official who is responsible for developing and implementing its security policies and procedures.

Information Access Management
Consistent with the Privacy Rule standard limiting uses and disclosures of PHI to the “minimum necessary,” the Security Rule requires a covered entity to implement policies and procedures for authorizing access to ePHI only when such access is appropriate based on the user or recipient's role (role-based access).

Workforce Training and Management
A covered entity must provide for appropriate authorization and supervision of workforce members who work with ePHI. A covered entity must train all workforce members regarding its security policies and procedures, and must have and apply appropriate sanctions against workforce members who violate its policies and procedures.

Evaluation
A covered entity must perform a periodic assessment of how well its security policies and procedures meet the requirements of the Security Rule.

Physical Safeguards

Facility Access and Control
A covered entity must limit physical access to its facilities while ensuring that authorized access is allowed.

Workstation and Device Security
A covered entity must implement policies and procedures to specify proper use of and access to workstations and electronic media. A covered entity also must have in place policies and procedures regarding the transfer, removal, disposal, and re-use of electronic media, to ensure appropriate protection of electronic protected health information (ePHI).

Technical Safeguards

Access Control
A covered entity must implement technical policies and procedures that allow only authorized persons to access electronic protected health information (ePHI).

Audit Controls
A covered entity must implement hardware, software, and/or procedural mechanisms to record and examine access and other activity in information systems that contain or use ePHI.

Integrity Controls
A covered entity must implement policies and procedures to ensure that ePHI is not improperly altered or destroyed. Electronic measures must be put in place to confirm that ePHI has not been improperly altered or destroyed.

Transmission Security
A covered entity must implement technical security measures that guard against unauthorized access to ePHI that is being transmitted over an electronic network.

Depending on the situation, Filevine may enter into BAA, or Sub BAAs as needed.

3. SOC 2 Type II

Annually, Filevine participates in SOC 2 Type II audits including all five Trust Services Criteria (TSC) including: Information Security, Privacy, Processing Integrity, Confidentiality and Availability.

These audits are conducted by an independent, AICPA certified auditing firm. As part of the SOC 2 audit, Filevine is required to have an external penetration testing company to independently inspect and test the Filevine software platforms, including all Filevine, LeadDocket, Vinesign and Outlaw product suites.

The 2022 SOC 2 Audit report, for the reporting period September 1, 2021 to August 31, 2022 included +HIPAA, +CJIS and +ISO security control to ensure we were following the requirements for the HIPAA Security and Privacy Rules and subsequent HiTECH controls. In addition, the audit included testing the CJIS security controls for the second year in a row.

For the 2022 audit, we added the ISO 27002 security controls. In 2023 additional audit controls are being added for ISO 27017, ISO 27018, CSTAR and additional security and compliance frameworks.

4 . E-Sign Act - eSignature Compliance

Electronic signatures (eSignatures) have become ubiquitous and widely accepted for business use in our modern digital age. While the acceptance of eSignature use is common, there are a plethora of use cases in which an eSignature must be verified with a higher level of compliance.[13]

To meet these assurance demands, eSignature standards have been developed and adopted as trusted frameworks that accurately help regulate these digital procedures. The European electronic Identification, Authentication and trust Services (eIDAS) is a European Union regulation that has led the way for the verification of electronic transactions. Among the several different security layers that eIDAS has yielded, there are two that play a critical role to Filevine's eSignature assurance: Simple Electronic Signature (SES) and Advanced Electronic Signature (AES).

Simple Electronic Signature (SES)
SES is seen as the foundation for eSignature compliance, offering the simplest level of requirement to ensure the identity of an electronic signer. eIDAS describes and eSignature under SES as:

"Data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign."

Advanced Electronic Signature (AES)
AES includes a stronger emphasis on verifying signer identification, which prevents the forgery of an electronic signature. In addition to uniquely identifying and connecting the signer, AES maintains a link to the signed data that will trigger notifications of changes, enabling a more dependable and truthful eSignature experience.

As part of this connection process, AES typically involves public-key infrastructure (PKI) technology to employ certificates and cryptographic keys for the security of the signature.

Qualified Electronic Signature (QES)
QES provides users with an advanced level of eSignature verification. This is possible because:

- The signature is executed by a certified signer
- The executed signature is based on a Qualified Signature Creation Device (QSCD)
- By adding a stronger influence on certifying the people and technology parts of an eSignature process, QES affords the most compliant and regulated form of digital signature available. As such, a QES is considered to have nearly equal legal implicity as a traditional handwritten signature.

> **eSignature Regulation at Filevine**
> Filevine's electronic signature solutions meet electronic signature standards intended to protect our customer and ensure documents are legally binding and admissible in court.

5 . ISO 27001/2 Compliance and Certification

In 2022 Filevine included the ISO 27002 technical controls in the SOC 2 Type iI audit. The report indicated that Filevine was compliant with the controls.

In 2023, Filevine is striving to complete the ISO 27001 Certification process. We have documented our statement of applicability and have mapped our security controls to the ISO 27002 control set in addition to the NIST 800-53 Moderate control set. We anticipate this audit work will be completed in Q4, 2023, including certification.

Thank you for taking this journey with us through the Filevine information security, privacy and compliance programs. As you can tell, we really care alot about protecting Filevine and our clients from those who wish to cause us harm. We are constantly striving to make our defenses stronger and to evolve ourselves as the security threats around us evolve.

If you believe there are things we still need to do, Please reach out to security@filevine.com or your Filevine Account Manager and let us know. They can also be reached to provide a copy of this report, our SOC 2 Type II report or to help answer any other questions you may have. Thanks again!

APPENDIX

Security Certifications & References

References

1	ABA Rule 1.6: Confidentiality of Information
2	AWS Compliance Programs
3	High availability and scalability on AWS
4	AWS Compliance Programs
5	AWS Overview of Security Processes
6	Verizon Data Breach Investigations Report (DBIR) 2023
7	OWASP Top Ten
8	Infrastructure security in AWS Key Management Service
9	MITRE D3FEND
10	MITRE ATT&CK
11	Security at Stripe
12	HIPAA Security Series: 6 Basics of Risk Analysis and Risk Management
13	Electronic Signature Security with Filevine

If you have questions about security, privacy, compliance or the other ways that Filevine can help your practice, give us a call 801-657-5228 or email us at info@ filevine.com or security@filevine.com