Kiteworks

COMPLIANCE BRIEF

Meeting the Safeguards Rule for Customer Data Protection With Kiteworks

A Turnkey Solution for Financial Institutions to Meet the June 9, 2023, Deadline for Customer Data Protection as Laid Out by the Newly Revised FTC Safeguards Rule

New Data Protection Requirements for Financial Institutions and Penalties for Noncompliance

The newly updated FTC Safeguards Rule (revised November 15, 2022) requires financial institutions to have an information security plan in place by June 9, 2023, that includes products, processes, and procedures for protecting customer data and responding to security incidents. Kiteworks offers a range of features and tools to help organizations implement and maintain necessary safeguards, including detection and prevention of unauthorized access of file and email data containing sensitive customer information, which includes:

1. **Easily Meeting the Safeguards Rule's Access Control Requirements**
   The Safeguards Rule requires financial institutions to implement and review technical access controls to authenticate and limit access to authorized users only. Kiteworks offers features such as granular content access controls, email policies, role-based permissions, file type filtering, account expiration, block and allow lists, geofencing, password security, key rotation, and more to help financial institutions secure and manage access to their customers' data stored and shared in files or emails It also has FedRAMP Moderate Authorization and undergoes annual audits to ensure compliance with regulations and controls.

2. **Seamlessly Managing Customer Data and Protecting Against Unauthorized Accesss**
   The FTC Safeguards Rule requires financial institutions to identify and protect customer data against unauthorized access. The platform provides financial institutions with tools to organize and manage their information, such as creating folders with customizable permissions, adding tags and metadata to files, file versioning, user access controls, activity logs, and audit trails, to classify, track changes, and monitor user activity and compliance with the regulations.

3. **Automatically Protecting Customer Data in Transit and at Rest With Built-in Encryption**
   The FTC Safeguards Rule requires financial institutions to protect customer data in transit and at rest through encryption. Kiteworks uses various encryption methods, such as double encryption at the volume and file level, TLS for network communication, and SFTP encryption for data transfer.

4. **Ensuring Secure Development and Testing of In-house and Externally Developed Applications**
   The FTC Safeguards Rule requires financial institutions to conduct annual penetration testing and vulnerability assessments. Kiteworks follows secure development practices, incorporates DevSecOps best practices, and uses continuous monitoring by an authorized third party, periodic penetration testing, and vulnerability assessments to identify and prioritize vulnerabilities in the code during development, remediate them before deployment, and maintain the highest level of protection. It also uses ongoing bounty programs and remediation of potential threats in production to manage risk at the lowest possible level.

Kiteworks is unequivocally the first choice for any financial institution looking to ensure regulatory compliance with the FTC and effectively manage risk in every send, share, receive, and save of sensitive customer data.