FTC Extends Effective Date of Safeguard Rule Amendments to June

November 22, 2022

The Federal Trade Commission (FTC) has announced that the effective date for the new substantive information security requirements in the revised Safeguard Rule has been extended from December 9, 2022 to June 9, 2023.

This extension provides financial institutions subject to the Safeguards Rule with additional time to build out their safeguards programs in compliance with the amended rule. The FTC extended the deadline after receiving feedback that financial institutions have a shortage of qualified personnel to implement the required information security programs. In addition, the FTC recognized that supply chain issues may lead to delays in covered entities obtaining the equipment necessary to upgrade security systems and implement the changes. New requirements under the amended rule that have caused covered entities particular implementation issues are those related to multi-factor authorization and protecting customer information through encryption. Because of these challenges, the FTC stated that the circumstances "may make it difficult for financial institutions, especially small ones, to come into compliance by the deadline."

By way of background, the Safeguard Rule generally requires non-banking financial institutions to implement, maintain, and develop a security program to safeguard customer information. The Safeguard Rule amendments build on the requirements under the original rule with respect to the following areas:

Qualified Responsible Individual and Periodic Reports. A covered entity must designate a qualified individual responsible for overseeing, implementing, and enforcing its information security program. The qualified individual may be employed by the covered entity, an affiliate, or a service provider. The entity must also require its qualified individual to submit a written report, regularly and at least annually, to the entity's board of directors or equivalent governing body, with certain required information.

Risk Assessments. A covered entity must base its information security program on a written risk assessment that includes certain required elements. An entity must also periodically perform additional risk assessments that reexamine reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information.

In addition, an entity must design and implement specific safeguards to control the identified risks, including by: (1) implementing and reviewing access controls; (2) identifying data, personnel, and other factors that enable the entity to achieve business purposes; (3) protecting all customer information by encryption (or if encryption is not feasible, through effective alternative controls); (4) adopting secure development practices; (5)

implementing multi-factor authentication (or if not feasible, reasonably equivalent controls); (6) developing procedures for the secure disposal of customer information generally no later than two years after the last date the information is used; (7) adopting procedures for change management; and (8) implementing policies, procedures, and controls designed to monitor and log the activity of authorized users and detect unauthorized access or use of information by such users.

Testing and Monitoring of Safeguards. A covered entity must regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures, including those to detect actual and attempted attacks on, or intrusions into, information systems. Information system monitoring and testing must include continuous monitoring or periodic penetration testing and vulnerability assessments.

Policies and Procedures. A covered entity must implement policies and procedures to ensure that personnel are able to enact the entity's information security program by: (1) providing personnel with security awareness training; (2) using qualified information security personnel; (3) providing information security personnel with security updates and training; and (4) verifying that key information security personnel take steps to maintain current knowledge of changing threats.

Overseeing Service Providers. The amendments add a requirement related to periodically assessing service providers based on the risk they present and the continued adequacy of their safeguards.

Incident Response Plan. A covered entity must establish a written incident response plan designed to promptly respond to, and recover from, any security event materially affecting the confidentiality, integrity, or availability of customer information in the entity's control. The incident response plan must include a number of different requirements as listed in the amended Rule.

Overall, while the amended rule imposes additional requirements and presents implementation burdens, it also provides covered entities with more guidance regarding how to develop and implement specific aspects of their overall security program.

Related people

Aaron P. Kouhoupt

Paul J. Lysobey

David Tallman