Published on *The National Law Review* https://natlawreview.com

FTC Delays Compliance Date of the Safeguards Rule

Article By:

Timothy A. Butler

On Nov. 15, 2022, the Federal Trade Commission (FTC) announced that it is delaying the effective date of its recent amendments to the Safeguards Rule, promulgated under the Gramm-Leach-Bliley Act (GLBA).

Go-To Guide:

- The Safeguards Rule compliance deadline is delayed by six months
- Eight subsections of the Safeguards Rule are affected by the delay
- The new effective date for compliance is June 9, 2023
- The FTC cited implementation challenges for small business as the reason for the delay.

GT reported in November 2021 on the detailed requirements of the amended Safeguards Rule, another in a series of efforts by state and federal governments to move away from mandating generic security requirements in favor of specific data security measures.

Originally set to take effect Dec. 9, 2022, eight of the requirements will now be delayed until June 9, 2023. The FTC reevaluated the effective date after covered financial institutions voiced concerns regarding their inability to comply due to the economic impact of COVID-19, a shortage of qualified information security personnel, and supply chain issues in procuring the necessary technology to upgrade systems.

The following subsections of the Safeguards Rule are now effective June 9, 2023:

- **Designation of a Responsible "Qualified Individual"** (16 C.F.R. § 314.4(a)) – generally understood to be Chief Information Security Officer, or someone responsible for the implementation and oversight of the information security program;
- **Requirement that the Qualified Individual submit regular (at least annual) written reports to the financial institution's board of directors** (16 C.F.R. §314(i)) – the reports

would include the overall status of the infosec program, Safeguards Rule compliance, and material matters re the infosec program;

- **Development of written risk assessments** (16 C.F.R. §314.4(b)(1)) – the FTC outlines certain criteria and mitigation follow through based on the risk assessment results;

- **Using the risk assessments to design and implement safeguards to protect customer information** (16 C.F.R. §314.4(c)) – several of the requirements listed include access controls, data management principles, encryption of customer information at rest and in transit, privacy by design controls for in-house applications, multi-factor authentication, secure disposal of customer information (record retention and data minimization techniques, including regular review of data retention policy), change management procedures, and log activity reviews to detect unauthorized access to or tampering with customer information;

- **Continuous monitoring, or annual penetration testing with bi-annual vulnerability scans** (16 C.F.R. § 314.4(d)(2));

- **Security awareness training for employees, including risk-based training for information security personnel** (16 C.F.R. § 314.4(e)) – also requires hiring qualified infosec personnel or service provider;

- **Periodic assessment of third-party service providers' risks and adequacy of their cybersecurity programs** (16 C.F.R. § 314.4(f)(3); and

- **Establish a written incident response plan (IRP)** (16 C.F.R. § 314.4(h) – the IRP should include the goals, processes for responding to security event, definition of roles and responsibilities, communication and information sharing, remediation, documentation, and IRP revision as necessary.

While financial institutions gained a bit more breathing room to meet the FTC's amended compliance requirements under the Safeguards Rule, they have just under six months to put the above measures in place.

Tessa L. Cierny also contributed to this article.

National Law Review, Volume XIII, Number 5

Source URL:https://natlawreview.com/article/ftc-delays-compliance-date-safeguards-rule