CARLTON FIELDS

FTC Sharpens Its Cyber Enforcement Tool by Amending and Expanding the Safeguards Rule

November 04, 2021

In the culmination of a process that began in 2016, the Federal Trade Commission (FTC) last week issued a final rule to amend the Standards for Safeguarding Customer Information under the Gramm-Leach-Bliley Act. The Safeguards Rule requires non-banking financial institutions under FTC jurisdiction, such as payday lenders and mortgage brokers, to have measures in place to keep customer information secure.

Amendments to the Safeguards Rule

On October 27, 2021, the FTC voted 3–2 to amend the Safeguards Rule to "better protect the American public from breaches and cyberattacks." Using the New York State Department of Financial Services cybersecurity requirements as its model, the FTC has five main modifications to the existing Safeguards Rule.

1. The amended rule requires covered institutions to implement specific safeguards as part of their written information security program (WISP), including access controls, authentication requirements, and "encryption to secure ... data."
2. The amended rule also aims to improve the accountability of WISPs by requiring institutions to explain their information-sharing practices in additional detail. It also requires periodic reporting to the board of directors of the overall status of the company's WISP and compliance with the rule, among other material matters.

3. The amended rule carves out an exemption for financial institutions that maintain customer information for fewer than 5,000 customers. Under the exemption, certain provisions, such as those requiring monitoring and periodic penetration testing, do not apply to those small businesses.

4. It requires the designation of a single qualified individual to oversee the company's WISP, whereas the prior version of the rule requires companies to designate "one or more" individuals for this role.

5. Finally, the FTC expanded the rule's scope by amending the definition of "financial institution" to include entities engaged in activities that the Federal Reserve Board determines to be incidental to financial activities, such as "finders" — companies that bring together buyers and sellers of a financial product (if that product falls within the scope of the rule). The updated definition aligns with other federal agencies' safeguards rules, which already include such activities in their definition of a financial institution.

Proposed Notification Requirement

In addition to the issuance of the amended Safeguards Rule, the FTC issued a notice of supplemental rulemaking, for a rule that would require covered institutions to report certain cybersecurity events to the agency. Under the proposal, if the company determines that customer information has been, or is reasonably likely to be, misused and that 1,000 or more consumers have been, or reasonably may be, affected by the incident, it must report the event to the agency "as soon as possible and no later than 30 days" following discovery. The proposed standard for reporting harmonizes the current standard for customer notices under the Interagency Guidelines Establishing Information Security Standards.

Significance

Companies have 30 days or one year from publication in the Federal Register, depending on the provision, to comply with the amendments. Once the amended rule takes effect, the legal risk from noncompliance is substantial. In the meantime, covered institutions should familiarize themselves with the Safeguards Rule and review their WISPs to ensure compliance. As to the proposed notification requirement, commenters will have 60 days to submit comments once the notice is published in the Federal Register.

Authored By

John E. Clabby

Eden Marcu

Related Practices

Cybersecurity and Privacy
Banking, Commercial, and Consumer Finance

Related Industries

Banking, Commercial, and Consumer Finance