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

FTC Strengthens Data Security Requirements

Article By:

Chanley T. Howell

Christi A. Lawson

John J. Atallah

The Federal Trade Commission (FTC) recently published changes to data security requirements for financial institutions by revising the Safeguards Rule (Rule) under the Gramm-Leach-Bliley Act (GLBA). The law is designed to protect the privacy and security of consumer financial information when dealing with financial institutions. The scope of covered financial institutions is broad and includes a wide spectrum of companies in the financial industry, not just banks. In adopting the new security rules, the FTC recognized that "[i]n recent years, widespread data breaches and cyberattacks have resulted in significant harms to consumers, including monetary loss, identity theft, and other forms of financial distress."

Highlights

- The amendments to the Rule contain numerous specific and relatively detailed requirements for compliance, such as developing a written information security program and appointing a "Qualified Individual" (*e.g.*, a Chief Information Security Officer) to oversee and implement the program, encryption, and multifactor authentication
- While the Rule has always applied to "financial institutions" with a broader scope than just banks (for example, credit reporting agencies are covered), the definition has been expanded to cover companies that substantially engage in activities "incidental to" financial activities, such as "finders" that bring together buyers and sellers of a financial product or service
- While the Rule does not require reporting of data security incidents, the FTC has requested comments on whether in the future it should require covered financial institutions to report certain data breaches and other security incidents
- The modifications bring the Rule more in line with other data security laws and industry standards

- Many new requirements are effective 30 days after publication of the amended Rule in the Federal Register, and more significant changes go into effect one year from publication

Previously, the Rule was light on details and contained only general language requiring companies to implement appropriate data security measures. This led to uncertainty among and within the financial industry, with ad hoc rulings and guidance being issued by the regulators. The new Rule contains detailed requirements, including that covered financial institutions must:

- Develop, implement, and maintain a comprehensive information security program
- Designate a Qualified Individual responsible for overseeing and implementing the program
- Require the Qualified Individual to regularly (at least annually) report to the board of directors, or equivalent, on all security events that happened over the last year
- Conduct a risk assessment that identifies reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information
- Implement and periodically review access controls
- Create an inventory of and manage data, personnel, and devices which impact data privacy and security
- Encrypt all customer information held or transmitted by the company both in transit over external networks and at rest (in storage)
- Adopt secure development practices for in-house software development applications
- Implement multifactor authentication for individuals accessing the company’s information system
- Adopt a written incident response plan
- Securely dispose of customer information in accordance with written policies and procedures
- Implement a data retention policy to minimize unnecessary retention of data
- Adopt procedures for managing and controlling changes to the company’s data security safeguards
- Monitor and log activity of authorized users to detect unauthorized use of or tampering with customer information
- Test and monitor effectiveness of the organization’s data security program
- Conduct training and awareness exercises for all relevant personnel
- Oversee vendors and service providers with respect to data security safeguards and controls

- Evaluate and adjust the information security program as needed due to changes in the organization and security threats

The Rule expands the definition of “financial institution” to include entities engaged in activities that the Federal Reserve Board determines to be “incidental to” financial activities. A company will fall under the definition of financial institution if it is “significantly engaged in activities incidental to” financial activities. This change adds entities such as “finders” — companies that bring together buyers and sellers of a product or service — within the scope of the Rule. This type of activity has greatly increased with the significant development and expansion of the Internet and online marketing over the past several years since the Rule was first adopted. Finders often collect and maintain very sensitive consumer financial information, and this change will require them to comply with the Safeguards Rule’s requirements to protect that information.

A particular area of concern of the business community regarding revisions to the Rule was the extent to which companies are required to report data security breaches. The industry and the FTC recognize the potential friction between the benefits of sharing information relating to security breaches and the confidentiality and security concerns that are inherent when such information is provided to the government or made public. The FTC did not promulgate rules in this regard, but is seeking comment on whether financial institutions should be required to report certain data breaches and other security events.

The Rule was perhaps overdue for an update, with no modifications since its passage in 1999. The revisions bring the Rule more in line with data security regulations, including those under HIPAA and New York’s cybersecurity regulation, as well as prevailing industry standards such as the NIST Cybersecurity Framework and ISO/IEC 27001. While the new requirements apply to companies governed by the GLBA, it provides additional guidance and support for data security measures and safeguards that should be considered and adopted by organizations in all industries.

Effective Date

Some aspects of the amended Rule, including those that relate to implementing safeguards, undertaking a written risk assessment, appointing a Qualified Individual, and conducting continuous monitoring or annual penetration testing, are effective one year after the date of publication (thus, in October 2022). The other portions are effective 30 days after publication.

© 2025 Foley & Lardner LLP

National Law Review, Volume XI, Number 314

Source URL:https://natlawreview.com/article/ftc-strengthens-data-security-requirements