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

With Updated Safeguards Rule, FTC Signals New Wave of Cybersecurity Enforcement for Financial Institutions

Article By:

Jena M. Valdetero

Jessica D. Pedersen

Takeaways

- The FTC has expanded the definition of “Financial Institutions” to include more types of companies, although smaller companies remain exempt from more onerous requirements.
- Financial institutions must designate a “qualified individual” to oversee their cybersecurity compliance.
- Companies must have a written information security plan, an incident response plan, and a written risk assessment.
- More specific security measures are required, including multi-factor authentication, logging, monitoring or scanning and testing.
- Employee training is a must.
- Vendor management and oversight will be key.

On Oct. 27, 2021, the Federal Trade Commission (FTC) amended its Standards for Safeguarding Customer Information (the “Safeguards Rule”), promulgated under the Gramm-Leach-Bliley Act (GLBA). The updated Safeguards Rule is yet 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.

The data security requirements will look familiar to any company already regulated by other cybersecurity laws or regulations, like the New York Department of Financial Services Cybersecurity Regulation, but there are likely new requirements in the Safeguards Rule for most companies subject to the Rule.

The prior version of the Safeguards Rule required financial institutions to implement a written comprehensive information security program appropriate for the size and complexity of the financial institution, setting forth the administrative, technical, and physical safeguards used to protect customer information against unauthorized use or access that could result in substantial harm to customers.

The updated Safeguards Rule now contains additional specifics that must be included in the information security program on how the program must be implemented.

Specific Information Security Program Requirements

The new Safeguards Rule sets forth detailed requirements for a financial institution's information security program. Per the Rule, written information security plans must now contemplate:

- Access controls to authenticate and permit access only to authorized users and to limit authorized users' access only to information such users need to know;
- Identification and management of data, personnel, devices, systems, and facilities that enable the financial institution to achieve business purposes in accordance with their relative importance to business objectives and risk strategies;
- Encryption of all customer information held or transmitted over external networks and at rest (or, in some cases, compensating controls);
- Secure development practices for internally developed applications and procedures to test the security of externally developed applications;
- Multi-factor authentication (or a reasonably equivalent or more secure access control);
- Secure procedures for disposal of customer information and the disposal of customer information two years after the last date the information is used;
- Change management procedures;
- Logging of unauthorized users and detect activity of unauthorized users;
- Continuous monitoring, or annual penetration testing with bi-annual vulnerability scans;
- Security awareness training for employees, including risk-based training for information security personnel; and
- Contractual requirements that ensure service providers are capable of maintaining appropriate safeguards for customer information and the regular assessment of risks posed by service providers.

The information security program must be adjusted in light of the results of the required testing and monitoring when there are material operational changes to the financial institution's business, or any other circumstances where the financial institution knows or has reason to know something may have a material impact on the information security program.

Documentation of Risk Assessments

While the previous Safeguards Rule required a risk assessment identifying internal and external risks to the security, confidentiality, and integrity of customer information, the new final Safeguards Rule contains additional requirements:

- Criteria for the evaluation and categorization of the identified security risks faced;
- Criteria for the assessment of the confidentiality, integrity, and availability of information systems and customer information, including the adequacy of existing controls in the context of the identified risks or threats faced; and
- Descriptions of how identified risks will be mitigated or accepted and how the information security program will address the risks.

Additionally, financial institutions must periodically perform additional risk assessments.

Incident Response Plan Requirements

The Safeguards Rule now requires a written incident response plan designed to respond to, and recover from, any data security event that would materially affect the confidentiality, integrity, or availability of customer information. The Rule provides that the plan must address:

- The goals of the incident response plan;
- The internal processes for responding to a security event;
- Clear roles, responsibilities, and levels of decision-making authority;
- External and internal communications and information sharing;
- Identification of requirements for the remediation of any identified weaknesses within information systems and associated controls;
- Documentation and reporting regarding security events and related incident response activities;
- Evaluation and revision (as necessary) of the incident response plan following a security event.

Designation of a Responsible “Qualified Individual”

Responsibility for the implementation and oversight of the information security program must be assigned to a “Qualified Individual,” who can be an employee of the financial institution or employed by an affiliate or service provider (though the financial institution still retains responsibility for compliance with the Safeguards Rule and must designate one of its own employees to direct and oversee the Qualified Individual). The modified Safeguards Rule does not require a specific level of

education, experience, or certification for the Qualified Individual. The FTC, in its accompanying Supplementary Information, stated that a cybersecurity “expert” would only be required if the financial institution’s complexity or size of information systems required such level of services.

The Qualified Individual must be required to submit regular, written reports, at least annually, to the financial institution’s board of directors. The report must include the overall status of the information security program, compliance with the Safeguards Rule, and any other material matters related to the information security program.

Exemptions

The FTC also built in an exemption for financial institutions that collect information from fewer than 5,000 customers. These smaller financial institutions are not required to meet the requirements for a written risk assessment or incident response plan, or submit their Qualified Individual report annually to the board of directors.

Expanded Definition of Financial Institution

In addition to these requirements for information security programs, the Safeguards Rule expanded the definition of “Financial Institution” to now include any entity engaged in activities that the Federal Reserve Board has determined to be incidental to financial activities. The FTC stated that it explicitly intends to include “finders” that bring together buyers and sellers of financial products or services into the scope of enforcement. The modifications also updated several terms, including “Consumer,” “Customer,” “Nonpublic Personal Information,” and “Personally Identifiable Financial Information,” bringing the definitions into the Safeguards Rule itself, instead of incorporating the terms from the FTC’s related Privacy of Consumer Financial Information Rule.

Timing

The new Rule becomes effective 30 days after publication in the Federal Register. However, the requirement to appoint a Qualified Individual, adopt a written risk assessment, incorporate specific technical measures into the written information security plan, set up monitoring or scanning and testing, adopt employee training, assess service provider risks, adopt an incident response plan, and submit reports to the Board, go into effect one year after publication.

National Law Review, Volume XI, Number 322