Articles + Publications | November 3, 2021

FTC Amends “Safeguards Rule” for Covered Financial Institutions

WRITTEN BY

Ethan G. Ostroff | James W. Stevens | Sarah Hanna

On October 27, the Federal Trade Commission (FTC) announced a final rule (Final Rule), amending the Standards for Safeguarding Customer Information (Safeguards Rule) under the Gramm-Leach-Bliley Act (GLBA) as it applies to covered financial institutions. The Final Rule provides guidance on developing and implementing information security programs, such as access controls, authentication, and encryption. Notably, the Final 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 now subject to the FTC’s enforcement authority under the Safeguards Rule.

Expanded Definition of “Financial Institution”

The Final Rule expands the definition of “financial institution” to include entities engaged in activities that the Federal Reserve Board determines as incidental to financial activities. For example, an automobile dealership that, as a usual part of its business, leases automobiles on a nonoperating basis for longer than 90 days would qualify as a financial institution for its leasing business. The Final Rule explains, for this example, that leasing personal property on a nonoperating basis with an initial lease term of at least 90 days is a financial activity enumerated in the list of permissible nonbanking activities under 12 CFR 225.28 and referenced in the Bank Holding Company Act.

Additional examples of “financial institutions” that significantly engage in business incidental to financial activities include businesses that regularly wire money to and from consumers; retailers that extend credit by issuing their own credit cards directly to consumers; and check cashing businesses. A business only falls within the expanded definition of “financial institution” if it is “significantly” engaged in activities incidental to financial activities. For example, a retailer that accepts cash, check, or credit as a form of payment; a merchant that allows an individual to “run a tab”; and a grocery store that allows individuals to cash a check would not be considered to “significantly” engage in activities incidental to financial activities and therefore would not fall within the expanded definition.

By defining “financial institution” and enumerating examples, rather than incorporating by reference to the Privacy of Consumer Financial Information Rule (Privacy Rule) promulgated under the GLBA, the Final Rule allows readers to understand the requirements of the Safeguards Rule without having to refer separately to the Privacy Rule.

Requirements Under the Final Rule

Under the Final Rule, covered financial institutions — which now include nonbank lenders, mortgage brokers, consumer reporting agencies, etc. — will be required to develop, implement, and maintain a more comprehensive information security program. The information security program must be written and include, among other things, the following elements:

- **Designation of a Qualified Individual:** In its comprehensive written information security program, a covered financial institutional must designate a qualified individual (Qualified Individual) responsible for overseeing and implementing the information security program. The Qualified Individual may be an employee, an affiliate, or a service provider. In the event that the Qualified Individual is a service provider or an affiliate, he/she is subject to additional requirements.

- **Risk Assessments:** A covered financial institution must conduct risk assessments. Risk assessments must be written and include, among other things, criteria for the assessment of identified security risks, confidentiality, and integrity of information systems. A covered financial institution must design and implement safeguards to control the risks identified through such risk assessments.

- **Encryption and Multifactor Authentication:** A covered financial institution must encrypt all customer information held or transmitted both in transit over external networks and at rest. In the event that such encryption is infeasible, the covered financial institution may instead secure the customer information through an effective alternative control reviewed and approved by the Qualified Individual. In addition, a covered financial institution must implement multifactor authentication (or a reasonably equivalent or more secure method of access control approved in writing by the Qualified Individual) for any individual accessing any information system.

- **Periodic Penetration Testing and Vulnerability Assessments:** A covered financial institution must conduct annual penetration testing determined each year based on relevant identified risks (in accordance with the risk assessment). In addition, at least every six months, a covered financial institution is required to conduct vulnerability assessments, which must include systemic scans or reviews of information systems reasonably designated to identify publicly known security vulnerabilities (based on the risk assessment).

- **Oversight of Service Providers:** A covered financial institution must oversee service providers, including requiring service providers by contract to implement appropriate safeguards for customer information and periodically assessing service providers.

- **Annual Report to the Board of Directors:** At least annually, the Qualified Individual is required to report in writing to a covered financial institution’s board of directors or equivalent governing body (or in the absence of an equivalent governing body, a senior officer responsible for the information security program) on the overall status of the information security program and material matters related to such program.

The Final Rule exempts financial institutions that maintain customer information concerning less than 5,000 consumers from the above requirements to implement a written risk assessment, conduct annual penetration testing and biannual vulnerability assessments, and to compel the Qualified Individual to report annually to the board of directors or equivalent governing body.

Effective Date

The new Safeguards Rule will become effective 30 days after the date of publication in the *Federal Register*, with certain exceptions. Notwithstanding the foregoing, the certain requirements will become effective one year after the date of publication in the *Federal Register*, including:

- Written risk assessments;
- Designation of a Qualified Individual;
- Annual penetration testing and biannual vulnerability assessments;
- Periodic assessment of service providers;
- Establishment of a written incident response plan; and
- Annual reports to the board of directors or equivalent governing body by the Qualified Individual.

RELATED INDUSTRIES + PRACTICES

- Financial Services