Akin®

## FTC's New Updated Cybersecurity Safeguards

Feb 11, 2022

Reading Time : **5 min**

By: Natasha G. Kohne, Jo-Ellyn Sakowitz Klein

Effective as of January 10, 2022, the updated new final Safeguards Rule (the "Final Rule") is the FTC's latest measure against increasing cyberattacks, containing new requirements and definitions for financial institutions to develop, implement and maintain comprehensive security systems to secure consumer information. In the same announcement, the FTC also released a notice of proposed rulemaking (NPRM) that would require certain cybersecurity events to be reported to the FTC.

While some parts of the Final Rule are now effective, most of the more substantive provisions will not go into effect until December 9, 2022.

**Specific Requirements and New Definitions**

The Final Rule, which incorporates public commentary dating back to 2019, is the first update to the Safeguards Rule since its 2003 effective date. The Safeguards Rule was instituted to fulfill the FTC's mandate under the Gramm-Leach-Bliley Act (GLBA) to create rules for the processing and protection of personal information by nonbanking financial institutions under its jurisdiction. While the Safeguards Rule required these institutions to develop written information security plans, it did not generally dictate specific security measures, instead requiring plans tailored according to an institution's individual risk.

The Final Rule makes five key changes to the 2003 Safeguards Rule:

*1. Information Security Program Criteria*

The Final Rule adds specific requirements for financial institutions to implement an information security program, including access controls, data inventory and data classification, authentication, encryption, disposal procedures, incident response and conducting risk assessments. While the Final Rule retains previous employee training and service provider oversight requirements, it adds measures to ensure those requirements are implemented effectively: requiring training programs updates as necessary, and assessment of service providers' risk and safeguard adequacy.

*2. Designated Information Security Program Coordinator*

Instead of the previously required one or more employee coordinators, financial institutions will now be required to appoint a single "qualified individual" to oversee the information security program. This does not have to be a Chief Information Security Officer (CISO) position, nor does the Final Rule specify any particular expertise or certifications. While a third party service provider may fulfill this role, the financial institution is ultimately responsible, and must still maintain oversight of the service provider.

*3. Exemptions for Small Companies*

Although there is not an entity level exemption for small companies, the FTC did recognize that certain requirements may impose too large a burden on these companies. Thus, financial institutions that collect information on fewer than 5,000 customers will have specific exemptions from the requirements for written risk assessments, continuous monitoring or annual penetration testing and bi-annual vulnerability assessment, written incident response plans and annual reporting to the board of directors. They still must meet other requirements under the Final Rule: namely the requirement to appoint a qualified individual to oversee information security, conduct risk assessments, implement a written information security program, evaluate and adjust the program as needed, oversee service providers and train employees.

*4. Expanded Definition of "Financial Institution" and New Regulation for "Finders"*

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," namely the activities of "finders." Now under the scope of the Safeguards Rule, "finders" are companies that bring together buyers and sellers "of any product or service for transactions that the parties themselves negotiate and consummate." Examples of finder activities include

identifying and referring potential parties to each other, arranging meetings and conveying expressions of interest, bids and offers relating to a transaction. The scope is narrower than it may first appear, as the Final Rule clarifies that only finder activities that involve commercial transactions are covered, and only information from customers with which the financial institution has a continuing relationship.

*5. New Definitions and Examples*

Several new definitions and examples are added into the Safeguards Rule itself rather than incorporating them through references from related FTC rules. These include terms such as "personally identifiable financial information" and "financial institution," which readers can now examine without needing to reference the Privacy of Consumer Financial Information Rule (the "Privacy Rule") as they did previously.

## Scope

The Final Rule applies to nonbanking financial institutions, such as mortgage lenders, motor vehicle dealers, finance companies, pay day lenders, certain investment advisors, travel agencies operated in connection with financial services, mortgage brokers, account servicers, check cashers, wire transferors, collection agencies, tax preparation firms and credit counselors along with other financial advisors and financial institutions that are not otherwise subject to another financial regulator under Section 505 of the GLBA, 15 U.S.C. §6805.

## Compliance Deadlines

Most provisions (those under Section 314.5) will not take effect until one year after December 9, 2021, when the Final Rule was published in the Federal Register. However, several requirements are effective now:

- Regular Testing and Monitoring

The requirement of testing detailed in Section 314.4(d)(1) continues to be effective and companies presently must have key controls, systems and procedures will need to be routinely tested and monitored for effectiveness, including those intended to detect actual and attempted attacks or intrusions. The specific testing requirements outlined in Section 314.4(d)(2), however, will not be effective until December 9, 2022.

- Service Provider Oversight

Financial institutions must take reasonable steps to select and retain service providers that are capable of maintaining reasonable safeguards for protecting customer information. Contractual provisions requiring service providers to implement and maintain appropriate safeguards will also be required.

- Re-evaluating Written Information Security Programs

Financial institutions must evaluate and adjust their information security programs based on (1) the results of the regular testing and monitoring, (2) any material changes to their operations or business arrangements, (3) the results of risk assessments or (4) "any other circumstances that they know or have reason to know may have a material impact" on their information security program.

- Risk Assessments

Separately from the detailed written risk assessments required one year from publication, financial institutions will have a more immediate requirement to conduct additional periodic risk assessments that "reexamine the reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information." The re-evaluation of the written security program will be in part based on these assessments.

## Proposed Cybersecurity Event Reporting Requirement

In addition to the updates in the Final Rule, the FTC has announced it will now seek comment on whether to further amend the Safeguards Rule to include reporting requirements for certain cybersecurity incidents. When (1) a covered financial institution determines customer information has been or is reasonably likely to be misused and (2) at least 1,000 customers have been affected or reasonably may be affected by the incident, the financial institution will be required to report the incident to the FTC, according to the supplemental notice. Notification would have to be made as soon as possible but no later than 30 days after discovery of the incident, using a form on the FTC website.

The period for public commentary ended on February 7, with industry groups and the U.S. Chamber of Commerce calling for more streamlining of reporting regulations. In its commentary, the U.S. Chamber of Commerce called on the FTC to pause the rulemaking until it can come up with a plan to "harmonize the myriad regulations" from the Safeguards Rule.

## Takeaways

Financial institutions covered by the GLBA (including financial technology companies) now face detailed prescriptive requirements for cybersecurity protections and should begin reexamining their information security programs. The high-level elements prescribed by the old rule have been replaced with a more detailed regime that views the protection of customer information as a critical organization-wide effort.

Please contact a member of Akin Gump's cybersecurity, privacy and data protection team if you have any questions about how this updated rule may impact your company or your company's information security program.

## Categories

FTC | Federal Privacy Policy | Financial Data Privacy