Westlaw Today
powered by Reuters

FTC revises the safeguards rule and proposes mandatory reporting of cybersecurity events

By Kathleen Benway, Esq., Kimberly Kiefer Peretti, Esq., and Katherine Doty Hanniford, Esq., Alston & Bird LLP*

NOVEMBER 15, 2021

On October 27, 2021, the FTC released its much-anticipated final revisions to the Gramm-Leach-Bliley Safeguards Rule (Safeguards Rule or Final Rule), following a 3-2 vote along party lines and also released a notice of proposed rulemaking that would require reporting to the FTC of certain cybersecurity events.

Revisions to the safeguards rule

Effective since 2003, the Safeguards Rule[1] requires covered financial institutions[2] to develop, implement, and maintain a reasonably designed, comprehensive, written information security program (WISP) with appropriate administrative, technical, and physical safeguards relating to customer information.

The Final Rule represents a significant shift to more prescriptive requirements for information security and is the culmination of a multi-year effort by the FTC to amend the rule.

Financial institutions subject to FTC enforcement of the Safeguards Rule are entities that are not otherwise subject to enforcement of another financial regulator under Section 505 of the Gramm-Leach-Bliley Act.[3] These include mortgage lenders, "pay day" lenders, finance companies, account servicers, wire transferors, collection agencies, and investment advisors exempt from SEC registration, for example.

The Final Rule represents a significant shift to more prescriptive requirements for information security and is the culmination of a multi-year effort by the FTC to amend the rule. These changes to the Safeguards Rule were first proposed in a notice of proposed rulemaking and request for comment in March 2019.

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, which harmonizes other federal agencies' Safeguards Rules, which already include such activities in their definition of financial institution.

Going forward, the Final Rule applies to "finders," i.e., companies that bring together buyers and sellers "of any product or service for the transactions that the parties themselves negotiate and consummate."[4] Because the Safeguards Rule applies only to customer relationships and to transactions that are "for personal, family, or household purposes" finding services involving consumer transactions for customers (i.e., consumers with whom a financial institution has an ongoing relationship) will now be covered by the Safeguards Rule.

The overall effect of the final rule is to generally align the Safeguards Rule with the New York State Division of Financial Services Cybersecurity Requirements ("NYDFS Cybersecurity Regulations"),[5] which issued prescriptive information security requirements, including the requirement to implement multifactor authentication (MFA) for access to a financial institution's information system and the encryption of customer information in transit and at rest.

The FTC recognizes the need for senior management to be well-informed regarding the information security program, and that with that awareness, it is more likely that the information security program will receive the necessary resources.

In both instances, the FTC modeled its revised rule on the NYDFS Cybersecurity Regulations, and has adopted language that closely tracks it regarding these controls, including the limited carve-outs for reasonably equivalent controls instead of MFA and alternative compensating controls where encryption may be infeasible.

However, the FTC's Safeguards Rule is more prescriptive than the NYDFS Cybersecurity Regulations in its requirement for annual reporting to a company's Board by the designated "Qualified Individual," who is responsible for the implementation, management, and enforcement of the information security program.

In contrast to the NYDFS regulations which provide five topics to consider including in the annual Board report, the Final Rule specifies the required report to the Board shall include discussion of the overall status of the information security program, compliance with the Safeguards Rule, and material matters related to the information security program.

Then, in furtherance of the discussion of material issues, it provides seven areas as examples for inclusion in the report, which include management's responses to these issues and any recommendations for changes to the information security program. The Final Rule release indicates that the FTC recognizes the need for senior management to be well-informed regarding the information security program, and that with that awareness, it is more likely that the information security program will receive the necessary resources.

The FTC is now proposing to require financial institutions to report to the FTC certain cybersecurity events "as soon as possible and no later than 30 days" following discovery of the event.

Although as of this writing the Final Rule has not yet been published in the Federal Register, certain sections of the final rule will take effect 30 days from publication of the Final Rule in the Federal Register. These include:

- **4(d)(1) Testing & Monitoring**: This provision requires regular testing and monitoring of the effectiveness of key controls, systems, procedures, including those intended to detect actual and attempted attacks or intrusions.
- **4(f)(1)-(2) Service Provider Oversight**: These provisions require the financial institution to take reasonable steps to select and retain service providers that are capable of maintaining reasonable safeguards. This provision also requires the inclusion of contractual provisions that require service providers to implement and maintain appropriate safeguards.
- **4(g) Re-Evaluation of Written Information Security Program (WISP)**: Requires the financial institution to evaluate and adjust its WISP based on the results of the testing and monitoring required in 314.4(d), material changes to operations or business arrangements, the results of risk assessments, or any other circumstances that "you know or have reason to know may have a material impact" on the information security program.

Financial institutions will have one year to come into compliance with the following sections, as they will not take effect until one year from publication of the Final Rule in the Federal Register:

- **4(a) Qualified Individual**: The rule requires the appointment of a "Qualified Individual" to oversee, implement, and enforce the information security program. Although this section permits this role to be fulfilled by a service provider, it contains additional provisions for the oversight of that service provider and makes clear the covered financial institution still bears ultimate responsibility for compliance with the Safeguards Rule.
- **4(b)(1) Risk Assessments**: The rule requires a periodic written risk assessment as a basis for the written information security program. This provision is effectively identical to the risk assessment components required under NYDFS regulations, as they each require the inclusion of (i) the criteria for evaluation and categorization of security threats and risk, (ii) the criteria for the assessment of the confidentiality, integrity, and availability of information systems and customer information, including the adequacy of existing controls, and (iii) requirements describing how identified risks are mitigated or accepted and how those risks are addressed under the information security program. However, the Safeguards Rule places an additional obligation to periodically perform supplemental risk assessments that re-examine "reasonably foreseeable internal and external risks" that could result in a security event and to re-assess the sufficiency of any safeguards in place to control these risks.
- **4(c)(1)-(8) Required Safeguards**: This section includes prescriptive, required elements of an information security program and requires the implementation of policies, procedures, and controls to mitigate the risks identified in the risk assessment. These specific measures include: access controls; the identification and management of data, personnel, devices, systems, and facilities; encryption of all customer information in transit and at rest unless infeasible and effective alternative compensating controls are reviewed and approved by the Qualified Individual; secure development practices; implementation of MFA unless the Qualified Individual has approved in writing of reasonably equivalent or more secure controls; secure disposal within two years after the last date the information is used, needed, or required to be retained; change management; monitoring and logging of user activity and to detect unauthorized access or use of customer information.
- **4(d)(2) Monitoring**: This section requires continuous monitoring and periodic penetration testing and vulnerability assessments. If a financial institution lacks these capabilities, then it must perform annual penetration tests as well as vulnerability assessments no less frequently that every six months.
- **4(e) Training**: This section contains requirements for security training for personnel as well as a requirement to use sufficiently qualified personnel to manage and oversee

the WISP and security risks. This section also includes a requirement to provide information security personnel with sufficient security updates and training to address relevant risks and to verify that information security personnel take steps to stay abreast of the evolving threat landscape and mitigation tactics.

- **4(f)(3) Service Provider**: This section requires financial institutions to conduct risk assessments of its service providers based on the risks they pose and to assess the adequacy of their safeguards.
- **4(h) Incident Response Plan**: The rule requires the financial institution to establish a written incident response plan, which must specifically address seven core areas of incident response. These areas include: the goal of the incident response plan; internal response processes; the definition of roles and responsibilities, including decision-making authority; external and internal communications and information sharing; the identification of remediation requirements based on any identified weaknesses in information systems and related controls; documentation and reporting; and the evaluation and revisions as necessary of the incident response plan following a security incident.
- **4(i) Qualified Individual Report**: The rule requires the Qualified Individual to report at least annually via a written report to the financial institution's Board or other senior governing body, or if no such entity exists, the senior officer responsible for the WISP. This report shall include the overall status of the information security program, its compliance with the Safeguards Rule, and any material matters related to the information security program, including issues related to risk assessment, risk management and control decisions, service provider arrangements, testing and monitoring results, security events or violations of security, management's responses to these items, and any recommendations for changes to the information security program.

Note that the written risk assessment, continuous monitoring and pen testing and annual certification requirements do not apply to financial institutions that maintain customer information for fewer than 5,000 consumers.

Republican commissioners dissent

Objections to the Final Rule of the two dissenting Commissioners, Christine Wilson and Noah Phillips, focused on the prescriptive requirements, raising concerns that by introducing prescriptive requirements into the rule, it could have unintended consequences of weakening risk management functions and undermining the financial institution's ability to tailor its information security program based on its risk assessment.

The Commissioners also argued that it was premature to adopt NYDFS-like requirements as there was insufficient data to assess the impact and efficacy of NYDFS rules. Finally, the dissenting Commissioners expressed the view that given increased legislative interest and Congressional activity in data security, "intrusive mandates are best left to the people's representatives rather than to the vagaries of the administrative rulemaking process."

Proposed cybersecurity event reporting requirement

In conjunction with the issuance of the Final Rule, the FTC has also issued a notice of supplemental rulemaking to consider instituting a reporting obligation to the FTC in the event of a cybersecurity event in which the covered financial institution determines customer information has been misused or is reasonably likely to be misused and 1,000 or more consumers have been affected or reasonably may be affected by the security incident.

This standard for reporting based on a determination of misuse or reasonable likelihood of misuse of customer information is identical to the current standard for customer notices under the Interagency Guidelines Establishing Information Security Standards,6 and accordingly the proposed rule is limited to establishing FTC reporting requirements and does not separately define "customer information" or contain revisions to the criteria for customer notifications.

However, by aligning the criteria for notification to the FTC with the customer notification criteria, the proposed rule would differ from the regulator notification criteria to which other, non-FTC regulated financial institutions are subject, including in the banking and insurance sectors.

The FTC previously sought comment in connection with its amendments to the Safeguards Rule as to the timing, criteria, and nature of reporting cybersecurity events to the FTC. The FTC is now proposing to require financial institutions to report to the FTC certain cybersecurity events "as soon as possible and no later than 30 days" following discovery of the event. The FTC's rationale for reporting is to ensure that the FTC becomes aware of cybersecurity events that "could suggest a financial institution's security program does not comply with the Rule's requirements," which in turn would facilitate FTC enforcement of the Rule.

As a further justification for this rule, the FTC noted the patchwork of state data breach reporting statutes, in which regulatory reporting to state Attorneys General may vary, but proposes to require the same type of information to be reported to the FTC as is generally required under state regulatory notice requirements. The FTC further proposes to make this information publicly available. Once the notice is published in the Federal Register, commenters have 60 days to submit comments to the FTC.

Notes

[1] 16 C.F.R. Part 314

[2] https://bit.ly/3c6fPAS

[3] 15 U.S.C. 6805

[4] (f), modeled on 12 CFR 22586(d)(1).

[5] 23 NYCRR 500

[6] https://bit.ly/3n4RhhS

About the authors



Kathleen Benway (L) is a partner at **Alston & Bird LLP**, after having spent more than a dozen years at the Federal Trade Commission. She focuses her practice on helping clients navigate government investigations and develop practical strategies for compliance with applicable state, federal and global consumer protection and privacy laws. She can be reached at Kathleen.Benway@alston.com. **Kimberly Kiefer Peretti** (C) is a partner and co-leader of the cyber and data strategy team and national security and digital crimes team. She delivers cyber risk management and information security counsel to her clients. She can be reached at Kimberly.Peretti@alston.com. **Katherine Doty Hanniford** (R) is a senior associate whose practice focuses on resolving data security compliance issues proactively through counseling as well as representing clients under scrutiny through cybersecurity crises. She can be reached at Kate.Hanniford@alston.com. All of the authors are based in Washington, D.C. This article was originally published on Nov. 1, 2021, on the Alston & Bird website. Republished with permission.

This article was published on Westlaw Today on November 15, 2021.