November 12, 2021

FTC Updates Safeguards Rule for Consumer Financial Information

On October 27, 2021, the Federal Trade Commission ("FTC") announced updates to the Standards for Safeguarding Customer Information ("Safeguards Rule" or "Rule") governing the data security safeguards that financial institutions must implement to secure customer financial information. The updates, which will come into effect one year after publication in the Federal Register, require non-banking financial institutions, such as motor vehicle dealers, payday lenders, mortgage brokers, certain payment service providers, data aggregators and application providers, as well as loan brokers, to implement additional data security measures to protect sensitive consumer data. The FTC voted 3-2 to adopt the revisions to the Safeguards Rule,[1] with Commissioners Noah Joshua Phillips and Christine S. Wilson filing a dissenting statement.[2] In response, Chair Lina M. Khan and Rebecca Kelly Slaughter issued a separate joint statement supporting the updates.[3]

Background

The FTC promulgated the Safeguards Rule in 2002 pursuant to the Gramm Leach Bliley Act ("GLBA"), which requires the FTC and other federal agencies to establish standards for financial institutions to implement technical, administrative and physical safeguards for certain information.[4] For example, the Securities and Exchange Commission (SEC) also promulgated Regulation S-P under section 504 of the GLBA, which requires the SEC to adopt rules implementing notice requirements and restrictions on a financial institution's ability to disclose nonpublic personal information about consumers. The Office of the Comptroller of the Currency, the Federal Reserve Board, the Federal Deposit Insurance Corporation and the Office of the Thrift Supervision also issued an interagency regulation to implement the GLBA requirements that banks notify consumers about their privacy policies and allow consumers to opt out of information sharing between the bank and certain nonaffiliated third parties.

The Safeguards Rule became effective in May 2003. The FTC has enforcement authority under the Safeguards Rule over financial institutions that are not banks, credit unions, insurance carriers, or SEC-registered investment advisors and investment companies. Such financial institutions include non-bank lenders, check-cashing businesses, mortgage brokers, personal property or real estate appraisers, professional tax preparers, certain payment service providers, data aggregators, application providers, loan brokers and credit reporting agencies. There is no private right of action under the Rule. The Safeguards Rule requires financial institutions to develop, implement and maintain a comprehensive information security program for the handling of customer information. Financial institutions must designate one or more employees to coordinate their program, which should be appropriate to the size and complexity of the organization, the nature and scope of its activities, and the sensitivity of the customer information at issue. The Rule requires financial institutions to first conduct a risk assessment to identify reasonably foreseeable internal and external risks to customer information, and then develop appropriate safeguards to address the

---

1 FTC, Press Release, *FTC Strengthens Security Safeguards for Consumer Financial Information Following Widespread Data Breaches* (Oct. 27, 2021), *available* here.

2 FTC, *Joint Statement of Commissioners Noah Joshua Phillips and Christine S. Wilson* (Oct. 27, 2021), *available* here.

3 FTC, Statement of Chair Lina M. Khan Joined by Commissioner Rebecca Kelly Slaughter Regarding Regulatory Review of the Safeguards Rule (Oct. 27, 2021), available here.

4 *See* 15 U.S.C. 6801(b), 6805(b)(2).

identified risks. The Rule also requires financial institutions to regularly test or monitor the effectiveness of these safeguards.[5] In addition, the Rule requires financial institutions to take reasonable steps, including by contractual requirements, to ensure that their service providers maintain appropriate safeguards.

When the FTC first issued the Safeguards Rule in 2002, it sought to provide general parameters for the establishment of an information security program without prescribing detailed requirements. The rationale behind this approach was to give financial institutions the flexibility to shape programs based on their particular business needs and adapt quickly to technological changes. The October updates provide more detailed requirements, in light of widespread data breaches and cyberattacks in recent years.

Changes to the Safeguards Rule

The updated Safeguards Rule reflects four categories of changes:

I. An expanded definition of "financial institution"

The updates expand covered financial institutions to include "any institution the business of which is engaging in an activity that is . . . incidental to [] financial activities as described in section 4(k) of the Bank Holding Company Act of 1956."[6] The previous version of the Rule defined financial institutions with respect to the Bank Holding Company Act but applied only to financial institutions themselves and did not cover businesses engaged in activities "incidental" to financial institutions. This means that "finders"—companies that bring together buyers and sellers of a product or service—will now fall within the scope of the Rule.

Commenters to the proposed Rule expressed concern that the amended definition was overly broad and would draw in a large swath of companies not covered by the current Rule, including advertising and marketing firms. In response, the FTC noted that "[a]lthough this language is somewhat broad, its scope is significantly limited in the context of the Safeguards Rule" because the Rule applies only to finding services in the context of transactions "for personal, family, or household purposes" and only to "consumers with which a financial institution has a continuing relationship."[7] Thus, it will not cover finders that have only isolated interactions with consumers, such as in the context of a single advertisement.

It remains to be seen how broadly the FTC will interpret the amended definition.

II. Specific criteria for conducting risk assessments and implementing information security programs

Prior to the updates, the Safeguards Rule required covered financial institutions to implement an information security program but left the specific aspects of the program to the discretion of the business. The updates set forth requirements for such programs in significantly more detail.[8] Specifically, financial institutions must implement access controls, data inventory and classification, encryption, secure development practices, multi-factor authentication, information disposal procedures, change management, regular testing and incident response.[9] The criteria align in many ways with the security requirements that already apply to financial institutions under the New York Department of Financial Services' Part 500. Some commentators have theorized that the proposed modifications are based on the NYDFS regulation.[10]

The updates also set forth certain content of the initial risk assessment that financial institutions should use to inform their information security programs. Specifically, the updates require the risk assessment to include (i) criteria evaluating identified

---

5 16 CFR 314.4 (a)-(d).

6 16 C.F.R. § 314.2(h)(1).

7 16 C.F.R. Part 300, Supplementary Information § IV, Section-by-Section Analysis, p. 18, available here.

8 16 C.F.R. § 314.4(c)(1)-(8).

9 *Id*.

10 Victoria Hudgins, "FTC Mirrors New York DFS With Potentially Costly Cybersecurity Proposal" Law.com (Jul. 28, 2020), available here.

security risks or threats; (ii) criteria for assessing the confidentiality, integrity, and availability of a business's information systems and customer information, including the adequacy of the existing controls in the context of the identified risks or threats; and (iii) requirements describing how identified risks will be mitigated or accepted based on the risk assessment.[11]

Commentators have objected to these requirements as too prescriptive and thus not providing financial institutions with sufficient flexibility in managing their information security.[12] In response, the FTC noted that these requirements are intended to be "high-level principles that set forth basic issues that the [information security] programs must address," without "prescrib[ing] how they will be addressed."[13] The FTC further noted that the two most prescriptive elements required by the amended Rule—encryption and multi-factor authentication—allow financial institutions to adopt alternative solutions when necessary.[14]

III. A requirement that covered financial institutions designate a single qualified individual to oversee the information security program who reports to the company's board of directors

The updates expand on the previous requirement that institutions designate an "employee or employees to coordinate [their] information security program" and require that they "[d]esignate a qualified individual responsible for overseeing and implementing [the] information security program and enforcing [the] information security program."[15] The qualified individual may be an employee, an affiliate or a service provider.[16] The requirement that institutions designate a single qualified individual to oversee their information security programs is intended to clarify lines of reporting in enforcing the program, avoid gaps in responsibility in managing data security, and improve communication within organizations.

The updates also require the qualified individual to provide regular reports, at least annually, to the board of directors or equivalent governing body.[17] If no board of directors or equivalent governing body exists, the report must be presented to a senior officer responsible for the organization's information security program.[18] The report must include the following information: (i) the overall status of the information security program and the organization's compliance with the Safeguards Rule; and (ii) any material matters related to the information security program, including risk assessment, risk management and control decisions, service provider arrangements, results of testing, security events or violations and management's responses thereto, and recommendations for changes in the information security program.[19]

---

11 16 C.F.R. § 314.4(b)(1).

12 16 C.F.R. Part 300, Supplementary Information § IV, Section-by-Section Analysis, p. 27, available here.

13 *Id*. at 28.

14 16 C.F.R. § 314.4(c)(5) requires that financial institutions "[i]mplement multi-factor authentication for any individual accessing any information system, unless [the business's] Qualified Individual has approved in writing the use of reasonably equivalent or more secure access controls." 16 C.F.R. § 314.4(c)(3) similarly requires that financial institutions "[p]rotect by encryption all customer information held or transmitted [] both in transit over external networks and at rest. To the extent [the business] determine[s] that encryption of customer information, either in transit over external networks or at rest, is infeasible, [it] may instead secure such customer information using effective alternative compensating controls reviewed and approved by [the] Qualified Individual."

15 16 C.F.R. § 314.4(a).

16 *Id*. The original text of the Proposed Rule referred to the Qualified Individual as a Chief Information Security Officer, but the language was amended to reflect that any qualified individual who is appropriate for the size and complexity of business may serve in the role–"[n]o particular level of education, experience, or certification is prescribed by the Rule. 16 C.F.R. Part 300, Supplementary Information § IV, Section-by-Section Analysis, p. 31, available here.

17 16 C.F.R. § 314.4(i).

18 *Id*.

19 *Id*. at (i)(1)-(3).

IV. Smaller financial institutions are exempt from certain requirements

Finally, the updates exempt smaller financial institutions—those collecting information from fewer than 5,000 consumers annually—from certain requirements related to conducting written risk assessments, developing incident response plans, and presenting annual reports to the institution's board of directors or other governing body.[20] These exemptions recognize the high cost of compliance for these smaller institutions and seek to reduce their burden. Notably, however, these smaller institutions are not exempted from the designated individual requirement. In response to concerns about the increased cost of this requirement, the FTC reasoned that "the person designated to coordinate the information security program need only be 'qualified.' No particular level of education, experience, or certification is prescribed by the Rule. Accordingly, financial institutions may designate any qualified individual who is appropriate for their business."[21]

The FTC is still seeking comments on whether to make an additional change to the Safeguards Rule that would impose obligations on financial institutions to disclose to the FTC certain data breaches and security events affecting over 1,000 consumers.[22] The public will have 60 days to comment after the notice is published in the Federal Register.

The updates are the result of years of reviews, comments, workshops and discussions conducted by the FTC.[23] The FTC issued the current updates based on the comments and feedback it received. FTC Commissioners Phillips and Wilson opposed the updates, criticizing the more detailed requirements in their dissenting statement, and expressed concern that the heightened requirements would inhibit flexibility and "could weaken data security by diverting finite resources towards a check-the-box compliance exercise and away from risk management tailored to address the unique security needs of individual financial institutions."[24] The two dissenting Commissioners also called the updates premature, since new data privacy and security legislation is being developed that may overlap with these updates.

In response to the dissent, Chair Khan and Commissioner Slaughter issued a joint statement in which they emphasized the necessity of the updates: "The recent history of major data breaches affecting millions of consumers shows that more needs to be done to protect consumers' sensitive information. Despite the increasing sophistication of cyberattacks, many businesses continue to offer inadequate security."[25] For example, they noted that "it is likely that the massive breach at Equifax could have been prevented or mitigated by adopting practices required by these [updates]." Moreover, they disagreed that the new requirements undermine flexibility; although the updates require financial institutions to address certain aspects of security, they do not prescribe any particular method for doing so.

Implications

The updates to the Safeguards Rule follow widespread data breaches and cyberattacks across the financial industry and a years-long notice and comment process. They are consistent with increasing efforts generally by the FTC and other regulators to strengthen cybersecurity requirements for financial institutions and other organizations handling consumer information.

- These updates to the Safeguards Rule continue the trend of federal regulators, such as the FTC and SEC, developing policies to emphasize data privacy and security, including by expanding the scope and specificity of rules and regulations that set standards for data privacy and cybersecurity protections in specific industries. Although it is unclear how efforts to impose

[20] 16 C.F.R. § 314.6.

[21] 16 C.F.R. Part 314, Standards for Safeguarding Consumer Information (Final Rule), p. 54, available here.

[22] FTC, Press Release, *FTC Strengthens Security Safeguards for Consumer Financial Information Following Widespread Data Breaches* (Oct. 27, 2021), *available* here.

[23] In 2019, the FTC issued a Notice of Proposed Rulemaking outlining proposed changes to the Rule, and in July 2020, the FTC conducted a workshop and panels with information security experts concerning the proposed changes.

[24] FTC, *Joint Statement of Commissioners Noah Joshua Phillips and Christine S. Wilson* (Oct. 27, 2021), at 1, *available* here.

[25] FTC, *Statement of Chair Lina M. Khan Joined by Commissioner Rebecca Kelly Slaughter Regarding Regulatory Review of the Safeguards Rule* (Oct. 27, 2021), at 2, available here.

these types of requirements will influence whether Congress acts legislatively in this area, Congress has recently been considering similarly enhanced requirements in several bills currently pending.[26] The standards created by these rules and regulations, and in particular with the updates to the Safeguards Rule, may prove to be inconsistent with standards established by Congress in these laws, if they are enacted. Will the fact that updated rules are in place reduce the incentive for Congress to act? Or will the specificity of the new rules, including the new Safeguards Rule, provide Congress with additional incentives to impose its own requirements, rather than those imposed administratively?

- The FTC's solicitation of comments regarding potential requirements for reporting data security incidents, coupled with its acknowledgment that the proposed reporting requirements are modeled after the New York Department of Financial Services Cybersecurity Regulation, may indicate that federal regulators are increasingly looking to state authorities for guidance on federal programs and regulations.

- The growing number of state agencies promulgating cybersecurity and data privacy-related rules and regulations, such as the New York Department of Financial Services, the Colorado Attorney General under the Colorado Privacy Act, and the California Attorney General under the California Consumer Privacy Act, when combined with newly minted federal requirements, create an increasingly complex web of requirements for companies to follow. Companies will not only need to take steps to comply with the new rules and regulations, but will also need to devote additional resources to understanding which rules apply to them, and what they require the organization to do.

* * *

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

Michael E. Gertzman
+1-212-373-3281
mgertzman@paulweiss.com

Roberto J. Gonzalez
+1-202-223-7316
rgonzalez@paulweiss.com

Jeannie S. Rhee
+1-202-223-7466
jrhee@paulweiss.com

Steven C. Herzog
+1-212-373-3317
sherzog@paulweiss.com

Robin Linsenmayer
+1-628-432-5117
rlinsenmayer@paulweiss.com

Associates Emily M. Glavin, Cole A. Rabinowitz, Rosie Vail and Simona Xu contributed to this client memorandum

[26] *See e.g.*, H.R. 474, 117th Cong. (2021), Protecting Consumer Information Act of 2021, available here (requiring the FTC to review and potentially revise its current privacy standards with respect to whether they are sufficient to protect consumers' financial information from cybersecurity threats).