The Safeguards Rule: protecting information at financial institutions

By Edgar Vargas, Esq., Kim Phan, Esq., and Kamran Salour, Esq., Troutman Pepper Hamilton Sanders LLP

JANUARY 26, 2023

The Federal Trade Commission (FTC) announced a delay to the date of several of the amendments under § 314.5 to the Gramm-Leach-Bliley Act's (GLBA) Safeguards Rule, which requires certain financial institutions to meet several data security requirements to protect customers' personal financial information, and the institution's own sensitive information. For the financial institutions subject to the FTC's authority, the FTC can bring enforcement actions against those that fail to comply with the GLBA's provisions or rules.

The amendments were to take effect Dec. 9. However, on Nov. 15, the FTC announced a delay to the effective date of several provisions of the Safeguards Rule by six months, from Dec. 9 to June 9, 2023, due to reported challenges in institutions' ability to meet the requirements for designating "qualified individuals" responsible for implementation as well as supply chain issues.

The Gramm-Leach-Bliley Act's (GLBA) Safeguards Rule requires certain financial institutions to meet several data security requirements to protect customers' personal financial information, and the institution's own sensitive information.

The amendments that were delayed seek to enforce a more prescriptive Safeguards Rule — requiring financial institutions to engage in specific activities when developing and implementing aspects of their information security programs. This adjustment toward a more prescriptive approach acknowledges that comprehensive information security programs must account for the size and complexity of users/organizations, nature and scope of the activities, and sensitivity of any customer information.

Although the FTC has given financial institutions additional time to meet its requirements, financial institutions must avoid any tendencies to delay because of the new requirements' far-reaching and prescriptive nature.

Background on the Safeguards Rule

Although certain rulemaking authority was modified under the Dodd–Frank Wall Street Reform and Consumer Protection Act, the FTC can still issue industry-wide regulations and guidance to help financial institutions within its jurisdiction to comply with the GLBA. Regulations may specifically reference administrative, technical, and physical safeguards when handling customers' nonpublic personal financial information.

As part of the FTC's scheduled review, and after soliciting and reviewing public comments in the previous years, the FTC issued a notice of proposed rulemaking in 2019 to amend the Safeguards Rule. The FTC hasn't updated the Safeguards Rule since its implementation in 2003. When the FTC proposed this rulemaking to amend the Safeguards Rule, it stated that it was considering more detailed requirements to provide additional guidance, bearing in mind changing technology and security approaches.

Amendments delayed

The FTC published the amended Safeguards Rule on Dec. 9, 2021, and certain portions of the amendments to the Rule became effective on Jan. 10, 2022. The remaining, more prescriptive, provisions were scheduled to go into effect on Dec. 9.

However, the FTC delayed the effective date in response to a public comment letter submitted by the Small Business Administration noting that there is a "reported shortage of qualified personnel to implement information security programs" and issues in the supply chain that could impact the ability of smaller financial institutions to obtain the necessary equipment for upgrading security systems.

Fortunately for financial institutions, the delay offers some breathing room. Significantly, several delayed amendments include:

- **Designating qualified security individual**. A covered financial institution must designate a qualified individual to be responsible for implementing and overseeing its information security program. The amended Safeguards Rule permits a financial institution to use a third party to serve as the financial institution's qualified individual, reasoning that some "may prefer to retain an outside expert, lack the resources to employ a qualified person to oversee a program, or decide to pool

resources with affiliates to share staff to manage information security." § 314.4(a); see also https://bit.ly/3QKML5q.

- **Risk assessments**. The Safeguards Rule provides new requirements on how financial institutions that maintain customer information for 5,000 consumers or more must conduct risk assessments, which now must include the "(i) criteria for the evaluation and categorization of identified security risks or threats [the financial institution] face[s]; (ii) criteria for the assessment of the confidentiality, integrity, and availability of [the financial institution's] information systems and customer information[;] and (iii) requirements describing how identified risks will be mitigated or accepted based on the risk assessment and how the information security program will address the risks." § 314.4(b)(1).
- **Access restrictions**. Financial institutions will be required to implement technical and physical access controls that authenticate only authorized users and limit authorized users' access to information as required to perform their duties and functions. § 314.4(c)(1). Financial institutions must also implement other access requirements, such as multifactor authentication for individuals' access to information systems. § 314.4(c)(5).
- **Encryption**. Financial institutions will be required to encrypt all customer information in transit or at rest. If encryption is not feasible for certain financial institutions, the institution may secure the information by alternate means, if such compensating controls are reviewed and approved by the qualified individual (see above). § 314.4(c)(3).
- **Training**. Financial institutions will need to provide all personnel with security awareness training and update such training to reflect identified security risks. Information security personnel should receive additional training that is sufficient for such personnel to address relevant security risks. § 314.4(e).
- **Incident response plan**. Financial institutions that maintain customer information for 5,000 consumers or more must establish a written incident response plan that addresses: (1) the goals of the plan; (2) the internal processes for responding to an incident; (3) the responsibilities and roles of individuals; (4) communication plans; (5) remediation requirements; (6) logging and documentation of incidents; and (7) evaluation and revision of the plan following a security event. § 314.4(h).
- **Periodic assessments**. Financial institutions that maintain customer information for 5,000 consumers or more will be required to have continuous monitoring to detect changes in information systems that may create vulnerabilities. In the alternative, financial institutions may conduct: (1) annual penetration testing of those systems and (2) vulnerability assessments at least every six months, including "systemic scans or reviews of information systems reasonably designed to identify publicly known security vulnerabilities in information systems[.]" § 314.4(d)(2).
- **Data minimization**. Financial institutions are required to "[d]evelop, implement, and maintain procedures for the secure disposal of customer information in any format no later than two years after the last date the information is used in connection with the provision of a product or service to the customer to which it relates, unless such information is necessary for business operations" or other purposes. § 314.4(c)(6)(i). Financial institutions will also be required to review their data retention policies to minimize the retention of data. § 314.4(c)(6)(ii).

Expansion of the definition of 'financial institution'

The FTC's Nov. 15 announcement has not delayed an important provision of the amended Safeguards Rule, which expands the meaning of "financial institution" to include entities "significantly engaged in activities that are incidental to [] financial activity." According to the Federal Reserve Board, the only activity considered incidental to financial activity is "acting as a finder." 12 CFR § 225.86.

Financial institutions will be required to implement technical and physical access controls that authenticate only authorized users and limit authorized users' access to information as required to perform their duties and functions.

A finder is an entity that brings together one or more buyers and sellers of any product or service for a transaction that the parties themselves negotiate and consummate. 12 CFR § 225.86(d).

A finder may include an entity that:

(1) identifies potential parties;

(2) makes inquiries as to the interest;

(3) introduces and refers potential parties to each other;

(4) arranges contacts between and meetings of interested parties; and

(5) conveys between interested parties expressions of interest, bids, offers, orders, and confirmations relating to a transaction. 12 CFR § 225.86 (d)(1)(i).

Thus, the FTC's authority over the Safeguards Rule would include the following types of entities: "mortgage lenders, 'pay day' lenders, finance companies, mortgage brokers, account servicers, check cashers, wire transferors, travel agencies operated in connection with financial services, collection agencies, credit counselors and other financial advisors, tax preparation firms, non-federally insured credit unions, investment advisors that are not required to register with the Securities and Exchange Commission, and entities acting as finders." § 314.1(b).

To the extent that a business may now fall under this definition of "finders," such businesses should re-evaluate whether they now fall under the Safeguards Rule's purview.

Moving information security toward a more prescriptive approach

These changes are not without critique (the final Rule was approved along party lines). By adopting a more prescriptive approach, critics, including the two dissenting Republican Commissioners Noah J. Phillips and Christine S. Wilson, warned that the FTC risks the possibility of inadvertently distracting financial institutions with compliance activities that check-the-box, rather than allowing financial institutions to take steps toward enhancing security based on circumstances, such as considering the complexity of their information systems, size, and budget. *See* Standards for Safeguarding Customer Information, Federal Register, Dec. 9, 2021, https://bit.ly/3CMTaHz.

Critics argue this could be an issue within smaller organizations, where a single individual with few resources may be presented and tasked with meeting the FTC's more prescriptive rules.

The FTC argues that the new rules provide "sufficient flexibility" to allow financial institutions of all sizes the ability to implement information security programs that fit the unique nature of each organization.

The FTC specifically references the risk assessment requirement, stating that it sets only three general items that must be addressed: "(1) [c]riteria for evaluating risks faced by the financial institution; (2) criteria for assessing the security of its information systems; and (3) how the identified risks will be addressed." By providing only general requirements, financial institutions will be allowed to meet the risk assessment requirement "in whatever way they choose, using whatever method or approach works best for them[.]"

Conclusion

The FTC's delay in its amendment of several provisions of the Safeguards Rule provides financial institutions much-needed breathing room. Financial institutions should use this time to evaluate how the Safeguards Rule modifications affect operations, and should adjust practices to comply before June 9, 2023.

About the authors



Edgar Vargas (L) is an associate for **Troutman Pepper Hamilton Sanders'** privacy and cyber practice group and is part of the firm's consumer financial services section. He develops strategies for clients around issues related to new-to-market and emerging technologies. He also advises on the effective use of data and helps clients mitigate the potential risks associated with the commercialization of data assets. He is located in Orange County, Calif., and can be contacted at edgar.vargas@troutman.com. **Kim Phan** (C) is a partner for the firm's privacy and cyber practice group, where she is a privacy and data security attorney, who also assists companies with data breach prevention and response, including establishing effective security programs prior to a data breach and the assessment of breach response obligations following a breach. She is located in Washington, D.C., and can be contacted at kim.phan@troutman.com. **Kamran Salour** (R) is a partner for the firm's privacy and cyber practice group. He leverages his data privacy experience to guide clients through their toughest cybersecurity and privacy issues. He is CIPP/US, CIPP/E, and CIPT certified and focuses his practice on guiding his clients through the incident response process. He is located in Orange County and can be contacted at kamran.salour@troutman.com.

This article was first published on Reuters Legal News and Westlaw Today on January 26, 2023.