Updates
November 09, 2021
GLBA Safeguards Rule Updated to Impose New Data Security Requirements

Update: *This article was updated on December 14, 2021, to include that the new rule was published in the Federal Register on December 9, 2021 and will go into effect on January 10, 2022 (except for the portions with a stated one-year delay).*

Following a 3-2 vote, the Federal Trade Commission (FTC) recently announced amendments to the Safeguards Rule under the Gramm-Leach-Bliley Act. The Safeguards Rule was first promulgated in 2002. The revisions are meant to strengthen the data security safeguards employed by nonbank financial institutions (e.g., certain fintech companies, mortgage brokers, nonbank lenders, credit reporting agencies, accountants and tax preparation services, and others) to better protect customer financial information from data breaches and cyberattacks. Although the new, revised rule has a significant number of more specific requirements than the current rule, the Commission emphasized that financial institutions still maintain the flexibility to design an information security program that is appropriate to the size and complexity of the financial institution, the nature and scope of its activities, and the sensitivity of any customer information at issue.

Key Provisions in the New Safeguards Rule

Single Individual Responsible for the Information Security Program. The existing Safeguards Rule allows a covered financial institution to have one or more employees hold the responsibility for the information security program by designation. The new rule requires that a single "Qualified Individual" be solely responsible for overseeing and implementing the program. In response to comments arguing that it would be cost-prohibitive for small institutions to hire a chief information security officer (CISO), the Commission explained, "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. Only if the complexity or size of their

information systems require the services of an expert will the financial institution need to hire such an individual." At least annually, the Qualified Individual must report in writing to the board of directors or other governing body of the financial institution.

More Specific Requirements for Risk Assessments. The existing Safeguards Rule requires that information security programs be based on a financial institution's identification and assessment of reasonably foreseeable internal and external risks to customer information. The new rule continues to require risk assessments, but now also specifically requires that risk assessments be in writing and include criteria to evaluate and categorize identified security risks; criteria to assess the "confidentiality, integrity, and availability" of customer information and information systems, including whether the existing controls are adequate in context of the identified risks to customer information; and requirements that describe how risks identified will be accepted or mitigated based on the risk assessment and how the information security program will address them. While risk assessments must include these topics, each financial institution can tailor its assessments to its own structures and needs.

Specific Measures. To control the risks identified through risk assessments, financial institutions must implement a number of specific safeguards except where an exception or qualification applies, such as:

- Multifactor authentication for both consumer and internal users accessing an information system (unless the financial institution's Qualified Individual "approved in writing the use of reasonably equivalent or more secure access controls");
- Access controls for all customer information, including that stored in physical (non-electronic) systems and physical restrictions on access to hardware containing electronically stored customer information;
- The principle of least privilege ("The Commission does not believe it is appropriate, for example, for larger companies to give all employees and service providers access to all customer information.");
- Encryption of customer information in transit on external networks and at rest (unless the financial institution determines that such encryption is infeasible and instead secure such customer information using effective alternative compensating controls reviewed and approved by the institution's Qualified Individual);
- Data inventory and classification practices;
- Secure development practices;
- Change management;
- Logging and system monitoring;
- Penetration testing and vulnerability assessment;
- A written incident response plan; and
- Procedures for the secure disposal of customer information within two years of when the data was last used.

"Customer information" to be protected by the new rule includes all personally identifiable financial information held by or on behalf of the financial institution; the Commission specifically declined to narrow any of the requirements to more sensitive types of information.

Enhanced Security Training and Personnel Requirements. The existing Safeguards Rule requires security training for personnel. The new rule requires that the training be updated over time based on evolving risk assessments or changes in the financial institution's practices. It also requires that security personnel receive "security updates and training sufficient to address relevant security risks," and it requires that the financial institution keep verification that training requirements have been met. It requires that personnel in security functions be "qualified," but to allow flexibility, it does not mandate a certain type or form of qualification.

Oversight of Service Providers. The existing Safeguards Rule requires that financial institutions select appropriate service providers and require them by contract to maintain security and confidentiality. The new rule continues these requirements, and also now requires financial institutions to "periodically assess" their service providers on an ongoing basis.

Partial Exemption of Institutions that Maintain Information on a Limited Number of Consumers. The new rule allows financial institutions that maintain the customer information of less than 5,000 consumers to be exempt from certain requirements, such as the obligation to conduct written risk assessments, annual board reporting, certain monitoring and testing requirements, and a written incident response plan.

Expansion of the Definition of "Financial Institution." The new 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. The Commission stressed that this change only expands the rule to bring "finders"—a defined term consisting essentially of companies that bring together buyers and sellers of a product or service—within the rule's ambit. It also stressed that the scope limitations of the rule as a whole still govern, e.g., it only applies to finders involved in "consumer" transactions that are "for personal, family, or household purposes."

Requirements for a "Security Event." The new rule imposes certain requirements when a financial institution experiences a "security event," which it defines as "an event resulting in unauthorized access to, or disruption or misuse of, an information system, information stored on such information system, or customer information held in physical form." The Commission explained that this definition includes events affecting paper or hard copy records only, which it thinks financial institutions should protect just as much as they protect information in electronic form. It also explained that the language "or disruption or misuse of" is designed to sweep in incidents, such as ransomware, in which there is no unauthorized access but yet still, in the FTC's view, a threat to the integrity of customer information, or an indication of some other weakness in a system that could be exploited. It also rejected suggestions from commentators to add a harm threshold, or to exclude incidents affecting encrypted data without exposure of the key. The definition of "security event" under the new rule is thus much broader than the definitions of security breaches that trigger reporting under typical state data breach notification laws, but importantly the definition has a different function under the Safeguards Rule. A financial institution must have a written incident response plan that includes steps to respond to and remediate security events "materially affecting" customer information, and it must include information about security events in internal reporting.

Clarification, Expansion, or Modernization of Other Data-Security Related Terms. In addition, the new rule clarifies, expands, or modernizes definitions of several other data security terms, such as "authorized user" of an information system, "customer information," encryption, "information system," multifactor authentication, penetration testing, and "personally identifiable financial information."

* * *

The new rule will become effective a month after publication in the Federal Register but key requirements (e.g., appointment of a Qualified Individual, written risk assessments, written incident response plan) will not take effect until a year after publication in the Federal Register.

The FTC's discussion in the Federal Register Notice of its views on comments submitted during the rulemaking process and its reasoning may be of interest to entities subject to other laws or regimes regarding data security, even if the Safeguards Rule does not apply to them.

In addition to modifying the Safeguards Rule, the Commission solicited public comment on a proposed supplemental rule that would require financial institutions to report to the FTC security events in which the misuse of customer information has occurred or is reasonably likely, and at least 1,000 consumers have been affected or reasonably may be affected, within 30 days from discovery of the security event.

Authors

Explore more in

Privacy & Security Financial Services & Investments

Related insights

Update

Delaware Significantly Narrows Scope of Stockholder Inspection of Corporate Books and Records

Update

DOJ Launches Deregulation Task Force