CLIENT ALERTS & INSIGHTS

FTC Amends Financial Institution Safeguards Rule Including New Information Security Requirements

NOVEMBER 10, 2021

Authors: Ryan T. Sulkin

The updated rule also includes new exemptions, expands the definition of "financial institution," and creates new accountability requirements.

On October 27th the Federal Trade Commission ("**FTC**") adopted and published final amendments to the Safeguards Rule (the "**Rule**"). Commissioners voted 3-2 to adopt the amendments, with the narrow margin highlighting diverging theories on how best to regulate an industry suffering data breaches with growing frequency.

In 1999, Congress passed the Gramm-Leech-Bliley Act ("**GLBA**") that, among other things, outlined a framework of privacy and data protection standards that financial institutions must meet in their handling of customer information. The GLBA requires the FTC to create and update administrative, technical, and physical safeguard requirements for financial institutions to follow, which lead to the Rule.

The updates and amendments mainly consist of new information security program requirements and a new exception. The updates and amendments to the Rule will take effect on November 28, 2021 (30 days after it was published to the Federal Register).

Scope

As a reminder, the GLBA, and in turn the Rule, applies to any entity that is considered a financial institution.

The FTC and other government agencies take a broad approach in what constitutes a financial institution, as the definition includes, but is not limited to, mortgage lenders, account servicers, travel agencies operated in connection with financial services, tax preparation firms, and any other entity that engages in an activities that are "financial in nature" or related and incidental to financial activities.

The Rule, as well as the GLBA in general, only covers customer information. Breaking it down, the Rule's scope includes any individual who purchases financial products or services for personal or household purposes; and that individuals personally identifiable financial information as well as any list, description, or other grouping of such individuals that is created through the use of personally identifiable financial information.

The Rule does not govern a financial institution's use of information that is publicly available.

New Safeguards Rule

Overall, the new Rule offers financial institutions more specificity in terms of requirements and details related how a financial institution must comply with those requirements.

However, the FTC created a new exception to the Rule. Financial institutions that maintain customer information concerning fewer than 5,000 consumers do not have to comply with the requirements set forth in the Rule.

The biggest change is the Rule's specific information security program requirements. An information security program was already required under the original rule, but now the Rule requires specific measures and procedures.

Any financial institution subject to the Rule must implement an information security program that includes: **(1)** a designated individual in charge of, or overseeing and implementing, the program; **(2)** periodic risk assessments; **(3)** safeguards that control the risks identified in such risk assessments; **(4)** regular testing and monitoring of the effectiveness of the safeguards; **(5)** internal policies and procedures consistent with the information security program; **(6)** assess and oversee service providers' safeguards; **(7)** is updated in light of regular monitoring and identification or material issues identified in risk assessments; and **(8)** a written incident response plan.

The more complex requirements are explained below in greater depth.

- **Risk Assessment**

The risk assessment, which must be designed to identify reasonably foreseeable internal and external risks, must categorize any identified security risks, evaluate the adequacy of existing controls in light of those risks, and identify mitigation strategies for identified risks.

Additionally, the risk assessment must be written and conducted on a periodic basis.

- **Safeguards and Controls**

The most direct change in the Rule is its adoption of specific safeguards and controls.

A financial institution subject to the Rule must: **(1)** periodically review access controls; **(2)** identify and manage data and devices (i.e., data mapping); **(3)** encrypt all customer information-whether at rest or in transit-or use effective, adequate alternatives if encryption is infeasible; **(4)** adopt secure development practices for any software developed by the financial institution; **(5)** utilize multi-factor authentication for system access; **(6)** implement and periodically review data retention policies that ensure secure disposal of customer information within two years of the information's last use; **(7)** adopt procedures for change management; and **(8)** implement policies and procedures to monitor and log any activity or tampering that occurs in connection with customer information.

The multi-factor authentication requirement can be achieved through any verification requiring at least two of the following: **(1)** passwords; **(2)** tokens; or **(3)** biometric characteristics.

Further, if a financial institution is not continuously monitoring its systems, it must conduct annual penetration testing and biannual vulnerability assessments.

- **Personnel and Service Providers**

Under the Rule, financial institutions must employ qualified security personnel and provide periodic security awareness training to ensure the personnel can properly manage an information security program.

These requirements apply even if a financial institution uses a third-party service provider to manage the financial institution's information security program. Therefore, a financial institution must ensure that the third-party service provider is employing only qualified personnel and also implementing proper and regular training.

In their oversight of third-party service providers, a financial institution must **(1)** take reasonable steps to ensure they are only employing qualified third parties; **(2)** utilize contractual provisions to ensure proper implementation and maintenance of the required safeguards; and **(3)** periodically assess service providers to analyze the risks involved and the adequacy of the service provider's safeguards.

- **Response Plan**

The written incident response plan must be designed to quickly respond to any security event that affects the confidentiality, integrity, or availability of customer information, and must be designed to recover from any such event.

Specifically, the plan must include **(1)** the goals of the plan; **(2)** internal response processes; **(3)** clear assignment of roles, responsibility, and decision-making; **(4)** processes for internal and external communication; **(5)** requirements to identify and remediate any weaknesses in the systems or controls that lead to a security event; and **(6)** procedures related to documenting and reporting security events and the financial institutions subsequent responses.

Under the rule, a security event includes any event that results in any unauthorized access to, disruption to, or misuse of, any information system, information on such a system, or customer information held in physical form.

Close Vote

The new Rule was adopted on a narrow 3-2 vote, highlighting divergent ideologies on how the government should regulate cybersecurity and data protection.

The dissenting opinion highlighted the pitfalls of an "overly prescriptive" approach that forces a one-size-fits-all approach onto financial institutions. The fear, according to the dissent, is that financial institution compliance with the Rule will be merely performative; making sure they have the specific requirements instead of creating an information security program that is adaptive and balanced to the specific financial institution's security and data protection needs.

According to the dissent, the new requirements will divert crucial resources to “check-the-box” compliance, instead of to a more “tailored” risk management approach.

FTC Chair Lina M. Khan issued a separate statement in support of the new Rule after its adoption to highlight the need for the new requirements in a world of increasing collection of customer information (specifically, sensitive information) and data breaches.

Specifically, the statement pointed to the Equifax breach and alleged that the new Rule’s vulnerability scanning, encryption, and monitoring requirements would have likely prevented the breach.

It’s likely that the FTC and other government agencies will use rulemaking and regulations to implement and enforce stricter cybersecurity and data protection standards.

As the FTC continues to update its privacy and data protection requirements, and as financial institutions face new obligations, the Benesch Data Protection and Privacy team is committed to staying at the forefront of knowledge and experience to assist our clients in compliance efforts. We are available to assist you with any compliance needs.

Ryan T. Sulkin at rsulkin@beneschlaw.com or 312.624.6398.

Lucas Schaetzel at lschaetzel@beneschlaw.com or 312.212.4977.