CLIENT ALERTS & INSIGHTS

FTC Amends Financial Institution Safeguards Rule to Include New Obligation to Report Notification of Data Security Breaches

NOVEMBER 28, 2023

Authors: Megan C. Parker

The amended rule requires financial institutions to notify the FTC within 30 days of discovery of a security breach involving information of at least 500 consumers.

On October 27th the Federal Trade Commission ("**FTC**") approved and published a new amendment to the Safeguards Rule (the "**Safeguards Rule**") requiring financial institutions to report certain data breaches and other security events to the agency. Commissioners voted 3-0, highlighting a unanimous effort to continue combating widespread data breaches and cyberattacks.

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 Safeguards Rule and its companion, the Privacy Rule.

The new amendment to the Safeguards Rule follows on the heels of the FTC's 2021 amendments to the Safeguards Rule adding specific security measures-and a more prescriptive approach-to how the FTC is approaching the Safeguards Rule moving forward. The data breach requirements follow in-step with a more prescriptive approach and follows other government agencies' lead in implementing data breach standards.

The 2023 amendment to the Safeguards Rule consists of the new requirement that financial institutions report notification events to the FTC through an online reporting form to be made available on FTC.gov. The form is not yet available. The amendment to the Safeguards Rule will take effect 180 days after publication of the amended Safeguards Rule in the Federal Register.

Amended Safeguards Rule

- **Who Must Comply**

The new notification obligation would apply to financial institutions currently subject to the FTC's existing Safeguards Rule, including (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 activity that is financial in nature or related and incidental to financial activities.

- **Information Triggering Notification Obligation**

Similar to the existing Safeguards Rule, the amended Safeguards Rule applies to "customer information," which is non-public, personally identifiable financial information about individual who purchases financial products or services for personal or household purposes; including any list, description, or other grouping of such individuals that is created through the use of their personally identifiable financial information.

Neither the existing nor amended Safeguards Rule governs or regulates a financial institution's use of information that is publicly available.

- **Event Triggering Notification Obligation**

Notification is required for a "notification event" that impacts the customer information of at least 500 consumers. The amended Safeguards Rule defines a notification event as any "acquisition of unencrypted customer information without the authorization of the individual to which the information pertains." Notification of all incidents meeting this definition, including those with no risk of harm, must be reported to the FTC.

If there is such unauthorized access to customer information, the affected financial institution must demonstrate that the unencrypted customer information was not or could not reasonably have been acquired; otherwise, the incident is presumed to involve unencrypted customer information.

This definition not only covers traditional data breaches and security incidents, but also any voluntary or intentional sharing of customer information by a financial institution if done without the consent of the individual to whom the information pertains. It is important to keep in mind that an event giving rise to a "notification event" may be caused by a violation of GLBA's Privacy Rule.

- **Contents of Required Notification**

The content of the newly required notification to the FTC must include: (1) the name and contract information of the reporting company; (2) a description of the customer information involved; (3) the date range of the event, if it can be determined; (4) the number of impacted consumers; (5) a general description of the event; (6) whether a law enforcement has given notification in writing that informing the public would impede a criminal investigation or cause damage to national security; and (7) the contact information for the law enforcement official if such written notification is given.

- **Timeline for Notification**

Notification to the FTC must be made as soon as possible, but no later than 30 days after they are discovered. The amended Safeguards Rule provides that discovery occurs on "the first day on which such event is known . . . to any person, other than the person committing the breach, who is the financial institution's employee, officer, or other agent."

As reliance on technology providers and vendors that have access to personal information rises, in-scope entities need to keep the new Safeguards Rule's notification requirements in mind to ensure their technology providers and vendors alike have obligations to provide prompt (if not immediate) notice to the in-scope entity, for the in-scope entity to meet its reporting obligations.

- **Notification Will Be Public**

The FTC plans to publish such notification event reports in a publicly available database, with limited exception to those that law enforcement indicates would impede criminal investigation or cause damage to national security. Further, the FTC declined to impose a requirement of individual notification to affected consumers; although businesses and financial institutions alike still need to comply with U.S. state data breach notification laws along with the Interagency Guidelines promulgated by the FTC, CFPB, OCC, and FRB under GLBA, which requires in-scope entities to have data breach response programs in place that include customer notice.

Conclusion and Takeaways

Coupled with the new data security obligations under the Safeguards Rule from the FTC's 2021 amendment, the 2023 amendment represents a significant expansion of the FTC's requirements for financial institutions and demonstrates a focus on transparency regarding data breaches and other cybersecurity events in the United States.

As the FTC continues to update is 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.

Megan Parker at MParker@beneschlaw.com or 216.363.4416

Luke Schaetzel at lschaetzel@beneschlaw.com or 312.212.4977.