THOMPSON HINE

Privacy & Cybersecurity Update

November 2023

FTC Amends Safeguards Rule and Data Breach Notification Obligations

The Federal Trade Commission (FTC) has approved an amendment to its Safeguards Rule that requires non-banking financial institutions to report certain data breaches and other security events to the agency. This data breach notification obligation is separate and distinct from the cybersecurity and risk management rule recently promulgated by the Securities and Exchange Commission (SEC), which requires certain publicly traded companies to make public disclosures related to security incidents impacting their business. The FTC and SEC regulations present organizations with an important opportunity to reassess their data security incident plans to ensure they align with evolving information security threats and new data breach notification obligations.

Background

The FTC's Safeguards Rule requires non-banking financial institutions (e.g., mortgage brokers, motor vehicle dealers, and payday lenders) to develop, implement, and maintain a comprehensive information security program to protect the confidentiality and security of their customers' personal information. In October 2021, the FTC finalized changes to the Safeguards Rule that provide more concrete guidance for businesses and reflect core data security principles that all covered companies need to implement and maintain.

The Safeguards Rule amendment applies to financial institutions that are subject to the FTC's jurisdiction and are **not** subject to the enforcement authority of another regulator under the Gramm-Leach-Bliley Act, which defines "financial institution" as an entity that engages in an activity that is "financial in nature" or "incidental" to such financial activities.

New Reporting Requirements for Notification Events

Pursuant to the new Safeguards Rule amendment, covered financial institutions must report each "*notification event*" that involves *at least 500* customers to the FTC. A "notification event" is defined as the "acquisition of unencrypted customer information without the authorization of the individual to which the information pertains." In turn, customer information is considered "unencrypted" for purposes of the rule if the "encryption key was accessed by an unauthorized person" and "[u]nauthorized acquisition will be presumed to include unauthorized access to unencrypted customer information unless you have reliable evidence showing that there has not been, or could not reasonably have been, unauthorized acquisition of such information."

A covered financial institution must notify the FTC *as soon as possible, and no later than 30 days after discovery* of a notification event. The rule treats a notification event as discovered *as of the first day the event* is known by an employee, officer, or other agent of the company who did not commit the breach. In explaining this requirement, the FTC clarifies that discovery includes circumstances when an "employee, officer, or other agent of the financial institution accesses customer information without authorization," and that event "is known to another employee, officer, or other agent of the financial institution." Therefore, the reporting requirement considers

security incidents that implicates the actions of internal and external actors.

As is common in other federal and state data breach notification requirements, a covered entity must disclose the notification event to the FTC via an online webform available on the FTC's website. This disclosure must include:

- The name and contact information of the financial institution
- A description of the types of information impacted by the notification event
- The date or date range of the notification event, if it's possible to determine
- The number of individuals impacted by the notification event
- A general description of the notification event
- Where applicable, whether the reporting was delayed as a result of a law enforcement investigation

According to the new Safeguards Rule amendment, "[a] law enforcement official may request an initial delay of up to 30 days following the date when notice was provided" to the FTC by the impacted organization. This delay may be extended for an additional period of up to 60 days if the law enforcement official seeks such an extension in writing. Additional delay may be permitted only if the FTC staff determines that public disclosure of a security event continues to impede a criminal investigation or cause damage to national security.

FOR MORE INFORMATION

For more information, please contact:

Steven G. Stransky
216.566.5646
202.263.4126
Steve.Stransky@ThompsonHine.com
Certified Information Privacy Professional/Government (CIPP/G)
Certified Information Privacy Professional/United States (CIPP/US)

Thomas F. Zych
216.566.5605
Tom.Zych@ThompsonHine.com

Marla M. Izbicky
312.998.4253
Marla.Izbicky@ThompsonHine.com
Certified Information Privacy Professional/United States (CIPP/US)

Thora Knight
212.908.3971
Thora.Knight@ThompsonHine.com