HINSHAW

What Businesses Must Know About the New Federal Trade Commission Amendments on the Safeguards Rule

Privacy, Cyber & AI Decoded Alert | 2 min read
May 23, 2024

The recent Federal Trade Commission (FTC) amendment adds a new security breach reporting requirement to the Gramm–Leach–Bliley Act (GLBA) Safeguards Rule. The Safeguards Rule is a regulatory framework that mandates financial institutions to implement security measures for protecting customer data.

The amendment requires financial institutions to notify the FTC as soon as possible but no later than **30 days after the discovery of the security breach involving customer information of 500 or more customers.**

What Event Triggers Notification?

An unauthorized acquisition of unencrypted customer information triggers notification.

Customer information is considered unencrypted for this purpose if the encryption key is accessed by an unauthorized person. Unauthorized acquisition will be presumed to include unauthorized access to unencrypted customer information unless you have reliable evidence showing there has not been, or could not reasonably have been, unauthorized acquisition of such information.

When Did the Amendment Take Effect?

In October 2023, the FTC revised the requirements for reporting data breaches and security incidents but gave businesses six months to get ready for the changes. The above change took effect on Monday, **May 13, 2024**.

What Entities do the Safeguards Rule Reporting Requirements Apply to?

The Safeguards Rule applies to non-banking financial institutions, including mortgage lenders, to protect customer information security. The rule applies to financial institutions under FTC jurisdiction.

The Rule specifies the following examples of businesses that are covered, including but not limited to:

- mortgage lenders,
- payday lenders,
- finance companies,
- mortgage brokers,
- account servicers,
- check cashers,
- wire transferors,
- collection agencies,
- credit counselors and other financial advisors,
- tax preparation firms,
- non-federally insured credit unions, and
- investment advisors that aren't required to register with the SEC.

Are There any Exceptions to this Requirement?

- Similar to state breach notification laws, the amendment provides an exception to the time limit for reporting in the amendment if law enforcement requests an extension to public disclosure.
- Encrypted information where the encryption keys were not accessed.

If I Notify State Regulatory Bodies or the SEC About a Security Incident, do I Still Need to Notify the FTC?

Yes, this is a separate requirement.

What are the Enforcement Penalties if my Entity Does Not Comply?

The risk of large fines, not to mention lawsuits and negative press, for wrongly deciding the breach does not require timely reporting to the FTC, which means that qualified professionals must be involved with the review and decision.

The Safeguards Rule's enforcement penalties have so far ranged from Equifax agreeing to a settlement between $575 million and $700 million to Ascension Data & Analytics, LLC agreeing to implement and maintain

comprehensive data security programs overseen by designated employees, among other specific requirements.

Noncompliance penalties include fines of up to $100,000.00 per violation for the financial institution and fines of $10,000.00 for the individual found in violation. We are increasingly seeing regulators holding executive officers responsible for these types of actions.

What Should I Do to Comply Now?

Companies that must comply with the Safeguards Rule should amend their entity's incident response plan to include reporting the incident within the required time period to the FTC as part of the plan.

Related People

Cathy Mulrow-Peattie

Partner

212-655-3875

Related Capabilities

Consumer Financial Services

Data Privacy, AI & Cybersecurity