Akin®

FTC Requires Non-Banking Financial Institutions to Report Data Security Breaches

February 12, 2024

Reading Time : **3 min**

By: Natasha G. Kohne, Sara Catherine Ainsworth

Beginning May 11, 2024, non-banking financial institutions regulated by the Federal Trade Commission (FTC) will be required to submit notifications of data breaches or other security events that impact 500+ consumers. The FTC issued a final rule (the Rule) amending its Safeguards Rule[1] to impose this notification requirement. The FTC has indicated that such notices will be entered into a publicly available database. Below, we have outlined key requirements for non-banking financial institutions and next steps for compliance.

Key Requirements of the Revised Safeguard Rule

Who Needs to Report?

The Rule applies to all non-banking financial institutions regulated by the FTC, including exempt reporting advisers, state-registered advisers, technology companies, mortgage brokers, credit counselors, financial planners, credit reporting agencies and tax preparers, among others.

When Do You Need to Report?

The Rule requires covered entities to report a "notification event" that impacts at least 500 consumers to the FTC as soon as possible, but no later than 30 days following discovery. A "notification event" means acquisition of unencrypted "customer information" without the authorization of such customer. It is important to keep in mind that under the Safeguards Rule, "customer information" is defined broadly to mean any record containing nonpublic personal information about a customer. For example, such information may include

information provided by the consumer to obtain a financial product or service and information collected through cookies on a website.[2] The scope of noticeable information as defined in the Rule is much broader than most state data breach notification statutes.

Additionally, in defining a notification event, the FTC specifies that "customer information is considered unencrypted for this purpose if the encryption key was accessed by an unauthorized person."

The Rule also specifies that a notification event is considered discovered as of the first day on which the notification event is known to any person (other than the person committing the breach) that is an employee, officer or agent of the financial institution.

How Do You Report?

Notice to the FTC must be made electronically through a form that will be made available on the FTC's website.

What Do You Need to Report?

The notice to the FTC must include:

- Name and contact information of the reporting institution.
- A description of the types of information that were involved.
- The date or date range of the notification event (if possible to determine).
- Number of consumers affected.
- A general description of the notification event.
- If applicable, whether any law enforcement official has provided the financial institution with a written determination that notifying the public of the breach would impede a criminal investigation or cause damage to national security, and a means for the FTC to contact the law enforcement official.

Notably, though not an exception to reporting requirement, the Rule provides that a law enforcement official may request a delay in the notice of up to 30 days. The delay may be extended for an additional period of up to 60 days if the law enforcement official seeks such an extension in writing. Such additional delay may only be permitted if the FTC staff determines that public disclosure would continue to impede a criminal investigation or cause damage to national security.

When Will the Rule Go into Effect?

The Rule will take effect May 11, 2024, which is 180 days after the Rule was published the *Federal Register* (November 13, 2023).

Next Steps

Covered institutions should review existing incident response plans and related policies and procedures to ensure that notification requirements enable timely reporting under the Rule. Additionally, the Rule will likely lead to increased exposure for covered institutions and further affirms the FTC's ongoing engagement in security and privacy enforcement. Such entities should review their privacy and security programs for compliance with the Safeguards Rule and other requirements and implement any measures needed to enhance such compliance.

We will continue to monitor developments in this space and are happy to assist with your assessment of the Rule and your compliance programs. Please contact a member of Akin's cybersecurity, privacy and data protection team to learn more about how these incoming regulations may affect your company.

---

1 The Safeguards Rule took effect in 2003 and was recently updated in 2021 to specify what safeguards financial institutions must implement as part of a security program to protect their customer's financial information. This updated did not include any breach notification requirements, which was the purpose of the Rule. For additional information on the 2021 updates to the Safeguards Rule, please see our previous blog post here.

2 Note that the Safeguards Rule provides that a "cookie" is an information collecting device from a web server. 16 C.F.R § 314(n)(2).

Categories

Cybersecurity, Privacy & Data Protection | Data Breach