

FTC Issues Final Rule on New Breach Notice Requirement for Non-Bank Financial Institutions

On October 27, 2023, the Federal Trade Commission (FTC) announced a [significant amendment](#) to the agency's Safeguards Rule under the Gramm-Leach-Bliley Act (GLBA). This amendment, reflecting an increasingly strident stance by the FTC on cybersecurity topics, mandates that non-banking financial institutions report certain data breaches and security events. Interestingly, the prudential banking regulators introduced data breach notice requirements, using GLBA authority in 2005. At that time, the FTC did not follow, perhaps because of the agency's more limited rulemaking authority and because data breaches and notification are not specifically mentioned in GLBA. As a result of the revisions to the FTC Safeguards Rule, non-banking financial institutions will face federal notification requirements in addition to notice requirements under U.S. state laws.

The new rule, which becomes effective on May 13, 2024, requires notification to the FTC when a covered financial institution experiences a "notification event," defined as "acquisition of unencrypted customer information without the authorization of the individual to which the information pertains" involving at least 500 consumers. The notice must be submitted "as soon as possible and no later than 30 days after discovery of the event" and must include: (1) the name and contact information of the reporting financial institution; (2) a description of the types of information involved in the notification event; (3) if possible to determine, the date or date range of the notification event; (4) the number of consumers affected; (5) a general description of the notification event; and, 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. The notice must be provided electronically through a form to be accessible on the FTC's website.

Regarding the timing of the notification requirement, the FTC provides additional guidance on when a notification event is deemed to have been discovered, stating a "notification event shall be treated as discovered as of the first day on which such event is known to you. You shall be deemed to have knowledge of a notification event if such event is known to any person, other than the person committing the breach, who is your employee, officer, or other agent."

As we noted, the FTC has been notably more aggressive in rulemaking and enforcement actions involving cybersecurity in the past few years. Here are some additional alerts about notable FTC actions:

- [FTC issues fine to GoodRx over information sharing \(thompsoncoburn.com\)](#)
- [FTC solicits feedback on advance notice of proposed rulemaking related to commercial surveillance and data security practices \(thompsoncoburn.com\)](#)
- [Federal Trade Commission publishes final updated Safeguards Rule \(thompsoncoburn.com\)](#)

authorsTest