Reinhart

Covered Entities Must Comply with FTC Safeguards Rule

UPDATE: Compliance deadline extended to June 9, 2023.

Late last year, the Federal Trade Commission (FTC) released the final amendment to its Safeguards Rule, expanding on the types of entities covered by the Safeguards Rule and the specific elements required of the covered entity's security program in order to adequately protect customer information. While the effective date for certain requirements under the Safeguards Rule was initially delayed, the deadline for compliance is approaching quickly. On June 9, 2023 (formerly December 9, 2022), all covered entities will be expected to comply with all requirements of the amended Safeguards Rule.

Covered entities include all financial institutions under the FTC's authority, including mortgage lenders and brokers, finance companies, account servicers, collection agencies and financial advisers. Additionally, any entity "significantly engaged" in activities incidental to financial activities must comply with the Safeguards Rule, including retailers extending their own credit, dealers leasing automobiles longer than 90 days, and any entity acting as a "finder" by bringing buyers and sellers together. However, there is some relief in the form of certain exemptions for entities that collect information from less than 5,000 consumers in total.

If you are a covered entity, the Safeguards Rule requires the following administrative, technical and procedural safeguards:

1. Designating a qualified individual to oversee and enforce your information security program and collecting an annual written status report from the designated individual. This individual can be an affiliate or service provider, subject to the direction and oversight of a senior member of your team.

2. Conducting a regular written risk assessment that identifies your particular risks and threats, the adequacy of existing safeguards to address such risks and threats, and the manner of mitigation for any unaddressed risks and threats.

3. Implementing appropriate safeguards to control risks identified by your written risk assessment, including user access controls, encryption of all

POSTED:

Nov 4, 2022

RELATED PRACTICES:

Corporate Law
https://www.reinhartlaw.com/practices/corporate-law

Consumer Finance
https://www.reinhartlaw.com/practices/consumer-finance

RELATED SERVICES:

Data Privacy and Cybersecurity
https://www.reinhartlaw.com/services/data-privacy-and-cybersecurity

RELATED PEOPLE:

Kristi J. French
https://www.reinhartlaw.com/people/kristi-french

Jordan Jozwik
https://www.reinhartlaw.com/people/jordan-jozwik

customer information in transit and at rest, multifactor authentication for any individual accessing information, specific retention and disposal protocols, and consistent monitoring.

4. Performing annual penetration testing and biannual vulnerability assessments.
5. Establishing a written incident response plan identifying internal response processes, levels of decision-making authority, remediation methods for identified weaknesses, and appropriate documentation and reporting methods for incident responses.

If you are not sure whether you are a covered entity under the Safeguards Rule, or if you need compliance guidance, please contact Kristi French, Jordan Jozwik or your Reinhart attorney.