

FTC Overhauls Safeguards Rule Regarding Customer Information Applicable to Auto-Dealers and Other “Financial Institutions”

Privacy, Cyber & AI Decoded Alert | 6 min read

Dec 2, 2021

On October 27, 2021, the FTC [announced](#) that it intends to publish (1) a final rule to amend the Standards for Safeguarding Customer Information (Safeguards Rule); (2) a supplemental notice and request for public comment on further amendments to the Safeguards Rule; and (3) a final rule to amend the Privacy of Consumer Financial Information Rule (Privacy Rule) under the Gramm-Leach-Bliley Act (collectively, GLBA Rules).

To whom does it apply?

At present, the Safeguards Rule applies to “financial institutions,” defined as institutions “engaging in financial activities,” including auto-dealers, real estate appraisers, tax preparers, and investment advisors.^[1] In addition to those subject to the existing rule, the amended Safeguards Rule *may* apply to internet service providers, the gig economy, and online marketplaces.

The amended Safeguards Rule is expanded to include institutions “engaging in an activity that is financial in nature *or incidental to such financial activities*.” The practical effect of this language is to bring “finders” – e.g., “companies that bring together one or more buyers and sellers of any product or service that the parties themselves negotiate and consummate” – within the scope of the Safeguards Rule.^[2]

The definition of “finders” was developed by the Board of Governors of the Federal Reserve System (Board). In doing so, the Board gave examples of finder activities and services:

- (A) Identifying potential parties, making inquiries as to interest, introducing and referring potential parties to each other, and arranging contacts between and meetings of interested parties;
- (B) Conveying between interested parties expressions of interest, bids, offers, orders, and confirmations relating to a transaction; []
- (C) Transmitting information concerning products and services to potential parties in connection with the activities described in paragraphs [(A) and (B)] of this section [; and]
-
- [(D)] Operating an Internet web site that allows multiple buyers and sellers to exchange information concerning the products and services that they are willing to purchase or sell, locate potential counterparties for transactions, aggregate orders for goods or services with those made by other parties, and enter into transactions between themselves.^[3]

The amendment ostensibly aims to bring the FTC’s definition of “financial institution” “into harmony with other agencies’ GLB[A] Rules.”^[4] The FTC, however, did not compensate for the narrower enforcement jurisdiction of those “other agencies” that inherently limit the type of businesses subject to their rules.^[5] For example, when used by the Board, the term “finder” defines which activities are permissible for a certain subset of Bank Holding Companies. Conversely, the FTC has jurisdiction over any business that affects commerce, *except* banks, savings and loan institutions, federal credit unions, and common carriers.^[6]

The Association of National Advertisers, the Internet Association, and other commentators had raised concerns over the breadth of this definition. The Commission acknowledged in the final rule that the “language is somewhat broad,” but argued that the scope was limited to (a) transactions that are for “personal, family, or household purposes,” and (b) information of consumers with whom the “financial institution” has a “continuing relationship.” The Commission stated its belief that these limitations would exclude “most advertising agencies and similar businesses.” The Commission did not offer similar reassurances to the Internet Association, whose members range from online marketplaces to pioneers of the gig economy. The FTC rejected a request from the National Federation of Independent Business to exclude individuals and sole proprietors from the definition of “financial institution.”

The Commission did not update the examples of what constitutes a “continuing relationship” to reflect the revised definition of “financial institutions.” For now, the only thing we know for sure is that the amended Safeguards Rule will apply to “entities that perform finding services for consumers with whom they have an ongoing relationship,” and “will not apply to finders that have only isolated interactions with consumers *and* that do not receive information from other financial institutions about those institutions’ customers.”^[7] Future enforcement actions will shed light on whether the FTC intends to apply the Safeguards Rule to broad new sectors of the economy.

The amended Privacy Rule, on the other hand, only applies to “financial institutions” that are “predominantly engaged in the sale and servicing of motor vehicles or the leasing and servicing of motor vehicles, excluding those dealers that directly extend credit to consumers and do not routinely assign the extensions of credit to an unaffiliated third party.”

What type of information does it cover?

The amended Safeguards Rule applies to any information about a customer that is (a) provided by the consumer to obtain products or services; (b) about the consumer resulting from the transaction; or (c) otherwise obtained about the consumer in connection with the transaction. This includes any “list, description, or other grouping of consumers” derived therefrom that is not publicly available. A customer is a consumer with a continuing relationship with a “financial institution” who obtains any product or service offered by a “financial institution” to be used primarily for personal, family, or household purposes.

The Commission acknowledged the broad scope of information covered by the amended Safeguards Rule and rejected comments suggesting the Commission should specifically exempt aggregated or deidentified information that does not contain personal identifiers. “It includes not just information associated with types of personal information such as a name or address or account number, but also information linked to a persistent identifier” such as internet cookies.

What obligations does it Impose?

The amended Safeguards Rule expands the requirements imposed on a financial institution’s information security program. Financial institutions will be required to assess, develop, and implement safeguards for access controls; data inventory and classification; encryption; secure development practices; authentication; information disposal procedures; change management; testing; and incident response. The assessment, development, and implementation of these safeguards must be memorialized in writing.

Businesses subject to the amended Safeguards Rule must implement safeguards to control identified risks by taking certain proscribed measures, including encrypting all customer information to the maximum extent feasible; adopting multi-factor authentication for all means of access; disposing of customer information within two years; undergoing annual penetration testing; and performing system-wide scans every six months.

Financial institutions must also provide employee training on these safeguards and appropriate oversight of service providers. While the training and oversight is nothing new, the amended Safeguards Rule adds, what the Commission deems, “mechanisms designed to ensure that such training and oversight are effective.”

The amended Safeguards Rule also “adds requirements designed to improve accountability of financial institutions’ information security programs.” One such requirement is that a single “Qualified Individual” be responsible for the information security program and provide periodic reports to boards of directors or a senior officer of the business.

The supplemental amendment to the Safeguards Rule, if passed, would also require that financial institutions report detected security events to the Commission under certain circumstances.

How is it enforced?

Once the Commission has promulgated a trade regulation rule, anyone who violates the rule may be regarded as engaging in an unfair or deceptive act or practice in violation of the Federal Trade Commission Act. Companies that fail to comply with the rule could be subject to monetary penalties of up to \$43,792 per violation per day.

Where does it stand?

The amendment to the Safeguards Rule passed the Commission on a 3-2 vote. FTC Chair Lina M. Khan and Commissioner Rebecca K. Slaughter issued a [Joint Statement](#) in favor of the final rule. Commissioners Christine S. Wilson and Noah J. Phillips issued a [Joint Dissenting Statement](#). The Commission voted unanimously in favor of the other two publications.

Although the agency may have a legal fight on its hands over the use of “zombie” votes cast by former Commissioner Rohit Chopra before he stepped down on October 12, 2021, [\[8\] initial reporting](#) suggests that the Commission voted on the amended Safeguards Rule before Mr. Chopra officially departed. Still, the three actions the FTC announced on October 27, 2021 have yet to be published in the Federal Register.

[1] 16 CFR § 314.2(a) (eff. May 23, 2002); 16 CFR § 313.3(k)(1) (eff. Jan. 1, 2012).

[2] 12 U.S.C. § 1843(k)(4)(F); 12 CFR § 225.86(d)(1).

[3] 12 CFR § 225.86(d)(1)(i)(A) – (ii)(C).

[4] Final Safeguards Rule, p. 17.

[5] Those agencies are the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, the Board of Directors of the Federal Deposit Insurance Corporation, the National Credit Union Administration Board, and the Securities and Exchange Commission.

[6] 15 U.S.C. § 46(a).

[7] Final Safeguards Rule, pp. 18-19.

[8] See Letter from EVP and Chief Counsel Daryl Joseffer, U.S. Chamber Litigation Center, to Chair Lina Khan, Federal Trade Commission (Nov. 19, 2021), https://www.uschamber.com/assets/documents/211117_Comments_Zombie-Voting_FTC-with-signature.pdf; see also Dissenting Statement of Comm’rs Wilson and Phillips Regarding the Statement of the Commission on Use of Prior Approval Provisions in Merger Cases (Oct. 29, 2021), https://www.ftc.gov/system/files/documents/public_statements/1598095/wilson_phillips_prior_approval_dissenting_statement_102921.pdf.

Hinshaw & Culbertson LLP is a U.S.-based law firm with offices nationwide. The firm’s national reputation spans the insurance industry, the financial services sector, professional services, and other highly regulated industries. Hinshaw provides holistic legal solutions—from litigation and dispute resolution, and business advisory and transactional services, to regulatory compliance—for clients of all sizes. Visit www.hinshawlaw.com for more information and follow @Hinshaw on LinkedIn and X.

Related Capabilities

Data Privacy, AI & Cybersecurity

