

Services

[Privacy & Data Security](#)

FTC's Final Rule Amending Standards for Safeguarding Customer Information

On June 9, 2023 the FTC's Amended Safeguards Rule, pertaining to the safeguarding of customer information, became fully effective. The amendment was published in final form on December 9, 2021 by the Federal Trade Commission ("FTC"), in 86 FR 70272-01. The FTC sought, in the Amended Safeguards Rule, to update the Safeguards Rule promulgated under the 2003 Gramm-Leach-Bliley Act (the "GLBA") to address nearly two decades of changes in technology. The previous Safeguards Rule required financial institutions to implement an information security program that included sufficient safeguards to ensure the security and confidentiality of customer information against unauthorized access from identified threats.

The Amended Safeguards Rule amends the previous rule by (a) providing specific guidelines regarding a financial institutions' information security program including (i) designating an individual who will be accountable for the program's implementation and oversight, and (ii) offering guidance on how a program must identify and assess risks, and how those identified risks must be controlled; and (b) clarifying which institutions/organizations are subject to the Amended Safeguard Rule.

(a) What is required of a financial institution?

The Amended Safeguards Rule lays out the following requirements of a financial institution's information security program:

(1) Designation of a Qualified Individual for overseeing and implementing the program in order to increase accountability.

- This "Qualified Individual" may be an employee of the financial institution itself, an affiliate, or a service provider.
 - Please note however, if the Qualified Individual is an employee of an affiliate or service provider, the financial institution still retains responsibility for the program and must designate a senior member from among its personnel to furnish direction and oversight of the individual to ensure the individual's compliance with the Amended Safeguard Rule.
- Additionally, the Qualified Individual must report in writing, at least annually, to the board of directors or equivalent governing body of the institution, and such report must include the overall status of the information security program and its compliance with the Amended Safeguard Rule as well as any other material matters relating to the information security program.

(2) Establishing an internal process routinely to perform Risk Assessments.

- The financial institution needs to perform a written risk assessment that periodically identifies both internal and external risks to the security of confidential customer information, evaluates existing safeguards, and establishes requirements for mitigating those identified risks.

(3) Design and implement safeguards to control the identified risks.

- Said safeguards must be established and implemented such that authorized users are allowed access only to that customer information that is necessary, and any authorized user's activity must be logged.
- All customer information held or transmitted must be encrypted, and any customer information that is held or transmitted must be stored at all times within applications assessed and evaluated for security.
- Multi-factor authentication must be implemented for any individual accessing the information system.
- Customer information that is no longer necessary for business operations must be securely disposed of no later than two years after the last date the information was used.
- All of the safeguards and policies must be routinely evaluated to monitor their effectiveness.
 - If the safeguards and policies are no longer sufficient based on the institution's risk assessment, the safeguards must be adjusted such that the security program is up to date.
- There must be procedures implemented to ensure that personnel are able to enact the information security program.
- There must be a written incident response plan that identifies the process for responding to a security event, to allow the financial institution promptly to respond to and recover from any security event.

(b) Who does the Safeguards Rule apply to?

As mentioned throughout, the Safeguards Rule applies to "financial institutions" as defined by the FTC in 16 C.F.R. § 314.2(h), "[a]n institution that is significantly engaged in financial activities, or significantly engaged in activities incidental to such financial activities," and provides the following examples of entities that fall within this definition:

- a retailer that extends credit directly to customers;
- an automobile dealership that leases automobiles on a nonoperating business for longer than 90 days;
- a personal property or real estate appraiser;
- a career counselor that serves individuals involved in the financial industry;
- a business that prints and sells checks for consumers;
- a business that regularly wires money to and from consumers;
- a check cashing business;
- accountant or other tax preparation service;
- travel agencies;
- real estate settlement service providing entities;
- mortgage brokers;
- investment advisory company;
- a company acting as a finder in bringing together one or more buyers and sellers of any product or service.

Key Contacts**Bryan Stanley**

Kansas City
(816) 502-4645
bryan.stanley@kutakrock.com

Ed Marquette

Kansas City
(816) 502-4646
ed.marquette@kutakrock.com

Turquoise Early

Omaha
(402) 930-8019
turquoise.early@kutakrock.com

The Amended Safeguards Rule exempts businesses that collect information from fewer than 5,000 customers and expands the definition of “financial institutions” to include “finders,” which are companies that collect and maintain customer financial information to connect buyers and sellers of a product or service. The Amended Safeguards Rule can now be reviewed in its entirety in 16 C.F.R.

The full text of the article published by the FTC, entitled “FTC Safeguards Rule: What Your Business Needs to Know,” can be found [here](#). If you have questions about the Amended Safeguards Rule or the changes in the current standards, please contact your Kutak Rock attorney or one of the authors listed on the left. You can also visit us at www.KutakRock.com.

