Guide

The FTC's New Safeguards Rule + You:

Industries Impacted and What It Means for Your IT Strategy

entech

Table of Contents

The FTC's New Safeguards Rule + You:

Industries Impacted and What It Means for Your IT Strategy

When most of us hear the term "financial institution," our minds go straight to the traditional definition: banks and lenders. But the Federal Trade Commission (FTC) uses a much broader definition.

This means that if your business is handling sensitive consumer data around financial transactions, you're likely to be impacted by their new Safeguards Ruling that **goes into effect on summer 2023** —and will need to comply with several new updates and requirements— all of which will impact your IT planning, strategy, and budgeting as well.

In this Guide, we'll break down the FTC's "legalese" for you so you know if you're affected, what's new with these updates, what you'll need to do to be compliant and when, and lay out a roadmap to help you get there a little more easily.

1. What is the FTC Safeguards Rule (and Why Should I Care?)

First, a little background. Short for Standards for Safeguarding Consumer Information, the Safeguards Rule is part of The Gramm-Leach-Bliley Act of 1999 and meant to ensure that the security of consumer information is properly protected and secured by the business entities that handle it.

The Safeguards Rule was initially enacted in 2003, but in 2021, the FTC took actions to update and amend it. This was done in response to the immense changes in technology since 2003 as well as recent consumer data breaches. While the Gramm-Leach-Bliley Act is more extensive in its compliance requirements, the Safeguards Rule focuses on consumer information security and requires financial institutions covered under the FTC's jurisdiction to establish and maintain what they call a "reasonable information security program."

Reflective of the core data security principles the FTC now requires all covered businesses to implement, it's the type of rule that as consumers, we're thankful exists, but for businesses, can (rightfully) mean a lot of planning, process, and time invested in achieving compliance. However, another way to look at this ruling is as a tool you can use to ensure your business is taking proactive steps to stay on top of security and prevent the negative consequences associated with a preventable data breach.

2. Industries Impacted and How to Be Compliant

As we mentioned, the FTC's definition of a financial institution is a bit broader than what typically comes to mind.

FTC Definition of a Financial Institution

"*Financial institution* means any institution the business of which is engaging in an activity that is financial in nature or incidental to such financial activities as described in section 4(k) of the Bank Holding Company Act of 1956, 12 U.S.C. 1843(k). An institution that is significantly engaged in financial activities, or significantly engaged in activities incidental to such financial activities, is a financial institution." FTC 16 CFR 314.2

For example, they state that a bar or restaurant who "runs a tab" for a customer does not qualify as being "significantly engaged in financial activities", but a retailer who issues a formal line of credit to their customers would qualify.

We've validated some more clear-cut examples of businesses who are covered under the FTC's jurisdiction. The National Archives Code of Federal Regulations states that your business qualifies as a financial institution under the new FTC Safeguards if you're a(an):

1. **Automobile Dealerships:** "An automobile dealership that leases automobiles on a nonoperating basis for longer than 90 days."
2. **Accountants and Tax Preparation Services:** "An accountant or other tax preparation service, completing income tax returns."
3. **Investment Advisors:** "An investment advisory company and a credit counseling service."
4. **Real Estate Settlement Firms:** "An entity that provides real estate settlement services."

5. **Mortgage Brokers:** “A mortgage broker because they transact loans.”
6. **Real Estate Appraisers:** “A personal property or real estate appraiser.”
7. **Travel Agencies:** “A travel agency with related financial services.”
8. **Career Counselors:** “A career counselor that specializes in providing career counseling services to individuals currently employed by or recently displaced from a financial organization, individuals who are seeking employment with a financial organization, or individuals who are currently employed by or seeking placement with the finance, accounting, or audit departments of any company.”
9. **Check Cashing Companies:** “A check cashing business because money is exchanged.”
10. **Check Printing Companies:** “A business that prints and sells checks for consumers, either as its sole business or as one of its product lines.”
11. **Businesses That Wire Money:** “A business that regularly wires money to and from consumers.”
12. **Retailers:** “A retailer that extends credit by issuing its own credit card directly to consumers.”
13. **Finders:** "This category of business represents a new expansion under the latest Safeguards update. A company acting as a finder in bringing together one or more buyers and sellers of any product or service for transactions they negotiate and consummate.”

Small Business Exception to the Safeguards Rule

The FTC does set aside an exception for small businesses who maintain “customer information concerning fewer than 5,000 consumers.” (eCFR :: 16 CFR 314.6 -- Exceptions.)

3. How to Comply

Ah yes, the fun part of this, right? There are nine steps for IT departments to develop a written, formalized plan in order to comply. The FTC defines this plan—what they call a "reasonable information security program"—as "the administrative, technical, or physical safeguards you use to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information."

Each of these nine steps cover three core concepts:

- **Security and confidentiality** of customer information
- **Protection** against "potential and anticipated threats or risks to the security or integrity of customer information"
- **Protection** against unauthorized access to customer information that could result in "substantial harm or inconvenience to any customer"

If as a consumer, you've ever had to deal with a data breach or stolen information, you'll understand the thoroughness of these requirements. While extensive, they can also be viewed as an opportunity. You or your company's IT department can lean on this ruling to:

- Help your organization shift to a more proactive security approach
- Make a stronger case to executives, ownership, and your board for strategic IT investments
- Use requirements for firmer and more structured budgeting
- Hold peers and staff accountable
- Help educate the company on the necessity of moving to a supply-chain wide security mindset

And of course, the requirement to formalize and execute a program helps proactively set up your organization to avoid security breaches and their consequences, including fines, legal fees, bad publicity, and more.

4. Nine Steps to Compliance

Designate a Qualified Individual to Own the Program 314.4(a)

This new change represents an increase in responsibility for this role from "coordination" to full responsibility and ownership.

Now, the FTC requires that a qualified individual—such as a Chief Information Security Officer (CISO) or Chief Technology Officer (CTO)—owns this program. Ownership includes overseeing, executing, and enforcing security.

The FTC's goal was to maintain a flexibility in these requirements, while still increasing the levels of safeguards and protections. Some of this flexibility can be seen here: this role can be fulfilled either in-house or through a service provider. For example, the FTC also allows for a company's CFO or Finance Director to oversee this program through a partnership with your MSP.

Write and Exercise a Risk Assessment Plan 314.4(b)(1)

Before you can have a plan, you have to first know what information you have and where it's stored. Each affected business must complete an inventory of your customer information, then write a risk assessment plan that includes criteria to identify, evaluate, and manage internal and external security risks—and then carry out periodic risk assessments accordingly.

Your plan must be documented. It should cover what's known as the "CIA Triad": the confidentiality, integrity, and availability of consumer information, as it could lead to data breaches, misuse, or alterations. Your assessments should examine the safeguards that are in place to control these risks, requirements for identifying and mitigating risks, as well as criteria for accepting certain risks deemed as manageable for the current time-being.

And, because these risks are constantly evolving, your plan should take into consideration how you'll stay on top of new and emerging risks.

Once You've Identified the Risks, Implement Safeguards to Control Them 314.4

This is also pretty logical: once you've identified the risks through your risk assessments, you must implement safeguards to control them (unless they've been identified as reasonably manageable).

Risk assessments produce insights for managing risks with policies and procedures, including physical and technical access controls.

These controls and safeguards should cover:

- **Authenticating, managing, and limiting access -** Who has regular access to your customer information? This safeguard also represents a new update to the FTC's definition of an "authorized user". According to their new definition, this means "any employee, contractor, agent, customer, or another person that is authorized to access any of your information systems or data".
- **Identifying and managing data, personnel, devices, systems, and facilities -** "Know what you have and where you have it." Do you, for example, keep an asset inventory of all employees, devices, platforms, etc.? Where is customer information collected, stored, and transmitted? Are you currently on top of your organization's shadow IT?
- **Encrypting all customer information you're storing or transmitting –** Ding, ding, ding, it's another updated definition. Under the new rule, "encryption" means "the transformation of data into a form that results in a low probability of assigning meaning without the use of a protective process or key, consistent with current cryptographic standards and accompanied by appropriate safeguards for cryptographic key material."
- **Implementing Multi-Factor Authentication for anyone accessing consumer information -** Again, another updated definition. Under the new Safeguards Rule, the FTC defines multi-factor authentication as: "authentication through verification of at least two of the following types of authentication factors: (1) Knowledge factors, such as a password; (2) Possession factors, such as a token; or (3) Inherence factors, such as biometric characteristics."
- **Assessing the security of any in-house developed or third-party apps** that are used for transmitting, accessing, or storing customer information/consumer data. With so many apps and SaaS platforms in use, this one is critical to understand.
- **Creating procedures for, following timelines for, and ensuring the secure disposal of customer information. -** The FTC requires disposal to occur "no later than two years after your most recent use of it to serve the customer. The only exceptions: if you have a legitimate business need or legal requirement to hold on to it, or if targeted disposal isn't feasible because of the way the information is maintained."
- **Anticipating change and preparing for it –** Change is the only constant, right? The FTC knows this too, so they're requiring you to be on top of the ever-moving target of cybersecurity. You'll need to develop procedures and document best practices for change management.
- **Rolling out policies, procedures, and controls to monitor and log** the activity of authorized user activity and detect unauthorized access, use, or tampering.

Monitor and Test the Effectiveness of Your Safeguards Regularly 314.4(d)(2)

Monitoring and testing should be done frequently and regularly, looking for any attacks, real or attempted. Testing of your information systems can be done through ongoing monitoring. If continuous monitoring isn't implemented, then you're required to perform both annual penetration testing and vulnerability assessments—which include "system-wide scans every six months designed to test for publicly-known security vulnerabilities."

Another new definition that applies here is the FTC's update to "Penetration Testing", which under the Safeguards Rule "means a test methodology in which assessors attempt to circumvent or defeat the security features of an information system by attempting penetration of databases or controls from outside or inside your information systems."

Train Staff Regularly on Cybersecurity Awareness 314.4(3)

You can have the best policies in place, but if your employees are not aware of what cybersecurity looks like currently, your policy is bound to fail. Frequent and engaging training can help bring staff on board though, and help them spot potential issues, scams, and breach attempts. By keeping your employees' needs at the heart of your policy and training, you'll ensure better buy-in too. You should also make a point of specialized training for those employees who are authorized to handle sensitive consumer data.

Monitor Your Service Providers (Third-Party Risk Management) 314.4(f)(3)

Third-party service providers have become a key target for cyberscammers, who often will breach a service provider's system in order to gain access to a larger or more valuable system. When selecting your service providers, take steps—including contractually—to ensure they have the appropriate skills, experience, and ability to maintain appropriate safeguards.

You are now also required to periodically access their risks and safeguards, just as you are periodically assessing your own.

Regularly Evaluate and Adjust IT Security Safeguards 314.4(g)

We certainly don't need to tell you that technology and the internet are constantly changing, as are the skills of cybercriminals. Your business operations are likely constantly evolving as well. The FTC requires you to evaluate and adjust your information security program on a regular, ongoing basis to stay on top of new and emerging threats, new employees, new equipment, and new customers.

Creating a Written Incident Response Plan 314.4(h)

As the FTC puts it, every business needs a "What If?" plan. In the case of a security event or incidence, a plan gives you the confidence to take action quickly and while this is now a requirement for compliance, having one also communicates your integrity and level of preparation to your customers and partners.

To respond and recover quickly, the FTC recommends an incident response plan that addresses the following areas:

#1 "The goals of the incident response plan."

#2 "The internal processes for responding to a security event."

#3 "The definition of clear roles, responsibilities, and levels of decision-making authority."

#4 "External and internal communications and information sharing."

#5 "Identification of requirements for the remediation of any identified weaknesses in information systems and associated controls."

#6 "Documentation and reporting regarding security events and related incident response activities."

#7 "The evaluation and revision necessary for the incident response plan following a security event."

Program Owner Must Report Annually to Boards of Governors 314.4(I)

Whomever is your designated program owner (your CISO, vCISO, CIO, vCIO, CFO, or another qualified individual), they must deliver written annual reports on your security program to the board of directors or equivalent governing body. If you're working with a Managed Service Provider like Entech, they can also help you prepare an effective board report.

This documentation should include the program's status, compliance, incident updates, violations, and change recommendations.

5. Quick Steps to Start Your Compliance Journey Now

The deadline to be compliant with the new FTC Safeguards Rule is June 9, 2023—which is fast-approaching.

Start with an Expert Assessment to Get the Information You Need to Be Compliant in Time

Compliance with the new FTC Safeguards Rule is mission-critical for your business, both from a regulatory standpoint and as a part of your proactive security program. Even if you have an in-house IT person you love (maybe it's you!) or a third-party IT partner, you need an expert on this ruling to accurately and thoroughly perform an annual or biannual assessment, starting now.

Performed well and to the FTC's required standards, this assessment is also your first step to compliance. Remember, you can't write a plan or execute your safeguards until you know what customer information you have and where you have it. This assessment will set you up with the information you need to then carry out the remainder of the program.

Your in-house appointed program coordinator, such as your CFO, can also partner with your MSP on program ownership to take care of the remaining compliance requirements, avoid fines and penalties, and—most importantly—protect your customer's information.

More Helpful Resources:

- Need help writing your required Incident Response Plan? Download entech's Free Incident Response Plan Template specifically designed to walk through each point that should be included in an incident response plan. Our free template is easily customizable to your business.
- Schedule a Free FTC-Compliant Desktop Audit with entech to give you a quick idea of where you're starting from.

Entech is a leading Managed Technology & Cybersecurity Service Provider serving Fort Myers, Naples, Sarasota, Bradenton, and Tampa Bay. Priding itself on exceptional customer service, Entech unites people, process, and technology to keep companies on the move and data as secure as it is flexible.

At its core, Entech is a family business that's been doing what matters for more than two decades. We are passionate about partnerships, fanatical about fast IT support, and unwaveringly committed to results.

As far as IT providers go, we know we're the best of the best. The cream of the crop. So give us a call or drop us a line about how to get started with FTC Safeguards Rule compliance. You're guaranteed to receive a fast response from the Entech team.

CONNECT WITH ENTECH NOW

entech

(239) 230-0282 | entechUS.com