INTELLIGENT TECHNICAL SOLUTIONS

eBook

THE ULTIMATE GUIDE TO THE FTC SAFEGUARDS RULE

12 MINUTE READ

Thousands of US businesses are in for a challenging 2023 due to changes to the Federal Trade Commission's Safeguards Rule. The amendments can potentially cause serious consequences, imposing new requirements and harsher penalties for non-compliance.

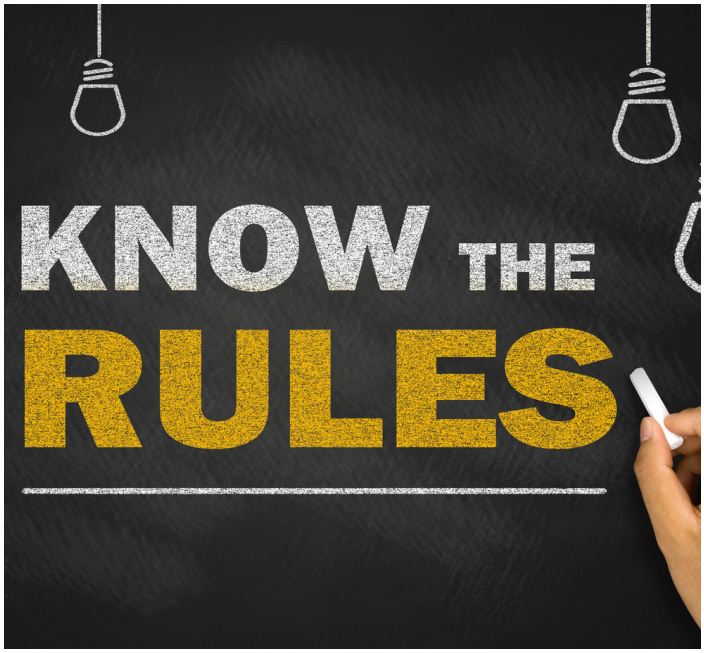
Is your organization ready to navigate the new regulations?

If not, downloading this eBook is a step in the right direction. Intelligent Technical Solutions (ITS) has been closely following the FTC Safeguards Rule amendments so we can help our clients with compliance.

In this guide, we'll discuss everything your organization needs to know about the rule change, like how it will impact you and what steps you need to take. After reading, you will be able to navigate the obstacles to help your business achieve compliance.

INTELLIGENT TECHNICAL SOLUTIONS

TABLE OF CONTENTS



1 WHAT IS THE FEDERAL TRADE COMMISSION SAFEGUARDS RULE?

2 PARADIGM SHIFT: WHY THE FTC CHANGED THE RULES

3 WHO'S COVERED BY THE SAFEGUARD RULE?

4 KEY RULE CHANGES YOUR BUSINESS SHOULD KNOW

5 BEYOND FINES AND REPUTATIONAL DAMAGE: PENALTIES FOR NON-COMPLIANCE

6 WHAT SHOULD YOU DO NEXT?

7 HOW INTELLIGENT TECHNICAL SOLUTIONS CAN HELP

CHAPTER 1:
WHAT IS THE FEDERAL TRADE COMMISSION (FTC) SAFEGUARDS RULE?

The US Congress passed the Gramm-Leach-Bliley Act (GBLA) in 1999. That move helped establish the 2002 Safeguards Rule, which gave the FTC enhanced regulatory powers. It all led to new requirements for financial institutions, including developing, implementing, and maintaining an information security program to prevent unauthorized access to sensitive customer information.

The original rule was highly flexible and relied on an honor system, which according to security experts, proved ineffective. "Sometimes that works. A lot of times, it doesn't. And I think the past 23 years have proven that the honor system does not work," said ITS Partner Ed Griffin.

After the pandemic saw an astronomical rise in cyber incidents, however, regulators finally realized that the Safeguards Rule was in dire need of an update.

CHAPTER 2:
PARADIGM SHIFT: WHY THE FTC CHANGED THE RULES

After a record-breaking number of cyber-attacks were recorded in 2020 and 2021, a significant change to the Safeguards Rule became the most logical step for the FTC to take. In response, they decided to add new technical requirements that will mandate organizations to conform to higher cybersecurity standards. In addition, the FTC broadened the definition of a financial institution in 2023 to include even more businesses.

Previously, "financial institution" was defined as any US company significantly engaged in financial activities. That all changed under the amended Safeguards Rule, as the new definition now includes any organization incidental to such financial activities. The FTC explains that this modification is intended to bring “finders”— companies that bring together buyers and sellers of a product or service — within the scope of the Safeguards Rule.

In short, you are subject to the Safeguards Rule if your organization:

- Handles big money
- Extends lines of credit or loans
- Connects consumers with financial institutions
- Is involved with others' ability to access capital.

CHAPTER 3:
WHO'S COVERED BY THE NEW SAFEGUARDS RULE?

Many non-financial institutions now fall right into that broader definition, many of which are not prepared to meet the steep security requirements.

Some of the non-financial institutions affected include:

- Auto Dealerships
- Mortgage Brokers
- Wire Transferors
- Mortgage Lenders
- Credit Counselors
- Investment Advisors (Not Registered with SEC)
- Entities Acting as Finders
- Check Printers
- Finance Career Counselor
- Account Services
- Travel Agencies
- Payday Lenders
- Financial Advisors
- Retailers with a Credit Card
- Home Appraisers
- Check Cashers
- Estate Settlement Planner
- Collection Agencies
- Finance Companies
- Non-Fed Insured Credit Unions

CHAPTER 4:
KEY RULE CHANGES YOUR BUSINESS SHOULD KNOW

There are several measures and solutions you should be aware of if you want to comply with the new Safeguards Rule. Review some of the most important ones below:

Multi-Factor Authentication (MFA)

You need to implement MFA on all systems containing customers' non-public information, including phone numbers, addresses, dates of birth, etc.

Data Encryption

All customer information needs to be encrypted both in transit and at rest. To do that, you will need to implement data encryption solutions on all devices, email accounts, and datasets containing private information.

Risk Assessment

You will also need a written risk assessment that details the risk criteria of your organization's information security program. It should include how your organization will address and mitigate those risks as well.

Incident Response Plan

The new rule will also require a written incident response plan. That is a predetermined set of instructions or procedures that you will have to go through in case of a security incident or a breach. Your plan should aim to detect, respond to, and limit the consequences of a malicious cyber-attack against your organization's information systems.

Change Management Procedures

Your business will also need a way to modify system configurations and settings. Change Management Procedures can help you do that. In addition, it's a system that helps track any changes made in your network.

Security Officer

The amended rule requires organizations to designate a single "qualified" individual to oversee the information security program. It's important to note, however, that this person could be chosen internally by your organization or a trusted third-party service provider.

Asset Management Program

Your business also needs to set up an asset management program that will track all your devices, data, personnel, systems, and facilities.

Management System for Policies and Procedures

Organizations must implement a management system that will log, track and monitor policies, procedures, and other technical controls.

Regular Information Systems Monitoring

Continuous monitoring of information systems needs to be in place, as well as an annual penetration test and twice-yearly vulnerability assessment.

Annual Reports to Senior Leadership

The designated security officer will be responsible for creating and presenting annual reports to your company's board of directors and other senior leadership. The reports will detail the current compliance status of your company.

Third-Party Vendor Audit

The new rule will require you to audit third-party vendors that have access to non-public customer data. They will have to comply with the same compliance rules. Otherwise, you might get penalized in the event of an audit or a breach.

CHAPTER 5:
BEYOND FINES AND PENALTIES: WHAT HAPPENS WHEN YOU DON'T COMPLY

Non-compliance with the new Safeguards Rule comes with some serious penalties and hefty fines. The FTC can potentially charge your business with extensive injunctive relief that could impede your operations or impose fines costing tens of thousands of dollars per violation.

Worse, that's not even the extent of what non-compliance can bring. It also goes beyond fines and penalties. It could jeopardize your business as there may be potential liability for deceptive trade practices, which could lead to litigation in the event of a security breach. You will also have to notify victims after a breach, increasing the chances that your business might be sued after an event.

Finally, there is a risk that banks will not buy your paper in the future, which will severely limit your ability to transact.

CHAPTER 6:
WHAT SHOULD YOU DO NEXT?

It can be overwhelming. There's simply too much to keep track of. So, to help you organize your compliance plan, you can check out our FTC Safeguards Rule Checklist below:

Getting Started on Compliance

- [ ] Seek help from an expert to start building your compliance plan
- [ ] Designate a single qualified individual to oversee the program
- [ ] Conduct risk assessments on data security infrastructure and existing safeguards

Implementing Mandatory Systems

- [ ] Access controls and encryption on all customer information
- [ ] Multi-factor authentication on all systems containing private customer info
- [ ] Implement continuous monitoring and log retention systems
- [ ] Conduct regular cybersecurity awareness training

Regular Control Testing and Monitoring

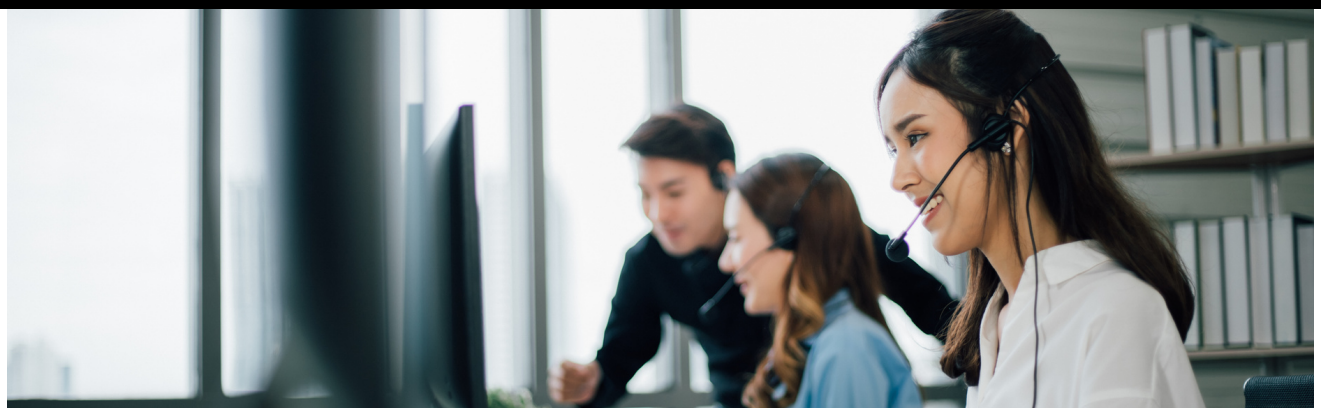
- [ ] Conduct annual penetration testing and bi-annual vulnerability scans

Vendor Auditing

- [ ] Ensure affiliates and third-party vendors comply with the rule

Documentation and Reporting to Senior Leadership

- [ ] Create a written system inventory
- [ ] Draft a written information security program and a written incident response plan



CHAPTER 7:
HOW CAN INTELLIGENT TECHNICAL SOLUTIONS (ITS) HELP?

There's a lot of things you need to implement, address and keep track of to comply with the amended Safeguards Rule. Without proper guidance, you could face complex challenges that could derail your efforts.

ITS can help break it all down for you, tell you exactly where your company stands, and discuss how we can get your business into compliance. We can help you develop a roadmap so you can navigate the obstacles, so you move forward with your compliance plan more smoothly.

In addition, we offer many of the advanced security solutions and measures mandated by the new Safeguards Rule. That way, we can help our clients set everything up effectively.

Reach out to us by scheduling a meeting with our experts to learn how we can help you achieve your compliance goals.

> Ready or not, the FTC Safeguards Rule is coming. [Businesses] have an opportunity to ride the impending wave or potentially get crushed by it. Those with clear-eyed awareness will navigate these changes successfully and lead [their] industry forward.
>
> -Rob Schenk, Chief Experience Officer, ITS

FREQUENTLY ASKED QUESTIONS ABOUT THE NEW SAFEGUARDS RULE:

Are there any exceptions to the new rule?

The amended rules do not apply to organizations that maintain 5,000 or fewer customer records. However, you should still consult with your IT services provider to ensure you are exempt from the rule changes.

How expensive will this be for my business?

That depends on what cybersecurity solutions your organization already has in place. However, since the new requirements are extensive, that means it has the potential to add high costs to those who have yet to implement necessary security measures.

How do I make sure everything is set up by the deadline?

The best way to meet the requirements is to seek help from experts who will be able to guide you through the process with a clear roadmap. You will also need to commit to your compliance plan and ensure that everything is in proper working order.

THE ULTIMATE GUIDE TO THE FTC SAFEGUARDS RULE

ABOUT INTELLIGENT TECHNICAL SOLUTIONS (ITS)

Intelligent Technical Solutions (ITS) is a managed security service provider offering federal-grade cybersecurity to businesses across the country. The company was founded in 2003 and has helped countless businesses meet their current and future goals through technology. ITS has also received a number of accolades and recognition throughout the years. Most recently, the company has been included in MSSP Alert's Top 250 MSSPs.

FURTHER READING:

- What is FTC Safeguards Rule and What Does it Mean for Your Business?
- Can an MSP Help You with Regulatory Compliance?
- What Businesses Need to Know About Managed Cybersecurity Services
- What You Need to Know About the New FTC Safeguards Deadline Extension