TIP SHEET:

NEW FTC SAFEGUARDS RULE CHECKLIST

CLEARTECHGROUP
IT Solutions for Business

Understanding the New FTC Safeguards Rule for 2023

If you think cybersecurity is just for tech companies or Fortune 500 giants, think again! In an increasingly digital world, the security and protection of consumer information have become paramount. To address growing concerns over data breaches and privacy violations, the Federal Trade Commission (FTC) has introduced an updated Safeguards Rule that went into effect on June 9, 2023, and impacts a wide range of organizations. Frankly, with the financial, business, and reputational damage a breach can cause, these are best practices that every organization should consider implementing regardless of whether they are covered by the new Safeguards Rule. Let's look at the organizations impacted by the rule, and we'll share our FTC Safeguards Rule checklist of what you can do to be compliant.

What is the Updated Safeguards Rule?

The FTC website states that the Safeguards Rule "requires covered companies to develop, implement, and maintain an information security program with administrative, technical, and physical safeguards designed to protect customer information." While initially established under Gramm-Leach-Bliley Act (GLBA), the rule has undergone significant revisions to align with the evolving threat landscape and technological advancements.

The updated Safeguards Rule that goes into effect in 2023 places a stronger emphasis on risk assessment, implementation of data protection measures, and incident response planning. It requires covered entities to develop a comprehensive information security program that takes into account the size and complexity of their operations, as well as the sensitivity of the consumer information they handle. This may feel complex, but we'll provide a simplified FTC Safeguards Rule checklist that simplifies things later in this blog.

FTC Safeguards Rule Checklist

To achieve compliance with the new FTC Safeguards Rule, organizations must establish an effective and robust information security program. The FTC states, **"Your information security program must be written and it must be appropriate to the size and complexity of your business, the nature and scope of your activities, and the sensitivity of the information at issue."** Here's a checklist of the main requirements, but as we just noted, there is some leeway for interpretation based on the size and complexity of your organization:

- ☑ **Designate a "qualified individual" to lead your cybersecurity program**. The best choices for a "qualified individual" are a

What Types of Organization Must Comply with the Updated FTC Safeguards Rule?

The new Safeguards Rule applies to a broad range of organizations that handle consumer data. This can include:

- Mortgage lenders & brokers
- Personal property/real estate appraisers
- Travel agencies in connection with financial services
- Investment advisors not required to register with the SEC
- Accountants
- Account servicers
- Automobile dealerships
- Tax preparation firms
- Credit counselors
- Retailers that issue their own credit cards
- Non-federally insured credit unions
- Wire transferors
- Collection agencies
- Payday lender
-

However, covered organizations with less than 5,000 customer records are allowed to skip a few of the requirements.

CISO, virtual CISO, or a skilled MSP. The FTC Safeguards rule requires your "qualified individual" to report to your Board of Directors (BOD) at least annually (some organizations are exempt from the BOD reporting requirement). Most SMBs cannot afford or find a CISO (they are expensive and in short supply), but you can get the same expertise from a fractional vCISO and only pay for the hours you need. A CISO or vCISO can help your organization meet all the requirements in this FTC Safeguards Rule checklist, including assessing your current security measures, identifying vulnerabilities, implementing robust safeguards, and developing an incident response plan. Their expertise ensures that your organization stays compliant and avoids costly penalties.

- ☑ **Risk assessment:** Conduct a thorough assessment of the organization's information systems, identifying potential vulnerabilities and threats to consumer data. This evaluation will help determine the appropriate safeguards and controls to implement.
- ☑ **Design and implement safeguards**: Develop and implement a comprehensive information security program that addresses the identified risks. This may include (varying by the size of your customer records) specific measures such as encryption, MFA, access controls, data, software and app asset inventory, secure network infrastructure, employee training, and regular security audits.
- ☑ **Incident response plan:** Establish an incident response plan that outlines the steps to be taken in the event of a data breach or security incident. This plan should include procedures for containing and mitigating the impact of the breach, notifying affected individuals, and coordinating with law enforcement and regulatory authorities.
- ☑ **Oversight of service providers:** Ensure that any service providers or third-party vendors who handle consumer information adhere to the same rigorous security standards. Contracts with service providers should include provisions requiring them to maintain appropriate safeguards and provide prompt notification of any security incidents.
- ☑ **Employee training and management:** Train employees on security best practices and their responsibilities in protecting consumer data. Regularly monitor and enforce compliance with established policies and procedures. This includes implementing access controls, conducting background checks, and regularly reviewing user access privileges.
- ☑ **Ongoing evaluation and adjustments:** Continuously monitor and evaluate the effectiveness of the information security program. Regularly review and update policies and procedures to address emerging threats and changes in the organization's operations.

FTC Offers Exemptions

The FTC offers exemptions for covered organizations with fewer than 5,000 consumer records. These organizations do NOT have to comply with the following provisions:

- Written risk assessment
- Incident response plan
- Annual reporting to the Board of Directors

Next Steps

The new FTC Safeguards Rule places increased responsibility on organizations to protect consumer data and respond effectively to data breaches. We strongly recommend that every impacted organization start with qualified cybersecurity leadership to help you ensure compliance, provide current guidance on the constantly evolving cybersecurity threats, and keep your organization and data safe.

We hope you found this information helpful! Please contact us for a **Free Security Assessment** or if you need managed IT service, Microsoft or cloud support, vCISO services, and more. Our expert team can provide customized IT solutions to fit your organization's needs.

