CPA Firm's Guide to
FTC Safeguards Rule

PREPARED FOR:

ADDITIONAL RESOURCES:

SHIELDITNETWORKS.COM/FTC-DEADLINE

VERSION
041123

FTC who?

The Federal Trade Commission "FTC" is a US agency that protects consumers and promotes competition in the marketplace. CPA firms, which provide financial services, may be subject to FTC regulations, such as those related to deceptive or unfair practices and data privacy and security. The FTC enforces regulations to ensure compliance and protect consumers.

What's Important About These New Rules?

The original FTC Safeguards rule was implemented in 2003 under the Gramm-Leach-Bliley Act (GLBA) - this was created to protect consumers' sensitive financial information and ensure businesses have proper data security measures in place.

In July 2021, the FTC passed a new set of rules with a compliance deadline of June 2023. These new rules were aimed to update and expand the existing requirements to address changes in technology and data privacy risks

My CPA Firm Doesn't Fall Under This...

We hate to break it to you, but it does. We'll pop up a link to the official language at the end of this guide, but to summarize:

> The FTC Safeguards rule applies to CPA firms that are considered "financial institutions" under the Gramm-Leach-Bliley Act (GLBA), which includes firms that provide financial services such as tax preparation, financial planning, or other services.

How Will the FTC Enforce These Rules?

The FTC enforces its rules through investigations, enforcement actions, and penalties. It may launch an investigation if it suspects noncompliance and can take enforcement action if it finds evidence of violations

Can I Get a Breakdown of These Rules?

The FTC Safeguards Rule outlines nine key elements that CPA Firms must include in their security plan to protect consumer data and to meet compliance requirements:

1.) Designated Responsible Individual or Party

CPA firms must designate one or more individuals to oversee the information security program, which could include a CSO or an IT manager. This individual is responsible for ensuring that the security program is operating effectively and that the firm is complying with the FTC Safeguards Rule.

2.) Perform Risk Assessments

CPA firms must conduct a risk assessment to identify and evaluate potential risks to consumer data. This includes identifying the types of data collected, how it is used and shared, and the potential risks to its confidentiality, integrity, and availability.

3.) Implement Reasonable Safeguards

CPA firms must implement reasonable safeguards to control the risks identified in the risk assessment. This could include implementing access controls, encrypting data, and monitoring systems for unauthorized access.

4.) Regular Testing and Monitoring

CPA firms must regularly test or monitor the effectiveness of the security program, including the safeguards implemented and the response plan.

5.) Develop an Incident Response Plan

CPA firms must develop and implement an incident response plan to address security incidents and mitigate any damage. This plan should include procedures for reporting incidents, identifying the scope of the breach, and notifying affected consumers and regulatory authorities.

cont'd →

6.) Service Provider Oversight

CPA firms must oversee the service providers with access to consumer data to ensure that they also have appropriate data security measures in place.

7.) Written Policies & Procedures

CPA firms must have written policies and procedures that outline the information security program and the responsibilities of employees.

8.) Employee Training

CPA firms must train employees on the information security program, including policies and procedures, and how to identify and respond to security incidents.

9.) Program Adjustments

CPA firms must oversee the information security program and make adjustments and updates as needed to ensure its continued effectiveness. This includes regularly reviewing and updating policies and procedures and assessing the risks to consumer data.

Satisfy These Requirements With our vCSO Program...

Our team of experienced cybersecurity professionals can provide guidance and support in implementing each of the nine elements of the rule, including conducting a risk assessment, implementing reasonable safeguards, and developing an incident response plan. Our vCSO Program also includes regular testing and monitoring services to ensure that the security program is operating effectively and that any vulnerabilities are identified and addressed.

- **Regular Monitoring**
- **Written Policies**
- **Responsible Party**
- **Incident Response**
- **Employee Training**
- **Risk Assessments**
- **Vendor Oversight**
- **Program Adjusting**
- **Implement Safeguards**

Why Choose a Virtual CSO?

Our vCSO program was developed to help CPA firms bypass the challenges that typically hold their organization back from implementing and maintaining a solid cybersecurity stack -- including the difficulties of sourcing talent, training, and high-turnover of an internal executive security position (CISO, CSO)

Our vCSO program provides CPA firms with the expertise, solutions, and support they need to comply with the FTC Safeguards Rule while also keeping their clients' data secure.

How To Get Started...

The first step is to schedule a high-level executive discovery call, for CalCPA Members only, you will be able to book directly with our CEO, Scott Hagizadegan.

During this consultation, we will discuss the specific needs and requirements of your firm, current security measures you already have in place, answer any questions, and provide a high-level overview of our vCSO program.

SHIELDITNETWORKS.COM/FTC-DEADLINE

EXCLUSIVE CALCPA MEMBER OFFER

Complimentary Risk Assessment

As an official partner of CalCPA, we are pleased to offer all active members a complimentary risk assessment, a critical requirement under the new FTC Safeguards Rule. This assessment, valued at over $8,000 per analysis for non-members, will identify vulnerabilities, compromises, and weaknesses in your organization's defenses.

To take advantage of this exclusive offer, simply schedule a high-level executive discovery call where we will verify your CalCPA membership and discuss your organization's unique needs.

SHIELDITNETWORKS.COM/FTC-DEADLINE