Is Your Data Security FTC Compliant?

Safeguard Comply

FTC SAFEGUARDS GUIDE

What are FTC Safeguard Rules?

In June 2023, the Federal Trade Commission put new standards in place for any non-banking entity that handles customer financial data.

Think mortgage brokers, CPA firms, registered investment advisors and car dealerships, for example. In an era when data breaches make headlines regularly, it's critical for a business to protect a customer's private data not only from a service perspective but also from a legal perspective.

If there is a data breach at your business and customer data is released, after the fact the FTC can refer your business for criminal prosecution.

The standards outline nine elements for businesses to develop and implement their plans.

The following pages outline each of the nine steps to create a plan to be in compliance.

The Federal Trade Commission Safeguard rule outlines nine specific steps to create a compliance plan. If your company encounters a data breach, this plan is critical to communications, security and reporting.

1 Designate an individual who is in charge.

Decide who the business' point person is for planning, implementing and overseeing the data protection plan. This person owns the plan, processes, management, analysis and reporting.

2 Do a risk assessment.

Consider internal and external risks to the security, confidentiality, and integrity of customer information. For firms with information pertaining of 5,000 or more customers, the risk assessment and mitigation plan must be in writing. We say it's a good idea, no matter the size of the business, to have a plan in writing.

Outline safeguards.

3

Review the risks outlined and discuss how they can be mitigated on a day-to-day basis. This is a list that could be used as part of a company's safeguard planning conversation. Review, discuss and document:

- Password strength requirements and company policies
- Inactivity locks on device screens
- Electronic file storage systems along with onsite cabinets and rooms that store data
- Encryption systems for data that is transmitted electronically
- Monitoring inbound and outbound transfers of data and access
- Shredding and disposal policies for documents and computer hardware
- Software updates and virus protection
- Firewalls
- Removal of terminated employee access to systems
- Data access, use, and transportation when working remotely
- Access to data on public networks
- Policies to verify identification for information requests from customers or third parties
- Rules regarding nonmonitored personal devices for accessing customer information
- Access by cleaning and building maintenance staff or other service providers not under direct contract
- Vendor engagement and monitoring

4 Testing and monitoring.

The rule calls for testing every six months, whenever there are “material changes” to operations or if there’s reason to know there has been a “material impact” on information.

5 Staff training and auditing.

If staff isn’t aware of the safeguards and testing system, how can they follow the rules to keep a customer’s data safe? Explaining the program, the importance of compliance and its implications if the rules aren’t followed provides a foundation for safeguard adherence.

6 Assess service providers.

Many businesses have outsourced service providers that support IT systems. These providers should be partners as it relates to these safeguards, your written plan and its execution. Trust is critical, so periodically assess your service provider to ensure they’re in compliance.

7 Continuous improvement.

A safeguards plan should not sit on a shelf in perpetuity. It needs regular review to identify potential gaps and updated to provide policy how to bridge those gaps as part of the mitigation plan.

8 Crisis plan.

If an incident would happen, how would you respond? Outline internal and external processes for the response, with clearly defined roles and responsibilities. This plan should be reviewed and updated regularly as part of the continuous improvement program.

9 Internal reporting

Annually, a report should be written and provided to leadership to outline the status of the program’s identified risks and mitigation.

Get a free consultation.

Web: www.SafeguardComply.com
Email: info@SafeguardComply.com

Indiana
Phone: 317.762.2294
15 S. Main Street
Zionsville, IN 46077

Safeguard Comply