FTC Safeguards Rule

What Your Business Needs to Know

FTC Safeguards Rule Overview

What is it?

A rule requiring financial institutions to take specific steps to protect customer information

Deadline

Must comply by 6/9/23

Penalties

Up to $100,000/violation of non-compliance

Who needs to comply with the Safeguards Rule?

An institution that is significantly engaged in financial activities, or significantly engaged in activities incidental to such financial activities, is a financial institution.

Examples include mortgage lenders, payday lenders, finance companies, mortgage brokers, account servicers, check cashers, wire transferors, collection agencies, credit counselors and other financial advisors, tax preparation firms, non-federally insured credit unions, and investment advisors that aren't required to register with the SEC.

What does the Safeguards Rule require companies to do?

Develop, implement, and maintain an information security program with administrative, technical, and physical safeguards designed to protect customer information.

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.

What does a reasonable information security program look like?

Section 314.4 of the Safeguards Rule identifies nine elements that your company's information security program must include.

1 **Designate a Qualified Individual** to implement and supervise your company's information security program (can be a service provider).

2 **Conduct a written risk assessment.**

3 **Design and implement safeguards** to control the risks identified through your risk assessment. [Details]

4 **Regularly monitor and test the effectiveness of your safeguards** through continuous monitoring of your system. If you don't implement that, you must conduct annual penetration testing, as well as vulnerability assessments, including system-wide scans every six months designed to test for publicly-known security vulnerabilities.

5 **Provide your people with security awareness training** and schedule regular refreshers.

6 **Monitor your service providers.** Select service providers with the skills and experience to maintain appropriate safeguards.

7 **Keep your information security program current.**

8 **Create a written incident response plan.**

9 **Require your Qualified Individual to report to your Board of Directors.** If your company doesn't have a Board or its equivalent, the report must go to a senior officer responsible for your information security program.

How TPx Helps

TPx is a leader in cybersecurity for small and medium businesses and public-sector organizations. Our depth of expertise enables us to offer standards-based security consulting services developed from our experiences in solving strategic and operational challenges for customers. All of our offerings are based on the best practices derived from Information Security Standards and our extensive experience deploying, architecting, operating and securing environments nationwide.

Our thorough understanding of security enables us to provide our customers with the confidence that their security program is constructed and executed in alignment with the applicable regulatory framework(s). If you are looking to be compliant with the new FTC Safeguards Rule and need a helping hand, consider TPx.

Foundations of the Safeguards Rule

There are three stages of running an effective security program: Creation, Operation, and Governance. TPx can assist in all of these phases, depending on the current maturity level of your organization's security activities. Our flexible model allows us to provide the support you need in a cost-effective manner, incorporating the in-house resources you already possess.

Creation. Security policies are the bedrock of any security program. Without these policies, no program can be successful. For organizations new to security programs, the development of these documents can be a daunting task. TPx will work with your organization to develop a complete set of foundational policy documentation that will serve as the basis for your program. This set includes nine (9) policy documents, as identified by 16 CFR 314.4(c) of the Safeguards Rule:

- System Security Plan (SSP)
- Access Control Policy
- Asset Management Policy
- Encryption Policy
- Multi-Factor Authentication (MFA) Policy
- Data Retention/Disposal Policy
- Change Management Policy
- Log/Activity Monitoring Policy
- Incident Response Plan

For those also developing software apps in-house, we'll develop another document outlining policies related to the Software Development Life Cycle. Each document will:

- Name the objective of each process included in the policy
- Define the specific control(s) to be deployed to implement each process
- Describe the way in which each control is to be monitored and evaluated for effectiveness

Operation. An effective security program requires discipline and diligence. Any compliance auditor would insist on seeing proof that your organization's policies are being followed properly and thoroughly. Regular review of policy operations ensures this. In this stage, TPx will perform quarterly reviews of aspects of the operations for compliance with the defined policies. This includes reviewing access logs and validating access policies, verifying MFA configuration(s), examining account management (personnel terms/hires/changes) logs, reviewing asset management logs, etc.

Governance. Paragraphs 16 CFR 314.4(g) and 16 CFR 314.4(i) of the Safeguards Rule specifically call for regular written reviews of your security program to your Board of Directors (or equivalent), as well as regular review of your SSP and other documents for changes in your network environment. TPx will perform a quarterly review of the policies and provide an annual readout to your Board stating the health and compliance of your program with the Safeguards Rule.

How TPx Can Help

Security Program Create

The TPx Advisory Services' Security Program Create is designed for an organization that has a qualified cybersecurity employee who can own and monitor a program but does not have the experience or time to create a security program. TPx security experts will create or review and modify the following security documents: Information Security Program, System Security Plan, Access Control Policy, Asset Management Policy, Data Protection Policy, Multi-Factor Authentication, Data Retention Policy, Change Management Policy, Log Monitoring Playbook, Incident Response Policy, Partner Security Policy

Security Program Maintain

Have you already created a security program, and you are confident it meets the requirements of the Safeguards Rule? TPx can verify that the program is and remains current, assist with changes as your business evolves, and report on the program annually. This offering helps an organization maintain the program per the Safeguards Rule requirements. If you don't have anyone ensuring the policies are enforced properly, we advise to choose Maintain & Report Program instead.

How TPx Helps

Security Program Maintain & Report

TPx can help verify that the policies defined in your security program are being put into practice. With periodic reviews of operational activities, the Maintain & Report offering ensures that policies are enforced properly, and that third-party providers are adhering to the agreements you have with them. Quarterly monitoring of security logs and activities provides a documented trail of compliance enforcement that will be crucial in the event of an audit.

Security Program Complete

If your organization doesn't know where to start and doesn't have anyone qualified to own the program, this solution is for you. TPx will do everything in "Security Program Creation" and "Security Program Maintain & Report" to enable a defensible position from day 1. As the owner of your program, TPx will define, create, maintain and report on the program per FTC Safeguards Rule definition.

Best Practice Review

Companies that qualify under FTC Rule must perform an annual Best Practice review of the standard best practices that review an organization's existing security program, policies, and operations, as it relates to nonpublic personal information. Using the industry standard NIST 800 series best practices, TPx security consultants will review and identify areas of compliance, areas of adjustment, and areas of creation needed per the Safeguards Rule. The report from the best practice review will be provided and utilized to be defensible for the Safeguards Rule. The results of the annual Risk Assessment are further used to inform the formation and ongoing oversight of the security program, policies, and processes. It provides a roadmap for program improvements based on a quantitative evaluation of risk across the environment.

Vulnerability and Penetration Scanning

All qualifying organizations must perform an annual Penetration Assessment utilizing "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." TPx can perform a penetration scan of your external environment and provide recommended mitigations to protect nonpublic personal information. Lastly, qualifying organizations must also perform, twice a year, a vulnerability scan of their environment. TPx can perform the scan of your external environment and provide mitigation recommendations for any vulnerabilities. Upon implementing recommended changes, TPx would perform a validation scan to ensure the customer has re-mediated defined risks.

Train Your Staff

Security Awareness Training Raise your staff's security aptitude. With phishing simulation emails and regular training courses, we can cut phishing email click rates by as much as 75%.

Managed Inbox Detection & Response (IDR) Email security filters are not foolproof. Phishing emails can still get through. Equip your staff with a simple tool that helps them determine if the email is a threat or "innocent".For a limited time, you get our Security Awareness Training for free when you get Managed IDR.

TPx Safeguards Rule Solutions

Solutions Overview	Create	Maintain	Maintain & Report	Complete
Risk/gap assessment	■	■	■	■
Policy creation and governance definition[1]	■			■
Create Incident Response Plan	■			■
Security program documented	■			■
Quarterly review		■	■	■
Annual report to the Board		■	■	■
Keep your information security program current		■	■	■
Risk review of service providers[2]		■	■	■
Verify enforcement of policies [3]			■	■
Periodic monitoring of security operations			■	■
Business review		■	■	■

Optional Add-Ons	
Vulnerability & penetration scan (Vuln: 2X yearly; Pen: 1X yearly)	On request[4]
Secure software development lifecycle policy doc (SDLC)	On request
AppSec assessment	On request
Develop incident response plan (included in Create and Complete)	On request[5]
Train your staff (SAT)	$4.50/email per license
Inbox Detection & Response (IDR)	$4.99/email per license

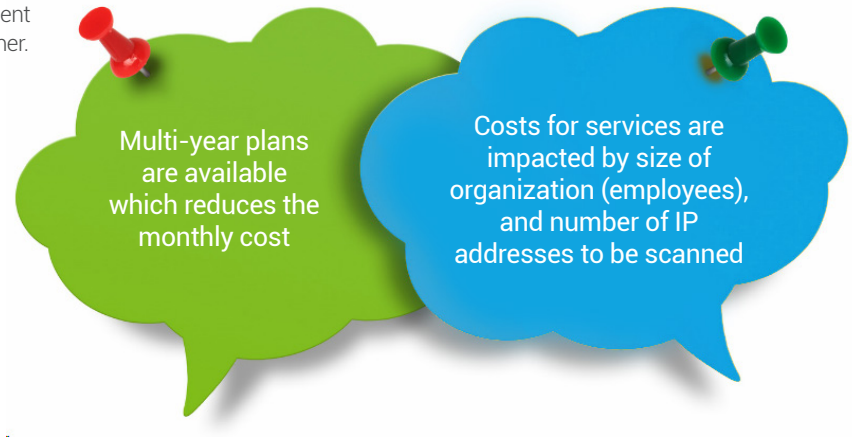
[1] Policies included: System Security Plan, Access Control, Asset Management, Encryption, MFA, Data Retention/Disposal, Change Management, Log / Activity Monitoring, Incident Response Plan.

[2] A review of the T&Cs document that the third-party service provider provided to the customer.

[3] Does not include technical implementation work to deploy or configure controls. For example, TPx will not configure logging for Windows authentication or implement Multi Factor Authentication (MFA) for a customer.

[4] Cost varies based on the number of IPs.

[5] A one-time cost if customer does not have a "Create" or "Complete" plan but needs an incident response plan.



TPx SOLUTIONS OVERVIEW