EBOOK

FTC Safeguards Rule

Compliance Guide for Institutions Engaged in Financial Activities

TPX

EXECUTIVE SUMMARY

The FTC Safeguards Rule requires institutions engaged in significant financial activities to take steps to protect consumer information. The rule has a fast-approaching compliance deadline of June 9, 2023. After this date, companies that are non-compliant can face costly penalties.

This guide explores the compliance requirements in the FTC Safeguards Rule and how organizations can ensure defensibility.

TPx can help companies of all sizes become defensible for the Safeguards Rule by creating, owning and maintaining companies' security programs in alignment with the requirements of the rule. TPx also offers add-on services, such as security awareness training (SAT), inbox detection and response (IDR) and more, so companies can avoid the hassle of managing multiple providers.

IMPORTANT REMINDER

Avoid $100,000 fines by complying by June 9, 2023

Key Takeaways

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

Organizations need to introduce physical and electronic data access controls on non-public personal financial information.

The scope of organizations bound by the FTC Safeguards Rule has expanded to include any organization significantly involved in economic activities.

The FTC can issue several penalties to non-compliant organizations, including fines of up to $100,000 per violation.

Table of Contents

Part 1: What Is the FTC Safeguards Rule?

- How Has the FTC Safeguards Rule Evolved Over Time?
- What Are FTC Safeguards Rule Compliance Requirements?
- What Is the Deadline for Compliance with the FTC Safeguards Rule?

Which Organizations Must Comply with the FTC Safeguards Rule?

- What Are Financial Institutions Bound by the FTC Safeguards Rule?
- What Other Institutions Are Bound by the FTC Safeguards Rule?
- Which Organizations Are Exempt from the FTC Safeguards Rule?

What Are the Consequences of Non-Compliance with the FTC Safeguards Rule?

- Real-world Examples of Penalties for Violation of the FTC Safeguards Rule
- How do Regulatory Organizations Enforce Compliance?

How Can Organizations Ensure Compliance with the FTC Safeguards Rule?

- Create an Information Security Program
- What Is an Information Security Program?
- What Are the Steps for Creating an Information Security Program?

How Does TPx Help Organizations Comply with the FTC Safeguards Rule?

- Running an Effective Security Program
- TPx FTC Safeguards Solutions

Why Choose TPx

- TPx is Your One-Stop Shop for Managed Services

ABOUT TPX

Part 1: What Is the FTC Safeguards Rule?

The Federal Trade Commission (FTC) Safeguards Rule is defined as a rule requiring financial institutions to take specific steps to protect customer information. However, it's not only financial institutions that need to comply. Any institution that is engaged in significant financial activities must comply with the FTC Safeguards Rule.

How Has the FTC Safeguards Rule Evolved Over Time?

In 1999, Congress passed the Gramm-Leach-Bliley Act (GBLA) that established the 2002 Safeguards Rule, which enhanced the regulatory power of the FTC. This move led to new requirements for financial institutions, including developing, implementing and maintaining an information security program to prevent unauthorized access to sensitive customer information.

In 2021, amendments were introduced to the FTC Safeguards Rule to keep pace with ever-changing technology with more precise guidance for businesses on the data security principles they need to adopt. The amendments stipulated that by December 9, 2022, financial institutions must comply with the FTC Safeguards Rule's requirements, outlined on the Code of Federal Regulations website.

Before 2022, "Financial institution" was defined as any U.S. company significantly engaged in financial activities. **Under the new FTC Safeguards Rule, "financial institution" 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.

On November 15, 2022, the FTC announced a delay to the effective date of several provisions of the Safeguards Rule from December 9, 2022, to June 9, 2023, due to supply chain issues and challenges in institutions' ability to meet the requirements for designating "qualified individuals" responsible for implementation.

What Are FTC Safeguards Rule Compliance Requirements?

The FTC Safeguards Rule requires organizations to 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.

There are basic requirements for your cybersecurity as well as data controls. Go to Part 4 of this guide to learn more about the requirements.

What Is the Deadline for Compliance with the FTC Safeguards Rule?

Organizations bound by the FTC Safeguards Rule must comply by June 9, 2023. After this date, companies can face consequences outlined in the Federal Civil Penalties Inflation Adjustment Act Improvements Act of 2015 and in the Federal Register notice.

FTC Amends Safeguards Rule to Require Non-Banking Financial Institutions to Report Data Security Breaches

The amendment announced requires financial institutions to notify the FTC as soon as possible, and no later than 30 days after discovery, of a security breach involving the information of at least 500 consumers.

Such an event requires notification if unencrypted customer information has been acquired without the authorization of the individual to which the information pertains. The notice to the FTC must include certain information about the event, such as the number of consumers affected or potentially affected.

The breach notification requirement becomes effective 180 days after publication of the rule in the Federal Register, which was on October 27, 2023.

PART 2:

Which Organizations Must Comply with the FTC Safeguards Rule?

The FTC Safeguards Rule was originally intended to regulate financial institutions, which, in the original drafting of this rule, meant any organization "significantly engaged in financial activities."

In 2022, a financial institution, according to the FTC's standards, is any organization that is significantly involved in economic activities and "activities incidental to such financial activities." Speaking generally, the FTC Safeguards Rule covers organizations that:

- Handle big money
- Extend lines of credit or loans
- Connect consumers with financial institutions
- Involved with others' ability to access capital

What Are Financial Institutions Bound by the FTC Safeguards Rule?

A financial institution includes the following organizations within the financial services sector:

- Non-Federally-Insured Banks + Credit Unions
- Trust Companies
- Insurance Companies
- Brokerage Firms
- Investment Dealers

A majority of lenders, including banks and federally-insured credit unions already fall under other federal regulations. If you're a mortgage lender that is not already complying with another consumer data privacy rule, then the FTC Safeguards Rule applies.

What Other Institutions Are Bound by the FTC Safeguards Rule?

Other organizations that must comply with the FTC Safeguards Rule include:

Finance Career Counselors	**Wire Transferors**	**Account Services**	**Travel Agencies**
Credit Counselors	**Investment Advisors** (Not Registered with the SEC)	**Entities Acting as Finders**	**Check Printers**
Pay Day Lenders	**Retailers Offering a Credit Card**	**Home Appraisers**	**Check Cashers**
Estate Settlement Planners	**Collection Agencies**	**Auto Dealers**	**Higher Education**

Which Organizations Are Exempt from the FTC Safeguards Rule?

According to the Federal Register, financial institutions that collect information on **less than 5,000 consumers** are exempt from the following requirements:

Written risk assessment

Incident response plan

Annual reporting to the board of directors

PART 3:

What Are the Consequences of Non-Compliance with the FTC Safeguards Rule?

Organizations that fall into non-compliance with the FTC Safeguards Rule could face business disruption, productivity losses, revenue losses, fines, penalties, litigation, reputational harm and more.

EXTENSIVE FINES

The FTC Safeguards Rule authorizes the FTC to impose fines on impacted entities that don't comply. Fines don't apply to first offenses.

The Gramm-Leach-Bliley Act (GLBA) authorizes fines up to $100,000 against non-compliant entities per violation and up to $10,000 against officers and directors in their personal capacities per violation.

Additionally, the FTC can seek damages for consent decree violations, which could total more than $43,000 for each violation.

The FTC is not the only regulatory organization that can enforce the FTC Safeguards Rule. Other regulatory agencies, such as the Consumer Financial Protection Bureau (CFPB) and state banking regulators, also have the authority to enforce the rule and impose penalties for non-compliance.

EXTENSIVE PENALTIES

The FTC can enforce long-term consent decrees or injunctive relief, which may impact business operations or force a company to cease certain activities related to the violation.

LITIGATION RISKS

Organizations can face legal liability for deceptive practices, meaning that they can be sued in the case of a security breach if they're found to be non-compliant with the FTC Safeguards Rule. Litigation risk is also increased if victims of the security breach must be notified.

REPUTATIONAL DAMAGE

Customer, partner, supplier and affiliate trust will be impacted if a security breach occurs and the organization is found non-compliant with the FTC Safeguards Rule.

REGULATORY SCRUTINY

Offending organizations can become subject to probing regulatory audits for years. The FTC may also require the financial institution to implement a compliance program to ensure compliance with the FTC Safeguards Rule in the future. This could include measures such as regular audits, employee training and the development of policies and procedures to protect customer information.

DATA LOSS

A successful cyberattack can put an organization's (and their clients') data in the wrong hands, leaving them a possible victim of ransomware.

IMPRISONMENT DUE TO CRIMINAL NEGLIGENCE

For the worst-case scenarios of non-compliance, key business stakeholders can be imprisoned for criminal negligence. Individuals found in violation can be put in prison for up to five years.

Real-world Examples of Penalties for Violation of the FTC Safeguards Rule

It's important that organizations bound by the FTC Safeguards Rule take compliance seriously as the rule is being actively enforced.

In 2018, Paypal settled allegations with the FTC that its peer-to-peer payment service Venmo engaged in deceptive acts and practices that violated the Gramm-Leach-Bliley Act (GLBA)'s Safeguards Rule and Privacy Rule. Previous infractions in 2016 resulted in PayPal paying more than $175,000 to the State of Texas.

In October 2022, the FTC announced enforcement actions against the online alcohol marketplace Drizly and its CEO over allegations that the company's security failures led to a security breach that exposed personal information of around 2.5 million customers. The FTC order linked here provides specifics on the consequences of this specific case.

How do Regulatory Organizations Enforce Compliance?

Self-assessment

Financial institutions may be required to conduct self-assessments to ensure they're in compliance with the FTC Safeguards Rule. This could include reviewing policies and procedures, conducting risk assessments and testing security controls.

Examination

Regulatory organizations may conduct on-site examinations of financial institutions to assess compliance with the FTC Safeguards Rule. These examinations may include reviewing documents, observing practices, and testing controls.

Audit

Financial institutions may also be required to undergo independent audits to assess compliance with the FTC Safeguards Rule. These audits may be conducted by third-party firms or by the regulatory organizations themselves.

PART 4:

How Can Organizations Ensure Compliance with the FTC Safeguards Rule?

Now that you know the downsides of non-compliance, you're undoubtedly anxious to learn how to become compliant with the FTC Safeguards Rule. It's a multistep and complex process with which TPx can help.

You don't need to go it alone. Regardless of where you are with your security and how much handholding you need, TPx can help.

Here are the key things to know:

Create an Information Security Program

The first step is to create an information security program that is defensible for the FTC Safeguards Rule for your organization.

The FTC directive states: "*You shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue. The information security program shall include the elements set forth in § 314.4 and shall be reasonably designed to achieve the objectives of this part, as set forth in paragraph (b) of this section.*"

What Is an Information Security Program?

FTC defines an Information Security Program as "*the administrative, technical, or physical safeguards you use to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information.*" in the Code of Federal Regulations.

The purpose of an Information Security Program is to:

1. **Protect Customer Information**
2. **Protect Against Anticipated Threats**
3. **Protect Against Unauthorized Access**

What Are the Steps for Creating an Information Security Program?

1 Designate a Qualified Individual, or service provider, to implement and supervise your company's information security program:

According to section 16 CFR 314.4(a) of the FTC Safeguards Rule, "*The Qualified Individual may be employed by you, an affiliate, or a service provider. To the extent the requirement in this paragraph (a) is met using a service provider or an affiliate, you shall:*

(1) Retain responsibility for compliance with this part;

(2) Designate a senior member of your personnel responsible for direction and oversight of the Qualified Individual; and

(3) Require the service provider or affiliate to maintain an information security program that protects you in accordance with the requirements of this part.

HOW TPX CAN HELP

TPx can create, own, and maintain your information security program that aligns with FTC Safeguards Rule requirements.

2 Conduct a written risk assessment.

A written risk assessment includes:

- Criteria for the evaluation and categorization of security risks.
- Assessment of the security, confidentiality and integrity of systems and customer information. Must include the judgment of efficacy of controls.
- Output detailing how risk will be mitigated or accepted.

WHAT IS A RISK ASSESSMENT?

A risk assessment is the combined effort of identifying and analyzing potential events that may negatively impact individuals, assets, and/or the environment; and making judgments "on the tolerability of the risk on the basis of risk analysis" while considering influencing factors.

The FTC states the following: *"Among other things, your risk assessment must be written and must include criteria for evaluating those risks and threats. Think through how customer information could be disclosed without authorization, misused, altered, or destroyed. The risks to information constantly morph and mutate, so the Safeguards Rule requires you to conduct periodic reassessments in light of changes to your operations or the emergence of new threats."*

COMPONENTS OF A RISK ASSESSMENT:

Gap Assessment Analysis

A cybersecurity gap analysis enables organizations to address the areas of weakness within their network and system security controls to ensure that they are effective.

Plus, this ensures compliance with Regulatory Frameworks for companies bound by them.

NIST 800 – 171 (Protecting Controlled Unclassified Information)

HIPAA (Health Insurance Portability and Accountability Act)

PCI DSS (Payment Card Industry Data Security Standard)

Sample Gap Assessment

OVERALL SECURITY PROGRAM SCORE:
2 Developing

SUMMARY
Developing information security requirements, practices, controls and/or documentation that translates into repeatable results

SECURITY DOMAINS	ACCESSOR RATING	TARGET LEVEL	RISK GAP
Access Control	1.4	5	-3.6
Awareness and Training	2.0	5	-3.0
Audit and Accountability	1.3	5	-3.7
Configuration Management	1.7	5	-3.3
Identification and Authentication	1.6	5	-3.4
Incident Response	0.0	5	-5.0
Maintenance	2.0	5	-3.0
Media Protection	2.0	5	-3.0
Personnel Security	0.0	5	-5.0
Physical Protection	2.5	5	-2.5
Risk Assessment	3.0	5	-2.0
Security Assessment	2.3	5	-2.7
System and Communications Protection	2.1	5	-2.9
System and Information Integrity	2.1	5	-2.9
TPx	2.3	5	-2.7
AVERAGE	1.8	5	-3.2

Vulnerability Assessment

A vulnerability assessment is a systematic review of security weaknesses in an information system. The FTC Safeguards Rule requires system-wide scans every six months designed to test for publicly-known security vulnerabilities.

Annual Penetration Scan

A penetration test, also known as a pen test, is a simulated cyberattack against your computer system to check for exploitable vulnerabilities.

Annual penetration testing of your information systems is determined each given year based on relevant identified risks in accordance with the risk assessment.

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.

HOW TPX CAN HELP

TPx can assist any organization with creating a written risk assessment or evaluating their current one to ensure it meets FTC Safeguards Rule requirements.

3 Design and implement safeguards to control the risks identified through your risk assessment.

1. Implement and review technical and physical access controls.
   - Authenticate and permit access only to authorized users.
   - Limit authorized user's access to data to only those needed for their job (principle of least privilege).
2. Inventory systems, people, data and facilities.
3. Encrypt customer information in transit and at rest.
4. Develop software with a secure process.
5. Implement MFA for access to any information system.
6. Define data destruction and retention policy/process:
   - No later than two years after last used
   - Periodically review your policy/process
7. Adopt procedures for change management.
8. Implement policies to monitor/log authorized users and unauthorized users of customer information.

HOW TPX CAN HELP

TPx can conduct your risk assessment and recommend safeguards to put in place in order to satisfy the FTC Safeguards Rule requirements.

4A Regularly monitor and test the effectiveness of your safeguards through continuous monitoring of your system.

According to section 16 CFR 314.4(d)(2) of the FTC Safeguards Rule: *"For information systems, the monitoring and testing shall include continuous monitoring or periodic penetration testing and vulnerability assessments."*

WHAT IS MONITORING?

"Observe and check the progress or quality of (something) over a period of time; keep under systematic review." as defined by Oxford Languages.

WHAT ARE MONITORING REQUIREMENTS?

Monitoring requirements include:

- All activity of authorized and unauthorized users
- Tampering with customer information
- Effectiveness of controls, systems and procedures
- Changes in information systems
- New vulnerabilities in systems
- Operationalize the process, so it's continuous

MONITORING USER ACCESS:

- GLBA Safeguards require you to monitor users' authentication continuously at the operating system, application, cloud and "as-a-service" solutions.
- On individual systems, ensure local logging is happening.
- Use Windows Audit Policy if your computer logs into a network.
- Track system activity in Windows 10, showing access to apps and services.

MONITORING SENSITIVE DATA ACCESS:

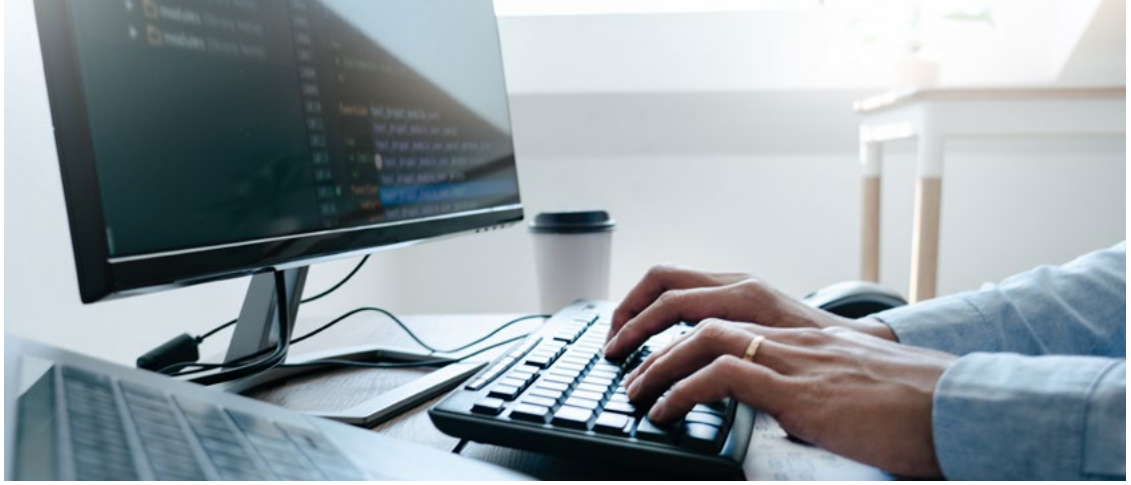
- In addition to monitoring users, you must also monitor the access to data where it resides, such as file servers, databases, applications, backups, etc.
- On individual systems, make sure local logging is happening.
- Use Windows Group Policy to monitor central access policies (if networked).
- Monitor Central Access Policies for file servers access and use.

MONITORING CLOUD DATA AND SYSTEMS:

- Cloud providers and systems have their own means of monitoring user and data access. The same rules apply; you must monitor user and data access continuously.
- The same rules apply if the file server/application server is in the cloud.
- Use Cloud Access Security Broker (CASB) if you have multiple applications in the cloud.
- Cloud Providers have native logging such as, Cloudwatch and Cloudtrail of AWS.

OR (Continued on Page 17)

4B If you don't implement Step 4A above, you must conduct annual penetration testing and vulnerability assessments, including systemwide scans every six months designed to test for publicly-known security vulnerabilities.



COMPONENTS OF PENETRATION TEST:

A penetration test is "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."

PENETRATION TESTS TYPICALLY INCLUDE:

- Annual testing based on relevant risks identified in the risk assessment
- Documented risks through specific execution of attack and access to systems/data
- Examples of enumeration or data acquired
- Third party oversight
- Cost (penetration tests) $10,000-$15,000, per Security Metrics (Don't fret – TPx has more budget-friendly options available!)

COMPONENTS OF VULNERABILITY SCAN:

A vulnerability scan is defined as "…including any systemic scans or reviews of information systems reasonably designed to identify publicly known security vulnerabilities in your information systems based on the risk assessment, at least every six months; and whenever there are material changes to your operations or business arrangements; and whenever there are circumstances you know or have reason to know may have a material impact on your information security program."

TYPICAL REQUIREMENTS OF A VULNERABILITY SCAN INCLUDE:

- Scans every six months at a minimum and when there are material changes to operations or if circumstances exist that might affect the information security program
- Identifying and documenting vulnerabilities
- Third-party oversight
- Costs start at $2,000 per PurpleSec (TPx has more budget-friendly options!)

HOW TPX CAN HELP

As a managed services provider, TPx monitors, manages and maintains customer environments 24/7/365. We can also run penetration and vulnerability scans for you.

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

According to section 16 CFR 314.4(e) of the FTC Safeguards Rule, organizations need to:

Implement policies and procedures to ensure that personnel are able to enact your information security program by:

1. Providing your personnel with security awareness training that is updated as necessary to reflect risks identified by the risk assessment
2. Using qualified information security personnel employed by you or an affiliate or service provider sufficient to manage your information security risks and to perform or oversee the information security program
3. Providing information security personnel with security updates and training sufficient to address relevant security risks
4. Verifying that key information security personnel take steps to maintain current knowledge of changing information security threats and countermeasures

WHAT IS SECURITY AWARENESS TRAINING?

Security awareness training is a formal process for educating an organization's employees and relevant third parties with system access on how to protect that organization's computer systems, data, people and assets from internet-based cyberattacks and security breaches.

HOW TPX CAN HELP

TPx offers a fully-managed program that follows industry best practices and uses industry leading training content.

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

Your organization will need to:

- Take reasonable steps to select and retain service providers.
- Require your service provider by contract to implement and maintain safeguards.
- Periodically assess your service provider based on risk present and adequacy of safeguards.

HOW TPX CAN HELP

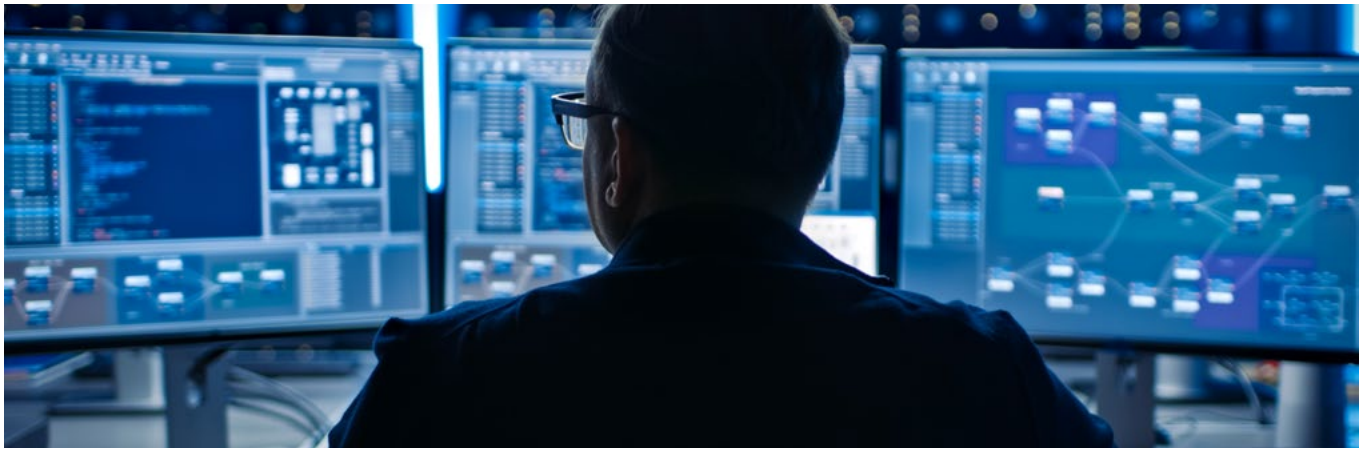
TPx can review T&Cs of your third-party service providers to make sure they align with the requirements of the rule.

7 Keep your information security program current.

According to the FTC, "*The only constant in information security is change – changes to your operations, changes based on what you learn during risk assessments, changes due to emerging threats, changes in personnel, and changes necessitated by other circumstances you know or have reason to know may have a material impact on your information security program. The best programs are flexible enough to accommodate periodic modifications*."

HOW TPX CAN HELP

TPx has access to threat intelligence and technical information to help keep your security program current.



8 Create a written incident response plan.

WHAT IS AN INCIDENT RESPONSE POLICY?

An Incident Response Policy is a documented process to "promptly respond to, and recover from, any security event materially affecting the confidentiality, integrity, or availability of customer information in your control."

STEPS TO CREATE AN INCIDENT RESPONSE POLICY

1. **Define the goals of the plan**

   What is the purpose of the Incident Response Policy?

   - Who, what, where, when, how and why
   - Designate an owner and manager of the incident
   - Make sure the policy is maintained and updated

2. **Establish internal processes to respond to an event**

   - Define breach vs. data loss
   - Define processes for responding

3. **Define clear roles, responsibilities and decision making**

   All the roles involved in an incident response include:

   - Legal
   - Technical
   - Executive
   - Business partners
   - Incident Responders
   - Communications

4. Establish external and internal communications and information sharing

What communications are required by law and to whom?

- External communications:
  - Customers
  - Partners
  - Law Enforcement (State/Federal)
  - Media
  - Associations
- Internal communications:
  - Employees
  - Board

5. Remediate any identified weaknesses and controls

- The standard process defined for weaknesses identified is to be remediated in an accelerated process
- The process for testing and validation of threat removal
- Manner of updating operational documents of the environment

Create procedures for documentation and reporting for events

- Incorporate tracking of the events of the incident.
- Include all parties and roles present and involved.
- Detail the data affected and communications occurred and when.
- Store the document in a repository that is backed up and secure.
- Register the document with legal and state/federal authorities.

6. Evaluation and revision of Incident Response plan following an event.

HOW TPX CAN HELP

TPx can generate an Incident Response Policy or evaluate your current one to ensure defensibility for the FTC Safeguards Rule requirements.

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. The report must:

- Report the overall status of the security program and company compliance
- Report material details regarding the program, including risk assessment, risk management, control decisions, etc.

HOW TPX CAN HELP

TPx can assist your organization in creating this report and if acting as a Qualified Individual will present it to your Board of Directors or equivalent.

FTC SAFEGUARDS RULE DATA CONTROLS REQUIREMENTS

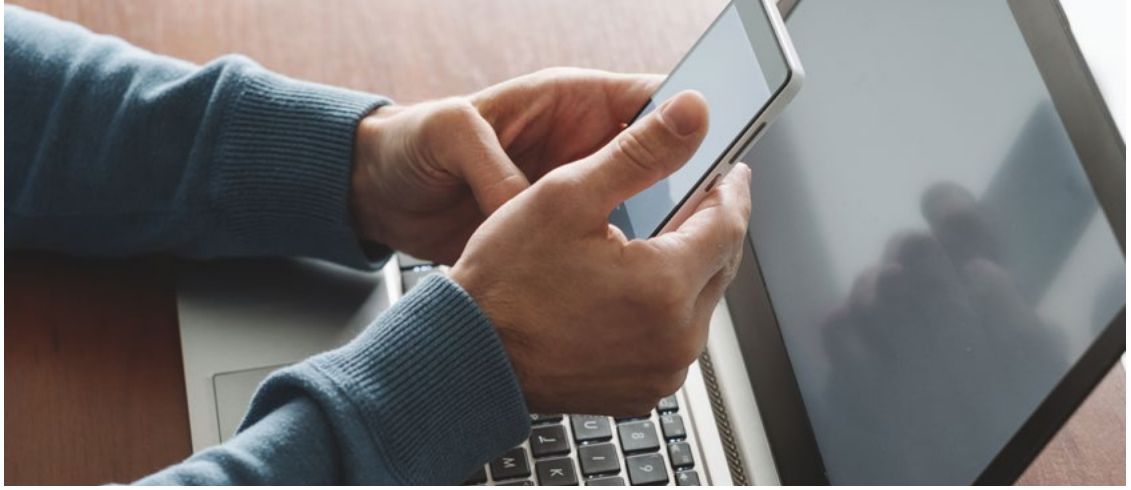
Data access control includes physical and electronic access to the non-public personal financial information. These data access control requirements include the following:

1. Only allow access to the data as needed by the job (Principle of least privilege and access control)
2. Must know where all the data resides to apply appropriate controls
3. Encrypt, if not, be defensible
4. Multi-factor authentication (MFA)
5. Secure disposal of data no later than 2 years after data is last used unless the business requires otherwise
6. Monitor and log user access to sensitive data
7. Access controls apply to wherever the data resides
8. Make sure you always document these practices

MAKING DATA ACCESS CONTROL EASY

You can establish effective data access control in three easy steps:

1. **DOCUMENT** – Know and document where data is located. This could be stored locally, in transit, in the cloud or service provider and backup.
2. **LOG** – Incorporate the "Principle of Least Privilege." Log who accesses what information at specific times.
3. **ENCRYPT** – Encryption is the most defensible of all controls you can place on your data.



ENFORCING MULTI-FACTOR AUTHENTICATION (MFA)

The FTC Safeguards Rule requires organizations to enforce MFA.

What is Multi-factor Authentication?

MFA means authentication through verification of at least two of the following types of authentication factors:

1. Knowledge factors, such as a password
2. Possession factors, such as a token
3. Inherence factors, such as biometric characteristics

What is Two-Factor Authentication (2FA)?

2FA is an electronic authentication method in which a user is granted access to a website or application only after successfully presenting two or more pieces of evidence to an authentication mechanism.

WHAT ARE THE TYPES OF IDENTITY AUTHENTICATION?

Knowledge Factor

The most commonly used type of identity authentication, knowledge factors, require the user to demonstrate knowledge of hidden information. Routinely used in single-layer authentication processes, knowledge factors can come in the form of passwords, passphrases, PINs or answers to secret questions.

Possession Factor

In a security context, the possession factor is a category of user authentication credentials based on items that the user has with them, typically a hardware device such as a security token or a mobile phone used in conjunction with a software token.

Possession Factor Options:

- **USB Keyfob** - This is a physical device you plug into the USB port of a laptop as a secondary means of authentication
- **Application on Phone** - A software-based two-step verification service using the Time-based One-time Password Algorithm and HMAC-based One-time Password algorithm
- **SMS Text Message** - A text message that is sent to a preset number for submission after entering a password

Inherence Factor

In a security context, the inherence factor is a category of user authentication credentials consisting of elements integral to the individual in question in the form of biometric data.

PART 5:

How Does TPx Help Organizations Comply with the FTC Safeguards Rule?

TPx helps organizations like yours become defensible for the FTC Safeguards Rule by helping to run effective security programs customized with the right support model to meet your needs.

Running an Effective Security Program

Creation of the Security Program

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:

1. System Security Plan (SSP)
2. Access Control Policy
3. Asset Management Policy
4. Encryption Policy
5. Multi-Factor Authentication (MFA) Policy
6. Data Retention/Disposal Policy
7. Change Management Policy
8. Log/Activity Monitoring Policy
9. Incident Response Plan

For those also developing software apps in-house, we can create 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 how each control is to be monitored and evaluated for effectiveness

Operation of the Security Program

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 of the Security Program

Paragraphs 16 CFR 314.4(g) and 16 CFR 314.4(i) of the FTC 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.

TPx FTC Safeguards Solutions

Security Program Create

The TPx Advisory Services' Security Program Create is designed for an organization with 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 & Report

Have you already created a security program, and you're confident it meets the requirements of the FTC Safeguards Rule? TPx can verify that the program is current, monitor that policies are appropriately enforced, and report on the program annually. This offering helps an organization maintain and "own" the program per the FTC Safeguards Rule requirements.

Security Program Complete

This solution is for you if your organization doesn't know where to start and has no one qualified to own the program. TPx will do everything in "Security Program Creation" and "Security Program Maintain & Report" to enable a defensible position from day one. 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 the FTC Safeguards 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, adjustment, and creation areas needed per the FTC Safeguards Rule. The report from the best practice review will be provided and utilized to be defensible for the FTC 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 remediated defined risks.

Train Your Staff

SECURITY AWARENESS TRAINING

Raise your staff's security aptitude. With phishing simulation emails and regular training courses, you can cut phishing email click rates by as much as 75 percent.

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.

PART 6:

Why Choose TPx

You have enough business challenges. Partnering with TPx provides your IT department the support it needs so you can focus on core business goals. At TPx, we have the products, services, experience and certifications to keep your productivity solutions running smoothly and safely.

We solve the biggest IT issues – cybersecurity, connectivity and collaboration – under one umbrella.

Our buying power enables us to customize your solutions for maximum effectiveness within your budget.

We have 120+ certifications across 60+ competencies, like CompTIA, Cisco, Fortinet, AWS, SMC and more.

We have the IT solutions, staff and experience you need for effective results within your budget.

We provide enterprise-class and 24/7 support for ongoing, proactive support tailored to your business.

We modernize your IT, connectivity and communications while minimizing your risk from cyberthreats.

With 18,000 clients in 49,000+ locations, we're big enough to get the job done and small enough to be agile.

We provide enhanced User Security solutions that protect your data and business from impending cyberthreats.

TPx is Your One-Stop Shop for Managed Services

We Make IT Easy

Security Advisory Services	Call Center	SD-WAN	Networks
Business Internet	Microsoft 365	Managed Detection and Response	Inbox Detection and Response
Security Awareness Training	Next-Generation Firewall (NGFW)	Endpoint Management and Security	Unified Threat Management (UTM)
DNS Protection	Backup and Disaster Recovery (BDR)	Ransomware Detection	UCx with Webex

Ready to Be Compliant with the FTC Safeguards Rule?

CONTACT US

ABOUT TPX

TPx is a leading nationwide managed services provider focused on the success of small and medium businesses (SMBs) with approximately 18,000 customers in more than 49,000 locations across the U.S. For more than two decades, TPx has offered managed services and solutions to help customers across every business sector address the growing complexity of their IT environments.

tpx.com