

FTC SAFEGUARDS RULE 2023

What? Who? Why? How?



TurnKeySolutions

INTRO:

- What is FTC Safeguards Rule ?
- Who needs to comply ?
- Why do clients need to comply ?
- How do I implement a solution ?



FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

About the FTC

Our mission is protecting consumers and competition by preventing anticompetitive, deceptive, and unfair business practices through law enforcement, advocacy, and education without unduly burdening legitimate business activity.

WHAT IS THE FTC SAFEGUARD RULE?

As the name suggests, the purpose of the Federal Trade Commission's Standards for Safeguarding Customer Information – the Safeguards Rule, for short – is to ensure that entities covered by the Rule maintain safeguards to protect the security of customer information. The Safeguards Rule took effect in 2003, but after public comment, the FTC amended it in 2021 to make sure the Rule keeps pace with current technology. While preserving the flexibility of the original Safeguards Rule, the revised Rule provides more concrete guidance for businesses. It reflects core data security principles that all covered companies need to implement.

FTC Safeguard Rule 2023

The purpose of the Safeguards Rule, is to protect the security of customer information. It reflects core data security principles that all covered companies need to implement.

Business Guidance

Bureau of Consumer Protection Business Center: Your go-to resource for advice on complying with FTC law. Questions about advertising, credit, privacy, security, tech, or FTC rules? The Business Center has nuts-and-bolts guidance for businesses, advertising professionals, and attorneys.



WHO NEEDS TO COMPLY?

- Retailer that extends credit
 - Automobile dealership
- Personal property or real estate appraiser
- Career counselor specializing in financial organizations
- Business that prints and sell checks for consumers
- Business that wires money to and from consumers
 - Check cashing business
 - Accountant or tax preparation service
- Travel agency in connection with financial services
 - Real estate settlement services
 - Mortgage broker
- Investment advisory company and a credit counseling service
 - Company acting as a finder for transactions

Who's covered by the FTC Safeguards Rule?

The Safeguards Rule applies to financial institutions subject to the FTC's jurisdiction and that aren't subject to the enforcement authority of another regulator under section 505 of the Gramm-Leach-Bliley Act. Some examples of that are:



Retailer that extends credit



Automobile dealership



Personal property or real estate appraiser



Career counselor in financial org.



Business that prints and sell checks



Business that wires money for consumers



Check cashing business



Accountant or tax preparation service



Travel agency with financial services



Real estate settlement services



Mortgage broker



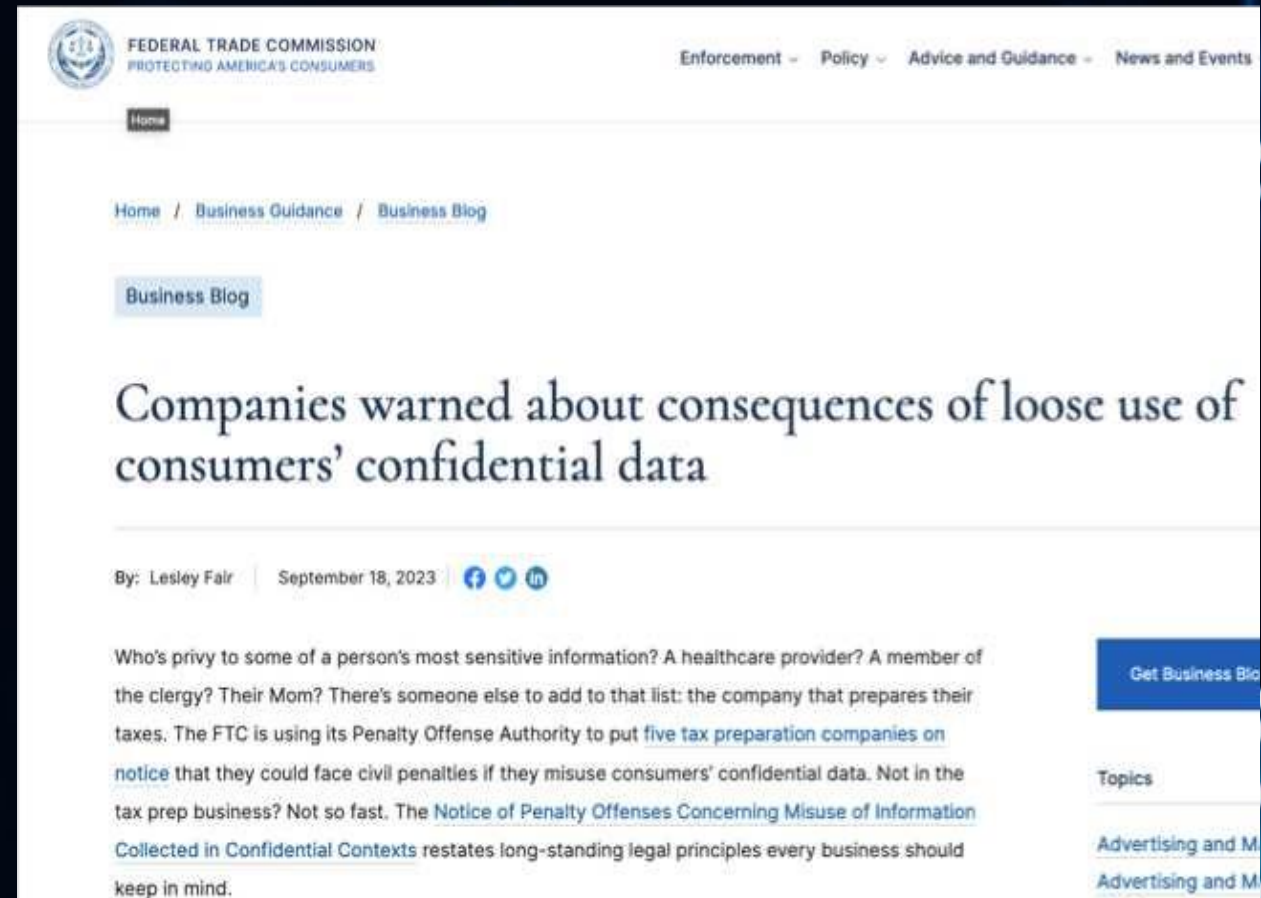
Investment advisory company



Company acting as a finder for transactions

Why do you need to comply?

- Follow the law.
- Civil penalties can help deter conduct that harms consumers.
- Companies can face civil penalties of up to \$50,120 per violation.



FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Enforcement - Policy - Advice and Guidance - News and Events

Home

Home / Business Guidance / Business Blog

Business Blog

Companies warned about consequences of loose use of consumers' confidential data

By: Lesley Fair | September 18, 2023 | [f](#) [t](#) [in](#)

Who's privy to some of a person's most sensitive information? A healthcare provider? A member of the clergy? Their Mom? There's someone else to add to that list: the company that prepares their taxes. The FTC is using its Penalty Offense Authority to put [five tax preparation companies on notice](#) that they could face civil penalties if they misuse consumers' confidential data. Not in the tax prep business? Not so fast. The [Notice of Penalty Offenses Concerning Misuse of Information Collected in Confidential Contexts](#) restates long-standing legal principles every business should keep in mind.

Get Business Blog

Topics

Advertising and M

Advertising and M

**If you think compliance is
expensive...**

...Try non-compliance

Former US Deputy Attorney General
Paul McNulty



Turn Key Solutions

THE REQUIREMENTS

The Safeguards Rule requires covered financial institutions to develop, implement, and maintain an information security program with administrative, technical, and physical safeguards designed to protect customer information.

The Rule defines customer information to mean “any record containing nonpublic personal information about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of you or your affiliates.”

What does the Safeguards Rule require companies to do?



Develop



Implement



Maintain



Administrative



Technical



Physical

Safeguards designed to protect customer information

THE INFORMATION SECURITY PROGRAM

- The 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. The objectives of your company's program are:
 - to ensure the security and confidentiality of customer information;
 - to protect against anticipated threats or hazards to the security or integrity of that information; and
 - to protect against unauthorized access to that information that could result in substantial harm or inconvenience to any customer.



What **Customer Information** needs to be protected?

"any record containing nonpublic personal information about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of you or your affiliates."

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.



HOW DO I IMPLEMENT A SOLUTION?

9 Elements of the Information Security Program

- Qualified Individual (QI)
- Risk Assessment
- Implement Safeguards
- Monitor and Test
- Training
- Service Providers.
- Security Program
- Incident Response Plan.
- Board of Directors



1. QUALIFIED INDIVIDUAL (QI)

Designate a Qualified Individual (QI) to implement and supervise an information security program.

- The Qualified Individual can be an employee of your company or can work for an affiliate or service provider. The person doesn't need a particular degree or title. What matters is real-world know-how suited to your circumstances. The Qualified Individual selected by a small business may have a background different from someone running a large corporation's complex system.
- If your company brings in a service provider to implement and supervise your program, the buck still stops with you. It's your company's responsibility to designate a senior employee to supervise that person.
- If the Qualified Individual works for an affiliate or service provider, that affiliate or service provider also must maintain an information security program that protects your business.



2. RISK ASSESSMENT

Conduct a Risk Assessment.

- You can't formulate an effective information security program until you know what information you have and where it's stored.
- After completing that inventory, conduct an assessment to determine foreseeable risks and threats, internal and external to the security, confidentiality, and integrity of customer information.
- 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.



3. IMPLEMENT SAFEGUARDS

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

- Implement and periodically review access controls.
- Know what you have and where you have it.
- Encrypt customer information on your system and when it's in transit
- Assess your apps.
- Implement multi-factor authentication for anyone accessing customer information on your system.
- Dispose of customer information securely.
- Anticipate and evaluate changes to your information system or network.
- Maintain a log of authorized users' activity and keep an eye out for unauthorized access.



4. MONITOR AND TEST

Regularly monitor and test the effectiveness of your safeguards.

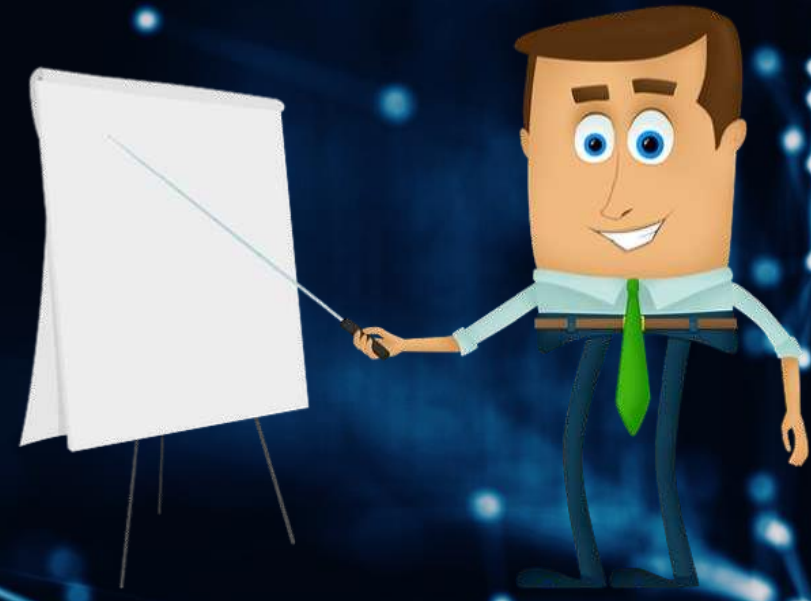
- Test your procedures for detecting actual and attempted attacks.
- For information systems, testing can be accomplished through continuous monitoring of your system.
- If you don't implement that, you must conduct annual penetration testing, as well as vulnerability assessments, including system-wide scans every six months designed to test for publicly-known security vulnerabilities.
- In addition, test
 - 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.



5. TRAINING

Implement Security Awareness Training for your staff.

- An institution's information security program is only as effective as its least vigilant staff member.
- Employees trained to spot risks can multiply the program's impact.
- Provide your people with security awareness training and schedule regular refreshers.
- Insist on specialized training for employees, affiliates, or service providers with hands-on responsibility for carrying out your information security program.
- Verify that your team are keeping their ear to the ground for the latest word on emerging threats and countermeasures.



6. SERVICE PROVIDERS

Monitor your service providers.

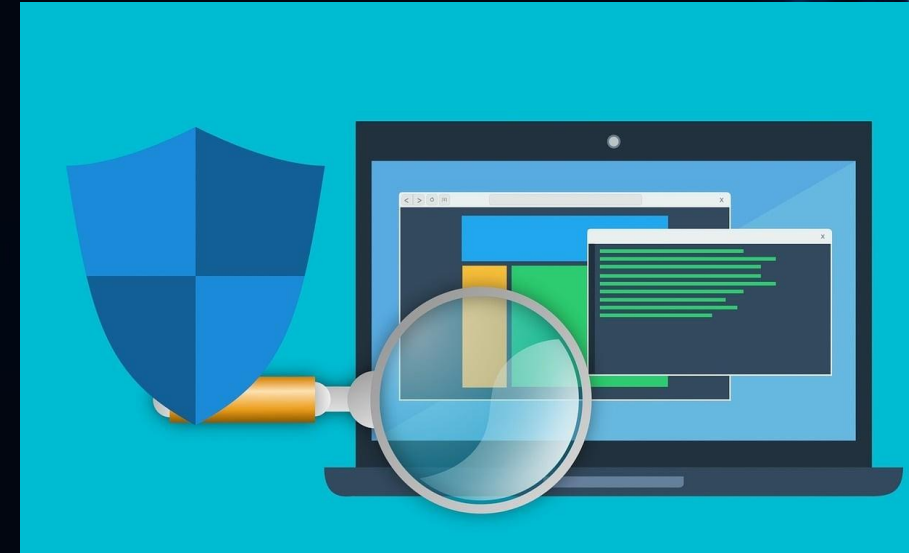
- Select service providers with the skills and experience to maintain appropriate safeguards.
- Your contracts must spell out your security expectations, build in ways to monitor your service provider's work.
- Provide for periodic reassessments of their suitability for the job.



7. SECURITY PROGRAM

Keep your information security program current.

- 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.
 - 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.



8. INCIDENT RESPONSE PLAN

Create a written incident response plan.

- *Every business needs a “What if?” response and recovery plan in place in case it experiences what the Rule calls a security event - an episode resulting in unauthorized access to or misuse of information stored on your system or maintained in physical form. Section 314.4(h) of the Safeguards Rule specifies what your response plan must cover:*
 - *The goals of your plan;*
 - *The internal processes your company will activate in response to a security event;*
 - *Clear roles, responsibilities, and levels of decision-making authority;*
 - *Communications and information sharing both inside and outside your company;*
 - *A process to fix any identified weaknesses in your systems and controls;*
 - *Procedures for documenting and reporting security events and your company’s response; and*
 - *A post mortem of what happened and a revision of your incident response plan and information security program based on what you learned.*



9. BOARD OF DIRECTORS

Require your Qualified Individual to report to your Board of Directors.

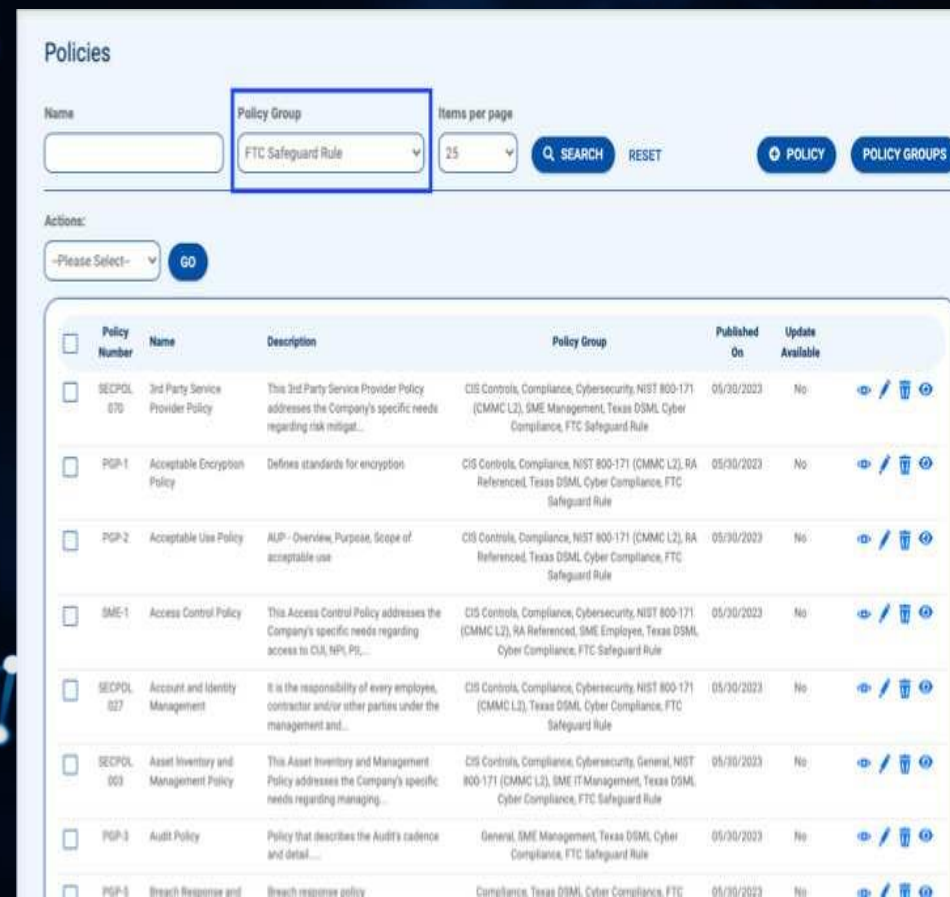
- Your Qualified Individual must report in writing regularly - and at least annually - to your Board of Directors or governing body.
- If your company doesn't have a Board or its equivalent, the report must go to a senior officer responsible for your information security program.
- What should the report address?
 - First, it must include an overall assessment of your company's compliance with its information security program.
 - In addition, it must cover specific topics related to the program - for example, risk assessment, risk management and control decisions, service provider arrangements, test results, security events and how management responded, and
 - recommendations for changes in the information security program.



HOW DO I IMPLEMENT A SOLUTION?

9 Elements of the Information Security Program

- Designate a Qualified Individual (QI) to implement and supervise an information security program.
 - The QI maybe an MSSP.
- Conduct a Risk Assessment.
- Design and implement safeguards to control the risks identified through your risk assessment.
- Regularly monitor and test the effectiveness of your safeguards.
- Implement Security Awareness Training for your staff.
- Monitor your service providers.
- Keep your information security program current.
- Create a written incident response plan.
- Require your Qualified Individual to report to your Board of Directors.



The screenshot displays a web interface for managing policies. At the top, there are search and filter controls, including a 'Policy Group' dropdown menu currently set to 'FTC Safeguard Rule'. Below this is a table listing various policies. Each row includes a checkbox, a policy number, a name, a description, a policy group, a published date, and an update availability status. Action icons for each row include a magnifying glass, a pencil, a trash can, and a refresh symbol.

Policy Number	Name	Description	Policy Group	Published On	Update Available
SECPOL-070	3rd Party Service Provider Policy	This 3rd Party Service Provider Policy addresses the Company's specific needs regarding risk mitigat...	CIS Controls, Compliance, Cybersecurity, NIST 800-171 (CMMC L2), SME Management, Texas DSML Cyber Compliance, FTC Safeguard Rule	05/30/2023	No
POP-1	Acceptable Encryption Policy	Defines standards for encryption	CIS Controls, Compliance, NIST 800-171 (CMMC L2), RA Referenced, Texas DSML Cyber Compliance, FTC Safeguard Rule	05/30/2023	No
POP-2	Acceptable Use Policy	AUP - Overview, Purpose, Scope of acceptable use	CIS Controls, Compliance, NIST 800-171 (CMMC L2), RA Referenced, Texas DSML Cyber Compliance, FTC Safeguard Rule	05/30/2023	No
SME-1	Access Control Policy	This Access Control Policy addresses the Company's specific needs regarding access to CUI, HIP, PS, ...	CIS Controls, Compliance, Cybersecurity, NIST 800-171 (CMMC L2), RA Referenced, SME Employees, Texas DSML Cyber Compliance, FTC Safeguard Rule	05/30/2023	No
SECPOL-027	Account and Identity Management	It is the responsibility of every employee, contractor and/or other parties under the management and...	CIS Controls, Compliance, Cybersecurity, NIST 800-171 (CMMC L2), Texas DSML Cyber Compliance, FTC Safeguard Rule	05/30/2023	No
SECPOL-003	Asset Inventory and Management Policy	This Asset Inventory and Management Policy addresses the Company's specific needs regarding managing...	CIS Controls, Compliance, Cybersecurity, General, NIST 800-171 (CMMC L2), SME IT Management, Texas DSML Cyber Compliance, FTC Safeguard Rule	05/30/2023	No
POP-3	Audit Policy	Policy that describes the Audit's cadence and detail...	General, SME Management, Texas DSML Cyber Compliance, FTC Safeguard Rule	05/30/2023	No
POP-3	Breach Response and	Breach response policy	Compliance, Texas DSML Cyber Compliance, FTC	05/30/2023	No

TurnKey Solutions



Securing Your Technology. Empowering Your Business.

Turnkeysol.com

225-751-4444