cbts

FTC Safeguards Rule

Enhancements for 2022 and 2023

John Bruggeman Consulting CISO

FTC Safeguard Rule Updates for 2022 and 2023

FTC Safeguard Rule Background

1. GLBA passed in 1999
   - Gramm-Leach-Bliley Act passed in 1999 requires FTC to develop safeguards and privacy standards and enforce them
   - Safeguards to protect consumer information
   - Privacy standards for consumers
   - Enforcement measures for non-compliance
2. FTC issued initial safeguards in 2003
   - Focused on data usage and risks for 1990s
3. FTC updated safeguards in 2021 published in Dec 2021
   - Focused on improving protection due to high profile data breaches
   - Provide concrete & specific guidance Financial Orgs must include
   - Updated for new technology & new risks
4. Financial organizations will need to be compliant by June 9, 2023
   - Original due December 9, 2022, extended to June 9,2023

FTC Safeguards apply *to organizations that are significantly engaged in financial activity*

1. Have a formal arrangement with customers, not ad-hoc

2. How often the organization engages in financial activity, lay-away plans do not count

3. Example organizations
   - Debt collection, Mortgage lending, Nonbank lending
   - Real estate settlement services
   - Higher Education establishments - Colleges and Universities
   - Check-cashing and payday loans
   - Brokering and servicing loans
   - Financial, economic, and investment advisory services
   - Courier services, Career counselors
   - Colleges and Universities

4. Customer information means
   - "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."

FTC Safeguard Rule Updates 2022

What are the main clauses?

1. Designate a **Qualified Individual (QI)** to supervise the Information Security Program and report in writing at least annually to the board of equivalent body. Including status of ISP, recommended changes and material maters including information risk.
2. Create, maintain and manage an **Information Security Program (ISP)**
3. Create and maintain a written **Risk Assessment** of the environment
4. Establish and maintain a written **Incident Response Plan**
5. Design and Implement **Safeguards** to control the risk
6. **Train and educate** staff
7. Oversee and **monitor service providers**
8. **Regularly test or monitor the effectiveness of safeguards**, like access controls, firewalls, software applications, data encryption

FTC Safeguard Rule Updates 2022

What are the main clauses?

1. What is a Qualified Individual (QI)?

- 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.

What are the main clauses?

2. What is an Information Security Program (ISP)?

- An Information Security Program is the
  - Administrative, Technical, or Physical safeguards you use to
    - access, collect, distribute, process, protect, store, use, transmit, dispose of,
    - or otherwise handle customer information
  - Administrative
    - Policies, procedures,
  - Technical
    - Firewalls, EDR, IDS, NIDS,
  - Physical
    - Locks, cameras, shredders, fences, etc.

What are the main clauses?

3. What is in a written Risk Assessment?

- Conduct an inventory of your current data
  - What information you have and where it's stored.
- Conduct an assessment to determine foreseeable risks and threats, internal and external, to confidentiality and integrity of customer information.
- Risk assessment must be written and must include criteria for evaluating those risks and threats. Develop a Risk Register to monitor your risk.
- How could customer information be disclosed without authorization, or be misused, altered, or destroyed.
- Risks to information constantly change so the Safeguards Rule requires you to conduct periodic reassessments in light of changes to your operations or the emergence of new threats.

What are the main clauses?

4. What is in a written Incident Response Plan?

- What your response plan must cover:
    1. The goals of your plan, RTO, RPO, BCP;
    2. The internal processes your company will activate in response to a security event;
    3. Clear roles, responsibilities, and levels of decision-making authority;
    4. Communications and information sharing both inside and outside your company;
    5. A process to fix any identified weaknesses in your systems and controls;
    6. Procedures for documenting and reporting security events and your company's response; and
    7. A post mortem of what happened and a revision of your incident response plan and information security program based on what you learned.

What are the main clauses?

5. What kind of Safeguards do you have to implement?

- Implement the principal of least privilege and periodically review ***access controls***
- Know **what** you have **and where** you have it, data inventory
- **Encrypt** customer information on your system and when it's in transit.
- **Assess your apps**, implement secure software development processes
- Implement **multi-factor authentication for anyone accessing customer information** on your system
- **Dispose of customer information securely** after 2 years
- **Anticipate and evaluate** changes to your information system or network, implement change management processes
- Maintain a **log of authorized users' activity** and keep an eye out for unauthorized access

What are the main clauses?

6. What kind of training and education is needed?

- Your ISP is only as effective **as its least vigilant staff member**.
- Train your team to spot risks
  - Crowdsource your security team, **multiply you ISP's impact**
- Provide your team with security awareness training and schedule regular refreshers, at least annually
- Insist on specialized training for employees, affiliates, or service providers **with hands-on responsibility for carrying out your ISP**
- Verify that your staff are keeping their ear to the ground for the latest threats and countermeasures

What are the main clauses?

7. How do you oversee and monitor service providers and third parties?

- Select service providers with the skills and experience to maintain appropriate safeguards
- Contracts must spell out your security expectations, build in ways to monitor your service provider's work
- Contracts must provide for periodic reassessments of their suitability for the job
- Monitor third party suppliers and vendors to ensure appropriate safeguards

What are the main clauses?

8. How do you regularly test or monitor the effectiveness of safeguards?

- Test your access controls at least annually
  - Review admin groups, root users, etc. Confirm AWS and Azure permissions are correct.
- Conduct vulnerability assessments
  - Either with an internal team or a 3rd party
- Perform penetration testing at least annually
  - Contract with a 3rd party to test external facing assets

CBTS Security Services

Road Map to Compliance

1. Security Program Assessment

2. Identify your QI, Risk Management

3. Document your Information Security Program

4. Vulnerability Management / Incident Response Plan

5. Develop Safeguards / Awareness and training

6. Third Party monitoring / Penetration testing

Questions?

John.Bruggeman@cbts.com