FTC Data Security Standard

- The FTC takes the position (Being tested now in litigation) that Section 5 of the FTC Act requires "Reasonable Security" under the circumstances: that companies have reasonable controls against reasonably foreseeable risks to the security, confidentiality, and integrity of personal information taking into account the size of the company and the sensitivity of the information it holds.
- Tort standard
- NOT strict liability
- What does this mean in practice?

1. Written Information Security Program

- Have a comprehensive security program that is reasonably designed to:
- (1) address security risks related to the development and management of new and existing products and services for consumers, and
- (2) protect the security, integrity, and confidentiality of covered information, whether collected by respondent or input into, stored on, captured with, or accessed through a computer using respondent's products or services.
- Such program, the content and implementation of which must be fully documented in writing, must contain administrative, technical, and physical safeguards appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the covered information, including:
- **<u>Responsible Employee or Employees for Program</u>**:
  - Designate an employee or employees to coordinate and be accountable for the security program;

2. Identify Reasonably Foreseeable Risks

- Identify material internal and external risks to the security, confidentiality, and integrity of covered information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other possession or is input into, stored on, captured with, or accessed through a computer using respondent's products or services, and assess of the sufficiency of any safeguards in place to control these risks.
- **<u>Assess Existing Safeguards to Address Identified Risks</u>:**

    - At a minimum, the risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to,
        1. employee training and management, including in secure engineering and defensive programming;
        2. product design, development and research;
        3. secure software design, development, and testing;
        4. review, assessment, and response to third-party security vulnerability reports, and
        5. prevention, detection, and response to attacks, intrusions, or systems failures;

3. Add Controls for Identified Risks Where Necessary; then Test and Monitor:

- Design and implement reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures, including through reasonable and appropriate software security testing techniques.
-

4. **Manage Service Providers Carefully:**

- Develop and use of reasonable steps to select and retain service providers capable of maintaining security practices consistent with this standard, and require service providers by contract to implement and maintain appropriate safeguards.

5. Update Security Program As Necessary:

- Evaluate and adjust your information security program in light of the results of your testing and monitoring, any material changes to your operations or business arrangements, or any other circumstances that you knows or have reason to know may have a material impact on the effectiveness of your information security program.

FTC Enforcement Actions: Actual Data Breach Allegations

- **Three Buckets:**
- Administrative
- Technical
- Physical

FTC Data Breach Allegations

- **Administrative**
- Failure to adequately train employees to handle and dispose of information securely
- Failure to implement policies and procedures regarding secure handling and disposal of personal information
- Failure to use reasonable measures to assess compliance with established policies and procedures
- Failure to employ a reasonable process to discover risk to personal information
- Failure to implement reasonable steps to address known or knowable risks
- Failure to assess scope of information stored, and delete this information after an appropriate period

FTC Data Breach Allegations

- **Administrative** (continued)
- Failure to require strong, different, or changing passwords, or to change default password
- Permitting sharing of login credentials
- Failure to develop or disseminate a comprehensive written security program
- Failure to monitor or test website for vulnerability to attack
- Failure to record and retain information sufficient to perform security audits
- Failure to implement or monitor policy requiring personal information be destroyed in a way to prevent read or reconstruction

FTC Data Breach Allegations

- **Administrative** (continued)
- Failure to inform employees of sensitive nature of data handled
- Failure to prevent (or affirmatively allowing) password storage in plaintext
- Failure to employ reasonable measures to respond to unauthorized access, or perform a security investigation
- Failure to remedy known security vulnerabilities
- Failure to inventory computers with access to network
- Failure to monitor against previously successful methods of intrusion
- Failure to maintain and update computer operating systems
- Failure to appropriately test, audit, assess, or review its applications

FTC Data Breach Allegations

- **Administrative** (continued)
- Failure to ensure that the transmission of sensitive personal information was secure
- Failure to maintain an adequate process for receiving and addressing security vulnerability reports from third parties
- Failing to strict employees' access to consumer information based on business need
- Providing service providers with access to consumers' complete personal information to develop new applications
- Using consumers' personal information in training sessions with employees and failing to ensure that the information was removed from employees' computers following the training
- Failure to supervise service providers or require them by contract to implement appropriate safeguards

FTC Data Breach Allegations

- **Administrative – Vendor Oversight**
- Failure to reasonable and appropriately oversee service provider's security practices
- Failure to require by contract that service providers implement and maintain appropriate safeguards for consumers personal information
- Failure to request or review relevant information about the service providers security practices
- Failure to adequately verify that the service provider implemented reasonable and appropriate security measures to protect personal information
- Failure to take adequate measures to monitor and assess whether the service provider employed measures to protect personal information

FTC Data Breach Allegations

- **Technical**
- Failure to use reasonable means to look for or prevent unauthorized activity
- Transmitting or storing personal information in clear text, or failing to encrypt personal data or credentials
- Failure to use reasonable security for wireless network
- Failure to use firewalls, server segmenting, or similar network security system
- Failure to suspend credentials after a certain number of failed login attempts
- Allowing storage of credential with access to nonpublic information in cookies
- Allowing creation of new credential without certifying that the creator was a customer

FTC Data Breach Allegations

- **Technical** (continued)
- Failure to adequately restrict third-party access (via specific IP or temporary access)
- Failure to adequately restrict third-party access (via software design or permissions)
- Failure to monitor outbound traffic to detect export of sensitive data
- Failure to institute reasonable technical limits on administrative access
- Allowing users to bypass authentication by going to a specific URL
- Failure to strip personal information before transmitting data to server

FTC Data Breach Allegations

- **Technical** (continued)
- Failure to restrict the number of requests any one account could make to application programming interface (API)
- Failure to implement any restrictions on serial and automated account creation
- Overriding the default SSL certificate validation settings, without implementing other security measures to compensate for the lack of SSL certificate validation
- Failure to use readily available security measures to limit wireless access to network

FTC Data Breach Allegations

- **Physical**
- Failure to adequately train employees to handle and dispose of physical information securely
- Failure to implement policies and procedures regarding secure physical handling and disposal of personal information
- Failure to store and dispose of physical personal information in a secure manner
- Transporting laptops containing personal information in a manner that made them vulnerable to theft or other misappropriation