The FTC and the Evolution of Privacy & Security Law

Presented by:
David Holtzman
VP of Compliance, CynergisTek

Today’s Presenter

• Vice President of Compliance Services, CynergisTek, Inc.
• Subject matter expert in health information privacy policy and compliance issues involving the HIPAA Privacy, Security and Breach Notification Rules
• Over 12 years of experience in developing, implementing and evaluating health information privacy and security compliance programs
• Former senior advisor for health information technology and the HIPAA Security Rule, Office for Civil Rights

David Holtzman
CynergisTek, Inc.
Agenda

1. Applying the FTC Act to the Protection of Privacy
2. Deceptive Trade Practices
3. Unfair Trade Practices
4. Data Security Standards
5. Enforcement and Corrective Actions
6. Wrap Up

Applying the FTC Act to Protection of Privacy
**FTC Act**

- Federal Trade Commission Act
  - Signed into law in 1914 to provide consumers protection against anticompetitive, deceptive or unfair business practices of companies in interstate commerce
  - Section 5 prohibits unfair or deceptive acts or practices
- Beginning in 1995 FTC sought industry self-regulation to combat threats to consumer privacy
- Since 2002 FTC has brought more than 55 cases alleging consumer data not reasonably safeguarded due to deceptive or unfair trade practices

---

**Common Law of Privacy & Security**

- Congress gave FTC very broad and general regulatory authority by design for an evolutionary approach
- Overlap in agency authority inevitable with other agencies and state law because jurisdiction in FTC Section 5 spans nearly all industries
- Use of a “reasonable” standard for data security looks to industry accepted standards instead of a rigid set of rules
- An evolving Common Law approach to privacy and data security requirements
Deceptive Trade Practices

Deception Jurisdiction Far Reaching

• Any materials representation, omission or practice that is likely to mislead a reasonable consumer
• Broken promises of privacy and data security
• Deceptive actions to induce disclosure of information
• Failure to give sufficient notice of invasive practices
Broken Promises of Privacy

- Promises to maintain confidentiality or to refrain from disclosing information to third parties
- Promises to only collect data consistent with the company’s policy
- Promises to provide adequate security for personal data
- Promises to maintain anonymity
- Promises not to disclose personal data to third parties by selling in bankruptcy proceedings

General Deception

- Deceptive actions taken by a company in order to induce disclosure of information of personal information
  - False and misleading claims
  - Misrepresenting the authority to receive personal information from consumers or those who hold information of consumers
- If the deception is egregious enough practice is considered to be an Unfair Trade Practice
  - Unfair practices that caused substantial injury, not reasonably avoidable by consumers
## Insufficient Notice

- Providing consumers Notice and Choice
  - Fair Information Privacy Principles (FIPP) widely adopted as industry standard practice
  - Adequate notice on data collected and used about them
  - Giving choice regarding certain forms of data collection or use.
- Companies ignored consumer privacy preferences

## Data Security

- Enforcing promises to provide reasonable security measures to protect personal information from unauthorized access, alteration, disclosure or destruction
- Reliance on industry standards and other norms to identify practices that constitute adequate security practices when collecting personal information
Unfair Trade Practices

• “Unfair” practices are defined through a 3 part test
  – Cause or are likely to cause substantial injury to consumers
  – Which is not reasonably avoidable by consumers themselves, and
  – Not outweighed by countervailing benefits to consumers or competition
# Theories of Unfair Trade Practices

- **Retroactive Changes**
  - Changing terms or privacy settings collected under a previous, different agreement

- **Deceitful Data Collection**
  - Collecting personal information through deceit, surreptitious data gathering or surveillance

- **Improper Use of Data**

- **Unfair Design or Unfair Default Settings**

- **Unfair Data Security Practices**

---

# Data Security Standards

---
Comprehensive Data Security Program

- Companies handling consumer information must implement a program
  - With administrative, technical, and physical safeguards appropriate to the organization’s size and complexity,
  - The nature and scope of its activities and
  - The sensitivity of the personal information collected from or about consumers
- Develop and implement procedures for data collection, storage, handling, transport, and disposal

Security Based on Industry Best Practice

- Formal data security procedures should employ readily available technology and practices for safeguarding consumer information
- Consider well-known threats and business specific vulnerabilities tailored to an organization’s business model and data needs
- Security policies should cover
  - Password procedures
  - Access limitations
  - Encryption protocol
  - Processes for data retention and disposal
Software and Product Review

- Implement appropriate checks and controls on the review and testing of software or products intended for internal use
- Follow industry best practices for programming including those described in the product’s OS guides
- Perform security reviews and testing of software and products at key points in development cycle

Managing Service Providers

- Require by contract that service providers implement and maintain appropriate safeguards for consumers’ personal information
- Ensure reasonable oversight of service providers’ security practices and their employees handling of personal information
  - Adequately verify through monitoring & assessments that service providers implement reasonable and appropriate security measures to protect personal information
  - Request and review relevant information about a service provider’s security practices
Risk Based Privacy & Security

• Companies implement a program that considers safeguards to security, integrity and confidentiality to personal information online
  – Material threats or hazards that would compromise the privacy or security of sensitive information
  – Ensure issues are addressed and corrected
  – Continuous monitoring and evaluation based on changing circumstances

Unauthorized Access & Disclosures

• Preventing and addressing incidents of unauthorized access to and disclosure of personal information
  – Check for & install critical patches and updates
• Implement reasonable measures to assess and enforce compliance with established security policies
  – Scanning networks & blocking unauthorized downloads
Detecting Unauthorized Access

• Implement policies for the detection of unauthorized access
  – Installing anti-virus or anti-spyware programs on components
  – Employing an intrusion detection system
  – Creating a formalized process to address security warnings and intrusion alerts
  – Logging network activity and reviewing activity in any network.

Employee Training

• Employee training program to assist employees in understanding & managing privacy and security standards
  – Line employees, IT administrators and executives should receive training on the sensitivity and safeguarding of personal information of consumers
  – IT administrators should receive appropriate training and oversight for detecting application vulnerabilities and conducting security testing
FTC Enforcement Under Section 5

How FTC Enforces Section 5

• Case-by-case enforcement actions through settlements
  – Prohibition on wrongful activities
  – Fines and other monetary penalties
  – Consumer notification and remediation
  – Deleting data and refraining from using it
  – Making changes in privacy policies
  – Establishing comprehensive programs
  – Assessments by independent monitors
  – Recordkeeping and compliance reports
  – Notification of material changes affecting compliance
Wrap Up

How to Keep Up With Evolution

• Review FTC Settlements
  – Development of privacy and security requirements explained in FTC settlements
  – Changes in consumer expectations
  – Industry standards evolve
  – Innovation in technology
• FTC Reports and Guides for Business
  – Privacy and Security Update
Questions

David Holtzman
david.holtzman@cynergistek.com
512.405.8550 x7020
@HITprivacy

Questions?