Protecting Electronic Data
Current Enforcement Landscape

- **Consumer Protection Statutes**
  - Consumer Protection Act, Uniform Deceptive Trade Practices Act
  - Similar to FTC’s enforcement authority

- **3 avenues of enforcement for data breaches**
  - Misrepresentations
  - Omissions
  - Unfairness

- Not every breach is a violation!
Investigation

- Inquiry Letter
  - Nebraska impact
  - Type of data
  - Security details
  - Remediation
  - Forensic report

- Red Flags

- Additional investigation
Current Data Security Standards

- **National**
  - NIST Framework (voluntary)
  - FTC Enforcement

- **Industry-Specific**
  - Payment Cards: PCI DSS
  - Healthcare: HIPAA
  - Financial Institutions and Creditors: Gramm-Leach-Bliley Act and FCRA

- **International**
  - ISO (International Standards Organization) standards for information security (voluntary)

- **State**
  - Massachusetts Data Security Regulations
  - New York Bill: Safe Harbor Approach (not yet enacted)
  - Data Security Guides (CA, IL, MS) (voluntary)
Difficulty of Defining a Standard

- Companies are different
  - Sensitivity of Data
  - Size/Available Resources
- Security evolves
- Checklist fallacy
  - Security is a process, NOT a checklist
Working with the AG - 2 Way Street

- **Attorney General**
  - Outreach/Education
  - Penetration Testing
  - Data Security Guides

- **Industry**
  - Contacting our office before a breach
  - Reach out to us when a breach occurs
  - Develop standards and expertise