MAYER·BROWN

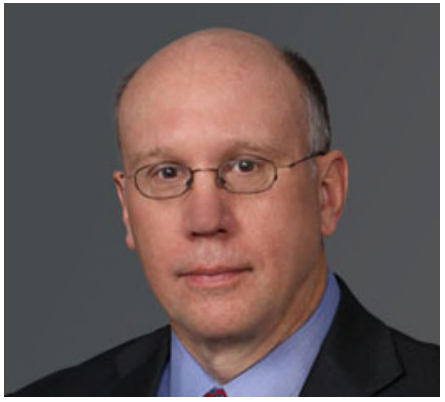
Cybersecurity Legal Requirements Today and Tomorrow

AND HOW TO MINIMIZE LIABILITY RISK IN CHANGING TIMES

Robert Kriss
Partner

+1 312 701 7165
rkriss@mayerbrown.com

Speakers



Robert Kriss

Partner - Chicago

MAYER·BROWN

Overview

- What is the current legal approach to cybersecurity in the United States?
- How might that approach change in the future?
- What can my company do to minimize liability risk in the evolving legal environment?

CURRENT REGULATORY APPROACHES TO CYBERSECURITY

State and Federal Regulation

- A general reasonableness/negligence standard is imposed by many federal and state regulatory agencies
- Often there is a requirement to conduct a risk assessment and take reasonable steps to mitigate the risks identified, as well as to prepare written plans and policies
- A few state and federal regulatory agencies have issued additional specific requirements such as encryption and multi-factor authentication

Examples of Specific Safeguards Required by States

- New York State Department of Financial Services (NYDFS) Cybersecurity Requirements for Financial Services Companies
  - Encryption of information at rest and transmitted over external networks or alternative compensating controls
  - Multi-factor authentication for external access or reasonably equivalent controls

Examples of Safeguards Required by the States

- Regular cybersecurity training for all personnel
- Penetration testing and vulnerability assessments
- Application security

Examples of Specific Safeguards Required by States

- California –
  - California law requires "reasonable security procedures and practices appropriate to the nature of the information."
  - However, the California Attorney General's Office has announced that the 20 CIS Critical Security Controls constitute minimal requirements for reasonable security
    - Examples: multi-factor authentication for remote and administrative access; encryption of information over public networks; continuous vulnerability assessments; installation of anti-malware protection

FTC Enforcement

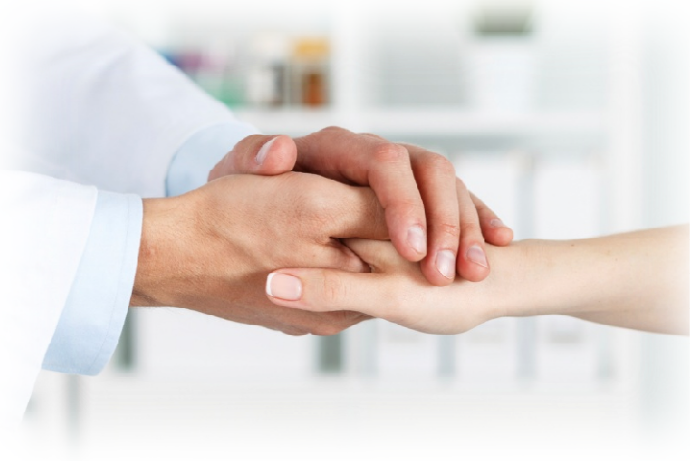
- The FTC brings enforcement actions under the "deception" and "unfairness" prongs of Section 5 of the FTC Act
- The FTC's approach is case-by-case and is based upon its view of reasonable practices rather than promulgated rules
- The FTC's approach was sustained on appeal. *See FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015)

FTC Enforcement

- FTC published a “best practices” guidance document based upon the enforcement cases it has brought
- FTC’s “Start With Security: A Guide for Business” - practical lessons based upon 50+ cases, including but not limited to:
  - Limit access to information on a “need to know” basis, particularly administrative access
  - Complex and unique passwords
  - Limit the number of unsuccessful attempts to log in
  - Encryption of sensitive data during storage and transmission
  - Segment network to isolate sensitive data
  - Application security
  - Include provisions requiring security precautions in service provider contracts

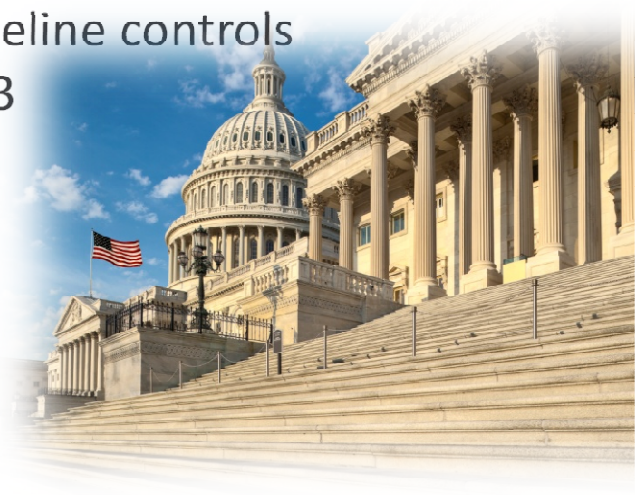
HIPAA

- HIPAA requires a risk assessment and reasonable safeguards but also specifies particular safeguards that must be implemented (e.g., developing a disaster recovery plan) and other safeguards that must be addressed and either implemented or a contemporaneous written explanation must be prepared to justify the decision not to implement (e.g., encryption)



Federal Information Security Management Act

- Applicable to federal agencies and private contractors of federal agencies
- Requires identification and classification of information by risk level
- Requires selection of specific controls from sets of baseline controls corresponding to risk levels, as set forth in NIST 800-53



CLASS ACTION LITIGATION

Class Action Litigation

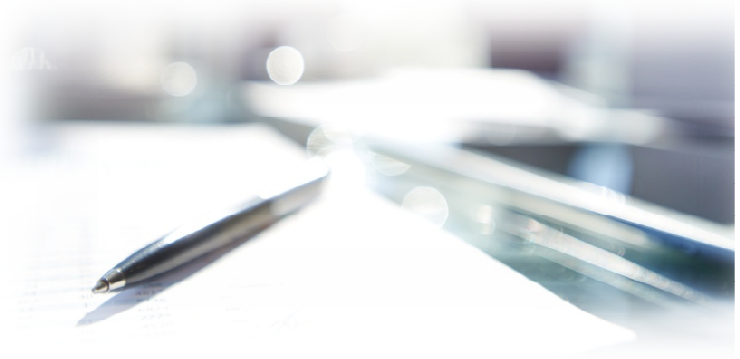
- Many hurdles for plaintiffs to clear
  - Standing
  - Motions to dismiss for failure to state a claim
  - Class certification
  - Liability
  - Proof of damages

Class Action Standing

- Disagreement among the federal circuits concerning standing requirements
  - Seventh Circuit decisions could be interpreted as finding standing based upon deliberate data breach. *See Remijas v. Neiman Marcus Grp.*, LLC, 794 F.3d 688 (7th Cir. 2015)
  - Other circuits require some evidence of actual misuse of data. *See Reilly v. Ceridian Corp.*, 664 F.3d 38 (3d Cir. 2011)

Motions to Dismiss

- Most common claims: breach of implied contract; negligence; violation of state consumer protection act; unjust enrichment; declaratory judgment/injunction to prevent future breach
- In many cases, one or more claims have survived, often implied contract and state consumer protection act



Motions to Dismiss (con't.)

- Highest risk claims – unjust enrichment and declaratory judgment/injunction to prevent future breach
- These claims could avoid difficulties in proving injury and damages on an individual basis
- We recently succeeded in having those claims dismissed
- Results are mixed around the country

Class Certification

- Until March of this year, no contested consumer class had been certified
- Very few cases have reached this procedural point because in the past most were dismissed on standing grounds

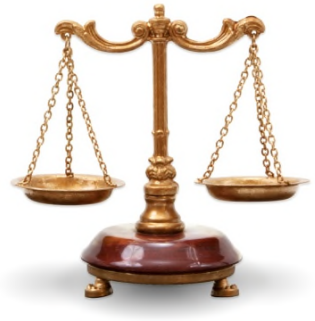
Class Certification (con't.)

- A class of banks suing a retailer was certified. *In re Target Corp. Customer Data Sec. Breach Litig.*, 309 F.R.D. 482 (D. Minn. 2015)
- A class of consumers was certified. *Smith v. Triad of Alabama, LLC*, No. 1:14-CV-324-WKW, 2017 WL 1044692, at *16 (M.D. Ala. Mar. 17, 2017)

Issues Not Addressed Yet

LIABILITY

- How to determine what is adequate security
- What is adequate secu



DAMAGES

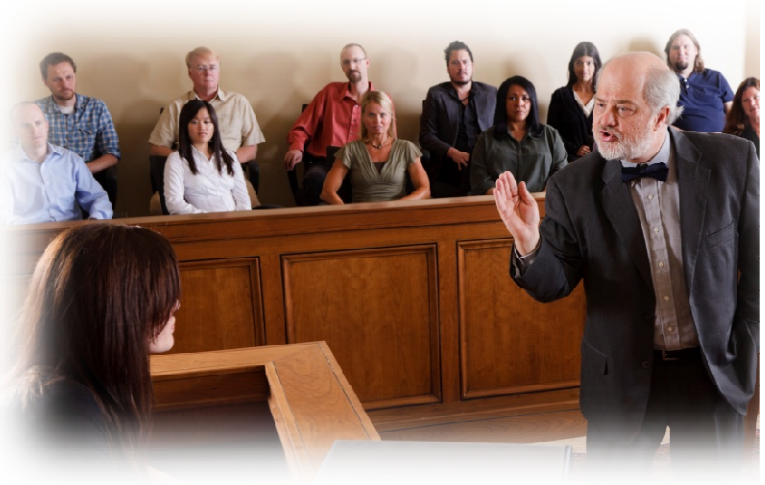
- How to determine damages in a cybersecurity class action
- What types of damages will be recoverable in a cybersecurity class action?

Possible Future Directions

- State and federal regulation
  - More rules imposing additional specific requirements probably will be issued by various agencies
  - Regulatory agencies may begin to scrutinize reasonableness of risk assessments and responses to risk assessments
  - FTC will likely continue its case-by-case approach; FTC will focus attention on failures to implement safeguards in its guidance document

Possible Future Directions (con't.)

- Class Action Litigation
  - More cases may be certified and defendants will have to address liability and damages
  - The issue of whether defendant implemented reasonable safeguards may be resolved in a manner similar to medical malpractice claims ("Battle of Experts" in front of a jury)



Possible Future Directions (con't.)

- Class Action Litigation (con't.)
  - State and federal regulations requiring specific safeguards and "guidance" documents may be used to establish at least a minimum standard for reasonable safeguards, whether or not the regulations or guidance technically apply to defendant
  - Consulting reports obtained by defendants in the regular course of business may be used to determine whether defendant implemented reasonable safeguards

Possible Future Directions (con't.)

- Class Action Litigation (con't.)
  - Rules Enabling Act and judicial precedent support requirement for individualized damages determinations (*See Smith v. Triad of Alabama, LLC*, No. 1:14-CV-324-WKW, 2017 WL 1044692 at *16 (M.C. Ala. Mar. 17, 2017))
  - Plaintiffs may press for class-wide damages for lost time based upon averages

Possible Future Directions (con't.)

- Class Action Litigation (con't.)
  - Plaintiffs may seek payment for credit monitoring or other types of identity-theft preventive measures regardless of whether class members incurred the cost on their own
    - Standing arguments against recovery for speculative injury
    - Analogous to medical monitoring and future injury cases

Possible Future Directions (con't.)

- Class Action Litigation (con't.)
  - Actions concerning the Internet of Things
    - Plaintiffs may seek injunctive relief to prevent injury
    - Plaintiffs may seek diminution in economic value

RISK MITIGATION

Risk Mitigation

- Disclaimers of liability for negligence in customer contracts and negation of implied contract obligations
- Restrained statements regarding cybersecurity protections in external cybersecurity policy statements
- Development of written information security plans and data-breach response plans based upon reasonable cybersecurity standards

Risk Mitigation (con't.)

- Reasonable cybersecurity standards
  - Risk assessment and reasonable safeguards to address risks
  - Determine legal requirements and guidance documents expressly applicable to your company's business
  - Continuously monitor regulatory developments in rapidly evolving environment

Risk Mitigation (con't.)

- Also consider FTC Guidance; HIPAA Security Regulations; CIS Critical Security Controls; N.Y. DFS Regulations; PCI DSS standards (applicable to credit card information);
  Mass. Data Security Regulations
  - Plaintiff may argue these sources describe the best practices applicable to any company holding sensitive information, so failure to comply constitutes a failure to implement reasonable safeguards
  - These sources are likely to have substantial credibility with the judge, so compliance with them may result in a judgment in favor of defendant

Risk Mitigation (con't.)

- Involve a litigator at the beginning of the process of obtaining consulting reports
  - Provides a basis for claiming confidentiality on the grounds of attorney-client privilege
  - Minimizes the risk that the report will be framed in a manner that can be used against your company as an industry standard that was not met
  - Consider asking for a list of addressable safeguards to enhance security
  - Avoid terminology such as "best practices," "requirements," "security gaps," system "maturity" levels

QUESTIONS?

Robert Kriss
Partner

+1 312 701 7165
rkriss@mayerbrown.com