NetDiligence®

Standard of Care

What is ‘reasonableness’?

Industry and regulator views

Speakers

Mark Mao (Moderator), *Troutman Sanders*
Doug Meal, *Ropes & Gray*
Tom Kang, *The Hartford*
Adam Hamm, *North Dakota Department of Insurance*
Edwin Acosta, *U.S Department of Health and Human Services, Office of Civil Rights*

Question 1 – Is Evidence of a Breach *Per Se* Evidence of Unreasonableness?

Industry View

- FTC has long expressly stated “no” (most recently in *LabMD*)
- Other regulators agree
- This is so whether “breach” means
  - A “data security breach” – an intrusion into the network or other event that puts personal information at risk, or
  - A “data breach” – an actual theft or loss or unauthorized disclosure of personal information
- Instead, "unreasonableness" must be independently proven (more on that later)

Question 1 – Is Evidence of a Breach *Per Se* Evidence of Unreasonableness?

- FTC Act and, by extension, most state consumer protection statutes, have an additive "consumer injury" element
  - Scope of injury requirement hotly debated (*LabMD* latest case)
  - And some state consumer protection statutes do not have an injury element
- Other regulatory regimes have no additive "consumer injury" element
  - GLBA and HIPAA in the US, e.g.
  - GDPR abroad, e.g.

Question 1 – Is Evidence of a Breach *Per Se* Evidence of Unreasonableness?

Regulators' View

- OCR opens investigations into breaches affecting 500+ individuals, and into number of smaller breaches
- Investigations involve looking at:
  - Underlying cause of the breach
  - Actions taken to respond to the breach (including compliance with breach notification requirements) and prevent future incidents
  - Entity's compliance prior to breach

Question 1 – Is Evidence of a Breach *Per Se* Evidence of Unreasonableness?

- In most cases, entities able to demonstrate satisfactory compliance through voluntary cooperation and corrective action
- In some cases though, nature or scope of indicated noncompliance warrants additional enforcement action
- Resolution Agreements/Corrective Action Plans
  - 36 settlement agreements that include detailed corrective action plans and monetary settlement amounts
- 2 civil money penalties

Question 2 – How Organizations Should Resolve Conflicts Between Different Regulatory Bodies' of Care?

Question 3 – In An Underwriting Situation, How Do You Determine What Controls Are Reasonable or Not?

- Underwriting challenges:
  - Underwriting process
  - Determining the right control level
  - Lack of data
- Considerations
  - Regulatory guidance
  - Internal and external security experts
  - Creating the right framework
  - Long term data analysis

NAIC Roadmap

Roadmap for Cybersecurity Consumer Protections

- Adopted December 2015
- What consumers can expect *all the time* from insurers
  - E.g., What information do they keep about me? What is their privacy policy? How are they protecting my information? Who are they sharing my information with?
- What consumers can expect *in the event of a breach*
  - E.g., How and when will I be notified? What are they doing to fix the problem? Who can I call for more information? Can I get identify theft protection, credit monitoring, or a credit freeze? Copies of relevant documents?

Data Collection

Cyber Liability Market Data Collection

- *Cybersecurity and Identity Theft Coverage Supplement* – insurer's annual financial reports
- Began **Q1 2016**
  - Identity theft insurance
  - Cybersecurity insurance

Insurance Data Security Model Law

Proposed Common Definitions

Consistent meanings for “Data Breach”, “Personal information”, etc.

Information Security Program

Requirements, Board of directors role, 3rd party service providers

Consumer Rights

Pre-breach, post-breach, investigations, notifications

Regulator’s Role

Commissioner’s power, hearings, witnesses, examination authority

Question 4 - How Can The Industry Be Better Prepared For Litigation, And Ensure & Prove That Reasonable Controls Are In Place?

Advice from the industry

- Diligently review public facing privacy statements;
- Conduct security assessments under privilege;
- Review insurance posture;
- Set incident response plan and test controls;
- Hire knowledgeable gatekeepers;
- Use reliable technology and be diligent about updates;
- Mindfully negotiate partner and vendor contracts;
- Thoughtfully plan and be well-advised

Question 4 - How Can The Industry Be Better Prepared For Litigation, And Ensure That Reasonable Controls Are In Place?

Advice From Industry

- Use a cost-benefit-analysis approach (per *Wyndham* and *LabMD*)
- Focus heavily on the security measures the company *did* have
- Bring the injury element (both magnitude and probability) into play as part of the analysis

Question 4 - How Can The Industry Be Better Prepared For Litigation, And Ensure That Reasonable Controls Are In Place?

Suggestions From Regulators (1 of 2 slides)

- Recurring Compliance Issues:
  - Business Associate Agreements
  - Risk Analysis
  - Failure to Manage Identified Risk, e.g. Encrypt
  - Lack of Transmission Security
  - Lack of Appropriate Auditing
  - No Patching of Software
  - Insider Threat
  - Improper Disposal
  - Insufficient Data Backup and Contingency Planning

Question 4 - How Can The Industry Be Better Prepared For Litigation, And Ensure That Reasonable Controls Are In Place?

Suggestions From Regulators (2 of 2 slides)

- Some Good Practices:
  - Review all vendor and contractor relationships to ensure BAAs are in place as appropriate and address breach/security incident obligations
  - Risk analysis and risk management should be integrated into business processes; conducted regularly and when new technologies and business operations are planned
  - Dispose of PHI on media and paper that has been identified for disposal in a timely manner
  - Incorporate lessons learned from incidents into the overall security management process
  - Provide training specific to organization and job responsibilities and on regular basis; reinforce workforce members' critical role in protecting privacy and security

Questions

Mark Mao (Moderator), *Troutman Sanders*
Doug Meal, *Ropes & Gray*
Tom Kang, *The Hartford*
Adam Hamm, *North Dakota Department of Insurance*
Edwin Acosta, *U.S Department of Health and Human Services, Office of Civil Rights*