CLM- Cyber Liability Conference
October 15, 2014- New York, NY

All Things Data Privacy

All Things Data Privacy Litigation

I. Sources of Data Privacy litigation

   a. Data Breaches and Class Actions
   b. Regulatory Enforcement Actions
   c. PCI Enforcement
   d. Other Litigation/Regulatory Enforcement
      i. Single Plaintiff in data breach context
      ii. Shareholder Derivative Suits
      iii. Privacy policy violations and Children's Online Privacy Protection Act (COPPA)
      iv. CAN-SPAM

II. Class Actions – Defenses Eroding
   a. Based on Data Breaches – Failure to protect data; Failure to properly notify; Failure to mitigate; Unjust enrichment; Consumer Protection violations
      i. NO VERDICTS. . . Yet
   b. Defenses Eroding
      i. *Stollenwerk v. Tri West* – 9th Cir. – must assert actual identity theft.
      ii. *Krottner v. Starbucks Corp.* – 9th Cir. – increased risk of identity theft constitutes an injury-in-fact.
      iii. *Heartland* – 5th Cir. – banks and credit unions not barred by economic loss doctrine from recouping card reissuance costs.
      iv. *Anderson v. Hannaford* – 1st Cir. – alleged actual fraud and money spent in mitigation efforts defeat dismissal
      v. *Resnick v. AvMed* – 11th Cir. – Similar to *Anderson*; also held unjust enrichment claims viable for failure to keep promise to protect information.
   c. California's CMIA
      i. Allows private right of action and statutory damages of up to $1,000 per person affected.
      ii. Stanford

III. Regulatory Enforcement Actions

i. HHS and OCR
    1. Presbyterian Hospital & Columbia University (2014)
        a. ePHI (medical information) was found to be accessible through internet search engines related to 6,800 individuals.
        b. Columbia physician attempted to deactivate personal internet server from the hospital network but lacked skills to do so securely.
        c. OCR investigation found that Hospital made no effort to assure the server was secure or contained appropriate software protections.
        d. No thorough risk analysis or risk management plan
        e. Failed to implement appropriate policies or to enforce those it did have in place
        f. $4.8 million settlement
    2. Affinity Health Plan, Inc. (2013)
        a. Photocopier formerly leased by Affinity contained PHI on copier hard drive.
        b. 344,579 individuals' affected.
        c. OCR investigation found that Affinity failed to delete PHI before returning the copier.
        d. Failed to implement appropriate policies related to copier return
        e. $1.2 million settlement

ii. State AGs and other agencies in CA, MA, VT, TX, IN and NC are consistently investigating reports of exposures
    1. California - Kaiser Foundation Health Plan Inc. (2014)
        a. Breach exposed over 20,0000 employees' SSN, dates of birth, addresses and other PII for spouses and children
        b. Breach allegedly occurred in December 2011 but notice was not provided until March 2012
        c. Settlement requires notification on a rolling basis, meaning "as soon as reasonably possible after identifying a portion of the total individuals affected by a breach, even if the investigation is ongoing[,]" with notification continuing throughout and until Kaiser competes its investigation
        d. Kaiser Permanent paid $150,000 in penalties and attorneys' fees
    2. Massachusetts - Women & Infants Hospital of Rhode Island (WIH) (2014)
        a. $150,000 settlement for a data breach involving 12,000 patients in Massachusetts that exposed patients' names, dates of birth Social Security numbers, dates of exams, physicians' names and ultrasound images.

b. WIH discovered 19 unencrypted backup tapes were missing in April 2012 after they were supposedly shipped in the summer of 2011
c. WIH did not provide notice to consumers and regulators until the fall of 2012

3. Indiana - WellPoint
    a. Records (including SS#s, health and financial info) of over 32,000 Indiana residents were potentially accessible on an unsecured website (Involved 645,000 nationally)
    b. Settlement includes $100,000 fine to the state, up to two years of credit protection to affected state residents, and reimbursement of up to $50,000 for any losses.

iii. FTC Actions
1. Background
    a. 50 enforcement actions brought since 2002
    b. Claim violations of Section 5(a) of the Federal Trade Commission Act, prohibiting "unfair and deceptive acts or practices."
2. Wyndham Worldwide Corporation
    a. Alleged repeated security failures (3 incidents over 2 years) resulting in the exposure of credit card information for over 600,000 people
    b. U.S. District Court for the District of N.J. denied Wyndham's attempts to dismiss the complaint
    c. Court found that the FTC had authority to bring an unfairness claim in data security context
    d. Court warned "this decision does not give the FTC a blank check to sustain a lawsuit against every business that has been hacked."

iv. SEC Enforcement
1. LPL Financial Corporation (2008) - Experienced series of breaches from July 2007 to February 2008
    a. Company failed to implement adequate controls, despite an awareness of the insufficiency of its controls
    b. Unauthorized person or persons accessed and traded, or attempted to trade, in the customer accounts of several of LPL's representatives
    c. Action based on failure to comply with Safeguards Rule of Regulation S-P (See 17 CFR 248) Registered entities must have written policies and procedures designed to:
        i. Insure the security and confidentiality of customer records and information;

ii. Protect against any anticipated threats or hazards to the security or integrity of customer records and information; and
iii. Protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.

d. Settled for $275,000

2. Commonwealth Equity Services, LLP (2009)
    a. Hacker gained access to system after the company failed to have adequate anti-virus software
    b. Intruder able to access 368 accounts enabling $523,000 in unauthorized security/stock purchases
    c. Action based on failure to comply with Safeguards Rule
    d. Settled for $100,000.00
3. Woodbury Financial Services, Inc. (2009)
    a. Woodbury encouraged recruits to take PII with them from former firms without getting consent.
    b. Action again based on violations of Safeguards Rule
    c. Settled for $65,000

b. PCI enforcement
    i. Payment Card Industry Security Standards Council (Visa, Mastercard, AmEx, Discover, JCB International)
    ii. PCI requires merchants and service providers to abide by certain protocols to protect customers' credit card information
        1. PFI
        2. Security Assessor and ongoing PCI compliance/certification
    iii. Imposes "fines" and "penalties" on offending merchants and service providers (can be millions)
    iv. Violations of PCI DSS have multiple consequences
    v. Impact on standard of care – industry investigations, outside lawsuits
    vi. Small minority of states have incorporated PCI-DSS requirements into data protection laws

c. Other litigation (10 Minutes)
    i. Shareholder Derivative Suits
        1. Target
            a. Allegations: failure to prevent breach and to timely report accurate information about the breach causing severe damage to the company
            b. Claims: Breach of fiduciary duty, waste of corporate assets, gross mismanagement and abuse of control
            c. Relief sought – Monetary damages and injunctive relief "by way of significant corporate and managerial reforms to prevent future harm to the Company by disloyal directors and officers."

2. Wyndham Worldwide Corporation
    a. Allegations: Company affected by 3 breaches between April 2008 and January 2010; Company failed "to take reasonable steps to maintain their customers' personal and financial information in a secure manner"
    b. Claims: Breaches of fiduciary duty, waste of corporate assets and unjust enrichment
    c. Relief sought: recovery of the damages the company allegedly has suffered, remedial action with respect to corporate governance and internal procedures and disgorgement of profits and compensation

ii. Single Plaintiff – if actual fraud and no redress;
iii. CAN-SPAM, COPPA
iv. Privacy Policy violations