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

Cyber Claims Crystal Ball

CLM - Cyber Claims Crystal Ball (50 minutes)

I. Recent Developments related to First and Third Party Claims
   a. First Party
      i. Incident response claims becoming more routine: counsel, forensics, notice, regulator notice, call center
      ii. Credit monitoring, despite no legal requirement, is becoming more mandatory and less of an optional add on
         1. Various regulators expect some type of offering regardless of the type of information exposed.
   b. Third Party
      i. Class actions continue to be filed
         1. Statutory damages available in CMIA
         2. Statutory damages available in CAN-SPAM (difficult to prove)
         3. More plaintiffs willing to initiate litigation despite continued failure to defeat dismissal
      ii. Business to business indemnity claims continue to be filed
         1. Recover notice costs including attorneys fees
   c. Subrogation

II. US. Regulatory Enforcement
   a. HIPAA remains most consistent source of Regulatory Action
      i. Breach reporting to HHS
      ii. OCR investigations
         1. Presbyterian Hospital & Columbia U. (2014) - $4.8 million settlement.
         2. Affinity Health (2013) - $1.2 million settlement.
   b. SEC
      i. No enforcement actions based on 2011 Guidance requiring disclosures related to data privacy
         1. SEC has issued approximately 50 comment letters regarding compliance
      ii. Continue to enforce other rules such as Safeguards Rule
         1. LPL Financial Corporation (2008) – Settled with SEC for $275K

2. Commonwealth Equity Services, LLP (2009) – Settled with SEC for $100K

c. FTC
    i. 50 enforcement actions since 2002 related to data privacy matters.
d. CA Dept. of Public Health – can fine up to $250,000 for violation of CMIA
    i. Routinely issues $50K and $100K fines (10 fines totaling $774K issued around July 24, 2014)
e. State Attorneys General
    i. California, Massachusetts, Indiana and others are moderately to significantly active.

III. PCI Enforcement
a. Intruders learning faster than security experts can stop them – ease of intruder access remains a significant risk
b. Large and mega-retailers are more frequently targeted (Target, Michaels)
c. PCI Data Security Standards 3.0 (new in 2013) is being incorporated into security assessments, investigations and fine structures.
    i. Fines can be in the multi-millions based on amount of fraud, number of cards affected, number of violations, cost of investigations
        1. Fines and PCI assessments are not public, but Heartland matter involved 130 million exposed cards, and settlements were: Visa for $60 million and; MasterCard for $41.4 million

IV. International Regulatory Enforcement
a. European focus continues to be on regulating the collection and sharing of data (not specifically notification in the event of security breach).
    i. Canada, Germany, and about ten other foreign states have varying degrees of requirements surrounding data exposure reporting.
b. Regardless of reporting requirements, when data exposures are public, regulators often conduct intrusive investigations and require significant security and policy improvements.

V. Impact on the Forms and Scope of Coverage Going Forward
a. What was covered?
b. What is covered now?
    i. Legal – managing investigations, notification, compliance reviews and legal defense.
    ii. Vendors
    iii. Fines and penalties
    iv. Settlements
c. What will be covered?