CLM CLAIMS & LITIGATION MANAGEMENT ALLIANCE™

ADVANCING ETHICS, COOPERATION AND EDUCATION

2014 CLM Annual Conference

April 9, 2014 – April 11, 2014

Boca Raton Resort
501 E. Camino Real
Boca Raton, FL 33432

Roundtable 2: Thursday, April 10, 2014 (11:30 am – 12:30 pm)

Cyber Liability is Coming to an Inbox Near You – Will You Be Ready?

I. Introduction

a. Current Events

Current events including the Snowden disclosure and the widely reported data breaches at Target, Nieman Marcus and others provide further evidence of the expansive growth of cyber risk not only for large retailers but also governmental entities, consumers and businesses of all sizes in the U.S. and throughout the world.

b. Threat Assessment

While large scale data breaches involving tens of millions of people grab most of the headlines, cyber liability claims more often involve smaller incidents such as: a lost briefcase with paper records; a misaddressed email; or an unencrypted lost smart phone.

II. Preparing for a Data Security Incident

a. Financial Impact of a Breach

The cost associated with data breach incidents are increasing exponentially. According to the Ponemon Institute's 2013 cost of data breach study, the average cost of a data breach in the U.S. is $5.4 million dollars, or $199 per record. These cost numbers are even more compelling given that very large data incidents (like Target) are excluded from the calculus. The cost factors include: legal defense, notification to customers, forensic experts, credit monitoring, lost customer sales. Quantifying more long term damage such as reputational injury is best described as a work "in progress."

b. How can Insurance Help?

First and third party coverage for cyber liability is now offered by an increasing number of insurers' worldwide. There is no standard coverage or policy form at this time and the amount and type of insurance can vary significantly. Cyber Liability insurance policies may cover damage arising from loss or disclosure of confidential information, mandated customer notification, credit monitoring, crisis management expenses, forensic experts, defense costs for civil suits or regulatory response.

c. Data Security Practices

The old adage an ounce of prevention is worth a pound of cure applies when it comes to managing risks of cyber liability exposure. Large companies commonly have senior executives who administer elaborate data security programs. Mid-market and small companies rarely have a full time CPO (Chief Privacy Officer) or team of in-house experts with multi-million dollar budgets.

A good place to start if a company does not have a professionally developed data security plan is the cyber liability insurance application process. This organized survey will yield a top-level understanding of the status of data security at a particular company.

Beyond the cyber insurance application process, the next step is to seek out a certified (or otherwise qualified) data security expert to help build organized data security program. Professionals certified as CIPP/US or CISSP® may be qualified to help companies establish and maintain Data Security Programs or Data Incident Plans (DIP). The steps include assessment, strategic planning, establishing information security practices, monitoring the compliance, and improvement practices. A good source to learn more is IAPP's Resource Center (http://privacyassociation.org/resource_center).

III. Managing a Data Security Incident

a. Detection and Investigation

The first thing to do if a data security incident is suspected is to engage internal and outside counsel. There may be a number of civil and/or criminal laws at both State and Federal levels which may be implicated.

b. Containment

Next, utilize internal and outside forensic IT resources to identify the source or cause of the incident and get it contained. Depending on what the investigation reveals, there may be legal obligations to notify law enforcement and regulatory agencies such as the state Attorney General's Office.

c. Reporting and Crisis Management

In cases where an investigation reveals potential criminal activity, the law may permit, or even require a delay in public notice of a data security incident. If the data incident involves disclosure of PII (personally identifiable information) it is likely that formal notice to governmental regulators will be required. As investigation, containment and notice compliance are underway, the crisis management team, should establish control of information outflows and respond to any false or inaccurate information from media or other sources after appropriate consultation with legal counsel.

d. Resolution and Strategic Response

Complete resolution of a data security incident may take months or even years to accomplish. In worst case scenarios, class action litigation or major regulatory fines and compliance programs may be necessary. The FTC has required adoption of comprehensive data security plans with third party monitoring and reporting for 20 years as part of consent decree resolutions.

In minor incidents such as unauthorized access to data without associated damages or public harm (such as identify theft), the incident may resolve shortly after the incident is contained.

IV. Defending Against Claims

a. Statutory and Regulatory Infrastructure

In the United States, the laws addressing data security and privacy are generally organized by industry or sector. A business in the financial sector will have one set of laws such as the Gramm-Leach-Bliley Act 15 U.S.C. Sec. 6801 *et seq*. requires financial institutions to provide each consumer with a privacy notice at the time the consumer relationship is established and annually thereafter. A business in the health industry will be subject to a significantly different set of rules such as HIPAA (Health Insurance Portability and Accountability Act) 42 U.S.C. Sec.1320d *et seq.*

By contrast, other countries follow a more centralized approach organized around a single set of privacy laws that apply across all industries or sectors such as the European Union see e.g. Data Protection Directive. In the United States the Federal-Trade Commission (FTC) addresses most cyber liability issues. It is fair to say that the FTC regulators go after companies that break promises to consumers about the scope and uses of data collection. Of particular concern are any practices that involve data collection from children under 13. See COPPA- Children's Online Privacy Protection Act 5 U.S.C. Sec. 6501*et seq.*; 16 CFR Part 312.

b. Potential Plaintiffs

Forty-six states have data breach notification laws that can subject businesses to fines or damage claims. The most likely plaintiffs are the State Attorneys General. However, ten states (notably California) allow some type of private action for money damages. There

have been class actions attempted under various theories, but most have been successfully defended. The better cases involve actual damages such as identity theft resulting in monetary losses.

c. Causes of Action

In general it is true that most tort and contract theories that may be brought outside the cyber world can also be brought as cyber liability actions. One recent case involved Schnuck Markets, a mid-west supermarket chain. Schhucks suffered a data security incident involving PII (personally identifiable information). In one case, a representative plaintiff, advanced a complaint which included: violation of Illinois Data Breach Notification Statute, unfair trade practices, breach of contract, invasion of privacy, negligence and third-party beneficiary claims. Class certification was sought on grounds that there were common questions of fact and law. The main litigation was settled for a reported 1.6 M, but collateral cases arose over insurance coverage and secondary actions to recoup some of the costs.

d. Defense Case Studies

- Rock Bottom Auto Sales, December 7, 2012
  - 8 Bags of Credit Applications
  - Contained Names, Driver's License Info, SSN's
  - Found unattended on a dirt road in Hudson, Florida
- West Pittsburgh Partnership, December 10, 2012
  - Job Placement Documents found in a dumpster
  - All Contained Names and SSN's
- Internal Revenue Service, 2008
  - Disposed of taxpayer documents as regular waste
  - Failed to consistently verify that contractors with access to those documents passed background checks.

- Unencrypted Laptop Lost
    - Univ. of Mississippi Medical Center,March 22, 2013
        - Contained patient names, SSN's, addresses, diagnoses, PII
        - Only protected by a password
- Unencrypted USB Flash Drive Stolen
    - Georgia Middle School Teacher's car on January 8, 2013
    - Unencrypted flash drive containing student SSN's
- Unencrypted Backup Tapes Missing in Transit
    - TD Bank, March 2012… reported by Calif. AG March 2013
    - Contained Customers & dependents SSN's, account info, credit and debit card numbers and addresses

V. Closing Comments

a. Prospective Markets, Prospective Risks

According to published reports, Cyber Insurance went from 1B to 1.3B in annual gross written premium in a single year. Health industry and mid-to-small size business are the leading sectors. Data breaches continue to occur at a more frequent rate and the count of data loss per breach and associated costs are on the increase. There is no reason to conclude that the risk and the market for insurance will continue to grow over the next few years.

b. Preparation is Best Defense

If there is one take away from this presentation it is: Preparation is key to preventing and minimizing risk for cyber liability yin general and data breach in particular. Data Incident Planning must be done before a data loss occurs, otherwise there is little opportunity for a good result. Professional data security advice and planning coupled with appropriate insurance coverage are what every business needs.