CLM 2015 Retail, Restaurant & Hospitality Conference
February 5-6, 2015 in Orlando, Florida

"How to Be Secure in an Unsecure Retail World"

I. How to Prevent a Cyber Breach/What to Do When One Occurs?

Hypothetical 1: BestShirtsAround is a popular clothing store that sells custom shirts to teenagers. A week ago it was learned that computer hackers used a local wireless network at one of BestShirtsAround's stores to access their main computer. Once on the system, the hackers accessed both credit card and checking account information for more than 1.4 million of its customers. Having never dealt with a situation like this before, BestShirtsAround's CEO contacts their in-house counsel in a panic wanting to know how to respond to this issue, as well as how to prevent a similar breach from occurring in the future.

- How Do You Protect Against a Cyber Breach?
  - BE PREPARED
    - Establish a committee to meet quarterly to discuss potential issues
    - Have policies in place regarding the privacy and security of business data. This includes use of encryption, remote access, mobile devices, laptops, email accounts, and social networking sites
    - Inventory company's software systems and data, and assign ownership and categorization of risk. The higher the sensitivity of the information the stronger the security protections and access control must be!
    - Identify points of contact with law enforcement, internet service providers, and the communications companies that service your business, and cyber forensic experts.
    - Conduct third-party vulnerability scans, penetration tests, and malware scans. Antivirus software is also essential, *BUT* does not catch everything.
    - Perform software code reviews on Web applications and custom code to detect vulnerabilities.
    - Conduct training for employees.
    - Develop security protocol.
    - Develop incident report/disaster recovery plans and communications plans AND test them.
- What Do You Do Once a Cyber Breach Occurs?
  - Retain a third party service provider to determine what information was obtained and the source of the breach.

- Contact counsel to determine legal notification requirements and coordinate remediation with law enforcement and governmental/regulatory agencies.
- Communicate with client/customer regarding breach.
- Consider hiring a public relations firm.

- Breach Notification Laws
  - Each state varies as to its definition of what constitutes personal identifiable information and the requirement for notifying customers of a data security breach.
    - Florida Information Protection Act of 2014 - Fla. Stat. § 501.171
      - Provides new notice requirements and possible civil penalties arising out of a data breach incident when the notice requirements are not followed
      - Requires covered businesses and governmental entities to take "reasonable measures to protect and secure data in electronic form containing personal information."
      - Under Florida's Act, "personal information" is defined to include (1) a person's name in combination with (a) a social security number, driver's license number, passport number, and/or other similar number on a government ID, (b) a financial account, debit card or credit card number in combination with a related password or access code, (c) medical history information, or (d) a health insurance policy number or identification number; or (2) a user name or email address in combination with a password or security question and answer that would permit access to an online account.
      - Under Florida's Act, a "breach" is considered the "unauthorized access of data in electronic form containing personal information."
      - With regard to the new notice requirements, the Act requires businesses and government entities to give notice to consumers "no later than 30 days after the determination of a breach or reason to believe that a breach occurred" unless the breach qualifies for exceptions. Exceptions include circumstances where information was released during an ongoing criminal investigation or the covered entity determines, after consultation with law enforcement, "that the breach has not and will not likely result in identify theft or other financial harm." This latter exception must be documented in writing and it must be maintained for 5 years.
      - The Act sets out exactly what must be included in the notice to individuals. And if a breach could affect more than 500 people, the Attorney General's office must also be notified within 30 days, along with other notice requirements.
      - Failure to adhere to the Act could be deemed "an unfair and deceptive trade practice" and also subject the covered entity to a civil penalty up to $500,000, with the penalties being imposed based on the number days the party is in violation of the Act.

- ***However***, the Act does specifically state that it does not create a private right of action.
    - Forty-seven states have now enacted data breach notification statutes, but Florida is one of just seven states that require notification within a specific period of time – 30 days from determination of the breach. States that do not require a specific time period tend to use broader language merely requiring notice in a reasonable time.
    - Florida is also one of only a handful of states that has expanded the definition of "personal information" to specifically include a user name/email address and password to access an online account.

- Types of Exposure
    - First Party Loss
        - Notify Insurers (Cyber, LPL and GL) that information was compromised or exposed;
        - Retain counsel to consult with relevant to legal, law enforcement and regulatory obligations as well as protect attorney-client privilege;
        - Investigate , remediate and coordinate with forensic experts;
        - Set up call centers and/or purchase credit monitoring services for customers affected by the breach or hacking incident;
        - Launch a public relations campaign to restore the reputation of the company affected by the breach; and
        - Compensate the business for income that it isn't able to earn while it deals with the fallout of the data breach (i.e., Business Interruption Insurance).
    - Third Party Loss - includes claim for damages against those within your company who were responsible for the safe storage of data.
        - Failure to anticipate or prevent the transmission of a virus to a third party. In other words, a security gap in your software let a virus onto your client's machine and it spread to all your client's email contacts;
        - The misuse, disclosure, or theft of confidential information stored on a network. This is your classic data breach: one or more of the systems you set up allowed a hacker to access and/or expose your clients' customers' information; and
        - Infringement of the right to privacy. This could involve an event in which a system you built failed to keep confidential information properly secure.
    - Prepare for potential class action litigation stemming from the above claims as well as third party indemnification claims.
    - The financial exposure associated with a data breach can be quite substantial. Studies show that the average defense costs for defending such a claim is over $500,000.
    - Besides the costs of defending a cyber lawsuit, the amount of damages can also be quite significant.
        - The U.S. Court of Appeals for the Sixth Circuit recently held in Retail Ventures, Inc. v. National Union Fire Insurance Company of Pittsburgh, PA, 691 F. 3d 821 (6th Cir. 2012), that DSW, Inc., DSW Shoe

Warehouse, Inc., and Retail Ventures, Inc. were entitled to coverage under a commercial crime policy for a $6.8 million loss resulting from a data breach.

- In Zurich American Insurance Co. v. Sony Corp. of American, et al., Index No. 651982/11 (N.Y. Sup. Ct.) while granting summary judgment in favor of Zurich in a coverage dispute, Sony alleged in its Court papers that a data breach stemming from the hacking of their PlayStation online services had exposed personal information of tens of millions of users, and Sony's losses were reportedly estimated to be as high as $2 billion.

- A cyber breach can also cause damage in other ways such as loss of productivity, loss of data and intellectual property, business interruption, and, perhaps, most importantly, injury to the brand or reputation.
- Regulators such as the Federal Trade Commission and State Attorney General offices are getting involved and imposing fines and penalties on businesses for failing to protect data or provide timely notice of a breach.

II. Directors and Officers Beware!

Hypothetical 2: Michael Money is a successful entrepreneur with years of experience in the hospitality industry. He is recently approached by a new hotel chain for dogs, Best Dogs Inn, to serve on the board of directors of their publicly traded company. Initially, Michael is reluctant because he has never served as a board of directors before. However, the other members of the board assure Michael that they will handle the majority of the decision making, and he simply has to show up once a month to a board meeting. Michael ultimately agrees to serve on the board of directors as he sees it as a lucrative opportunity to join a business from the ground level. Six months later, Michael turns on the television and learns that Best Dogs Inn is the subject of a cyber-attack wherein all of the personal identifiable information of their clients has been stolen. Shortly thereafter, Michael is served with a shareholder lawsuit alleging that as a member of the board he failed to maintain reasonable safeguards to prevent against a cyber-attack.

- Duty of Loyalty and Duty of Care
  - Besides the corporation itself, individual directors and officers can also be exposed to liability for breach of a fiduciary duty in failing to properly oversee cyber security.
  - With so much at stake in protecting personal identifiable information, it is not enough for a director and officer of a company to simply delegate responsibility for protecting such confidential information to their IT staff.
  - In general, corporate directors and officers have a legal duty to act carefully and with loyalty on behalf of the corporation. This duty of care requires them to act diligently and prudently in making decisions on behalf of the company including properly implementing and overseeing the company's system of controls. As a result, besides suing a company itself for an alleged data breach, lawsuits now are also being filed against individual directors and officers for failing to maintain reasonable safeguards to prevent against a cyber-attack.
- Directors and Officer Liability

- Directors and officers are vulnerable to a number of exposures arising out of a cyber breach from securities and business litigation, which includes breach of fiduciary duty, derivative shareholder action, securities fraud, and class action lawsuits.
- Directors and officers can also face being voted out of their position.
    - The proxy adviser, Institutional Shareholders Inc., recommended that Target stockholders vote against seven of ten directors because they failed to manage cyber risks arising out of their cyber breach.
    - This is the first time that there has been an effort to unseat board members because of a cyber breach. Thus, given the increased prevalence and effectiveness of cyber-attacks and breaches, it would be difficult to justify why proper protective measures, including sufficient cyber insurance, were not implemented, and why the risks were not disclosed to the investing public.

- Recommendations for Publicly Traded Companies
    - One of the more serious issues facing a company's directors and officers is providing prompt and adequate notice to customers of an alleged breach. Recently, the Division of Corporation Finance of the SEC recently issued a "Disclosure Guidance", which recommends that material information regarding cyber-security risks and cyber incidents should be disclosed in order to make other required disclosures, in light of the circumstances under which they are made, not misleading. Information is considered material if there is a substantial likelihood that a reasonable investor would consider it important in making an investment decision, or if the information would significantly alter the total mix of information made available.
    - While this is merely a recommendation by the SEC, not a rule or regulation, non-compliance is risky. Furthermore, although these recommendations are only directed at public companies under the SEC's jurisdictions, other businesses would be prudent to heed the same advice.
    - As a result, directors and officers must be attuned to new regulations to protect themselves against the impact of cyber risks and costs in the larger context of their company's disclosure obligations to customers and investors alike.

III. Am I Covered?

Hypothetical 3: Sal's Best Steakhouse is a popular restaurant in New York City, and the place of choice for dining for many famous celebrities. In order to ensure that Sal's business is sufficiently covered from liability, Sal retains the services of Coverage One, an experienced insurance brokerage firm. In particular, Sal specifically advises Coverage One that he would like a policy issued to him to cover his restaurant for any situation that may expose him to liability. Thus, Coverage One issues to Sal the following policies: General Liability, Errors & Omissions, Property Insurance, and Crime. A few years later, Sal's business is the subject of a data breach due to one of his waiters accidentally clicking an anonymous link in his work email proclaiming that he won a free trip to Aruba, which provided a point of entry into Sal's computer system. Having read about the significant expenses associated data breaches to other business, Sal is able to rest assured knowing that he has insurance in place to cover this type of loss. Shortly

thereafter, Sal receives a letter from his insurance company advising that the policies issued to him do not cover damages that constitute data breach expenses: forensic experts, notification, crisis management, credit monitoring expenses, legal expenses, etc. The policies also do not cover the loss of fees or profits by Sal's restaurant, or non-monetary relief.

- Why Should Businesses Be Concerned?
  - Businesses have potentially large amounts of consumer and employee data, including significant amount of credit card data being transmitted and/or stored.
  - Businesses are subject to regulatory statutes designed to protect consumers like the Fair Credit Report Act
  - Businesses are subject to PCI Security Standards/Plastic Card Security Statutes
  - Businesses are frequent targets of litigation following a data breach
- Why Are Standard Insurance Policies Not Enough?
  - General Liability → covers bodily injury and property damage, not economic loss
  - Errors & Omission → covers economic damages resulting from a failure of defined services only, and may contain exclusions for data and privacy breaches.
  - Property Insurance → covers tangible property, which data is not. Loss must be caused by a physical peril while perils to data are viruses and hackers.
  - Crime → covers employees and generally only money, securities, and tangible property. No coverage for third party property such as customer/client data
- Ultimately, whether or not a policy covers the insured is very fact-sensitive:
    - In Hartford Casualty Insurance Co. v. Corcino & Associates, et al., CV 13-3728 GAF (JCx) the U.S. District Court for the Central District of California ruled that there was coverage under a CGL policy for a data breach involving hospital records.
    - In Zurich American Insurance Co. v. Sony Corp. of American, et al., Index No. 651982/11 (N.Y. Sup. Ct.), the Court held that actions taken by a third party hacker was not covered under Sony's CGL policy
- What is the Scope of Cyber Coverage?
  - First Party Coverage
    - Network business interruption: loss of income and extra expense due to network security failure.
    - Intangible property: costs to restore or recreate data or software resulting from network security failure.
    - Breach response/management crisis
    - Cyber extortion
    - Loss of income due to failure of network security
  - Third Party Coverage
    - Wrongful disclosure of Personally Identifiable Information, Protected Health Information, or confidential information in the client's care, custody or control via a computer network or off-line
    - Failure of computer network security to guard against threats such as hackers, viruses, worms, Trojan horses and denial of service attacks whether or not resulting from the provision of professional services

        - Content liability peril such as defamation and infringement of intellectual property rights arising out of websites, marketing and advertising activities.
        - Security or privacy breach regulatory proceedings (including associated fines and penalties).
- Insurance Broker Liability
    - In the majority of states, insurance brokers owe a duty to their clients, which generally consist of using reasonable care, diligence, and judgment in procuring the insurance requested by the insured.
    - Thus, an insurance broker who fails to properly procure the right insurance policy for a client may held liable for any damages that result from same. See Klonis for Use & Benefit of Consol. Am. Ins. Co. v. Armstrong, 436 So. 2d 213 (Fla. 1st DCA 1983) ("[W]here an insurance agent or broker undertakes to obtain insurance coverage for another person and fails to do so, he may be held liable for resulting damages to that person for breach of contract or negligence."); Bennett v. Berk, 400 So. 2d 484, 485 (Fla. 3d DCA 1981) ("An insurance broker may be liable for damages where there is an agreement to procure insurance and a negligent failure to do so."); Caplan v. La Chance, 219 So. 2d 89 (Fla. 3d DCA 1969) (holding that an insurance agent's negligence in failing to procure the proper insurance coverage requested by the insured is a recognized cause of action).