ACC AMERICA
Association of Corporate Counsel
Delaware Valley (DELVACCA) Chapter

DELVACCA PRESENTS

How Our Ideas of Privacy are Changing and Why it Matters

Camille Miller
Chair, Intellectual Property, Cozen O'Connor

Scott Schwartz
General Counsel, Dansko LLC

In the News…

- On March 30, Global Payments, a company that processes credit card transactions, announced that it had experienced a data breach whereby 1.5 million credit and debit card numbers from major credit card companies may have been released
  - Company became aware of the event in early March
  - Already the company is experiencing reputational damage
    - Visa removed it from its preferred credit card processor list
    - Stock down 3.3% in a couple of days
    - Secret Service is investigating the incident
    - Privacy law implications?

Source: CNNMoney

ACC AMERICA
Association of Corporate Counsel
Delaware Valley (DELVACCA) Chapter

Overview

- Protecting Consumer Personal Identifiable Information- Why does it matter?
- A Brief Primer of Federal and State Data Privacy Laws
- Practical Measures to Limit Exposure Before a Security Breach Occurs
- A Data Breach Occurred… now what?
- Questions

ACC AMERICA
Association of Corporate Counsel
Delaware Valley (DELVACCA) Chapter

Protecting Personal Identifiable Information (PII)- Why does it matter?

- First, what is it?
  - Generally defined as any combination of the following:
    - Name; address; telephone number; electronic mail address; fingerprints; photographs or computerize images; a password; an official state or government-issued driver's license or identification card number; a government passport number; biometric data; an employer, student, or military identification number; date of birth; financial information
  - May also include medical information, tax information and/or disability information

ACC AMERICA
Association of Corporate Counsel
Delaware Valley (DELVACCA) Chapter

Protecting Personal Identifiable Information- Why does it matter?

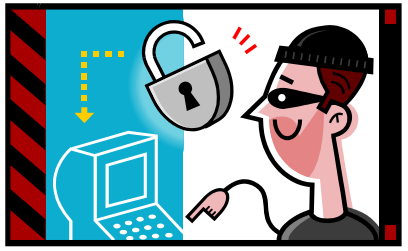
- As new technologies have emerged, consumers have become more aware of the privacy implications associated with their data
  - Consumers have come to expect a greater degree of protection of their private information
    - 2/3 of consumers say they want government to play a larger role in protecting their privacy on the Internet*
- Legal implications and costs associated with a data breach
- Ethical implications

*Source: Consumer Reports

ACC AMERICA
Association of Corporate Counsel
Delaware Valley (DELVACCA) Chapter

ID Theft Victims

- 11.6 million adults in 2011 (increase of 13 percent from 2010)
- Total amount of fraud remained steady
  - About $56 billion annually
- Data breach victims are 9.5 times more likely to be a victim of identity fraud
- Every minute, 28 consumers become victims

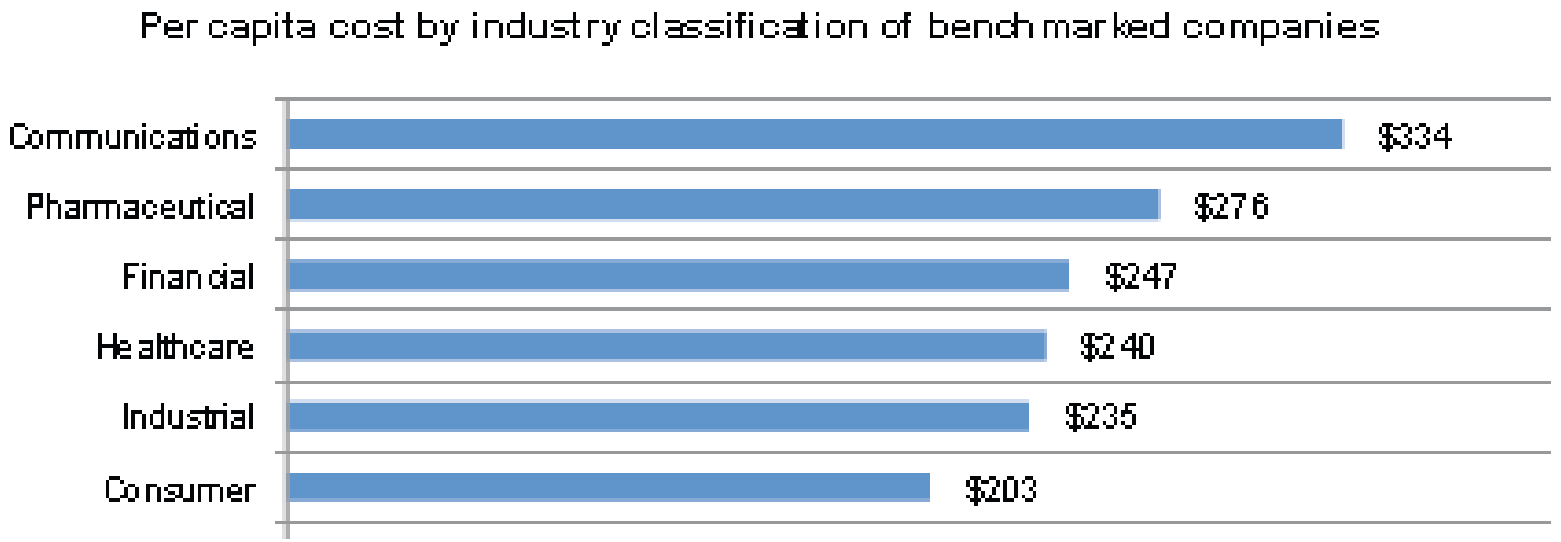


Sources Javelin Strategy & Research
J.D. Power & Associates

ACC AMERICA
Association of Corporate Counsel
Delaware Valley (DELVACCA) Chapter

Legal Implications / Expense

- Cost of data breach in 2011: $5.5 million
  - Cost per record: $194



- Notification costs have increased

Source: Ponemon Institute

ACC AMERICA
Association of Corporate Counsel
Delaware Valley (DELVACCA) Chapter

Civil or Criminal Penalties for Failure to Promptly Notify Customers of Breach

Arizona	Massachusetts	Texas
Arkansas	Michigan	Utah
Colorado	Minnesota	Vermont
Delaware	Montana	Wyoming
D.C.	Nebraska	
Florida	New York	
Hawaii	North Carolina	
Idaho	Ohio	
Kansas	Oregon	
Maine	Pennsylvania	
Maryland	Rhode Island	

ACC AMERICA
Association of Corporate Counsel
Delaware Valley (DELVACCA) Chapter

Case Study: RockYou

- In 2009, RockYou, an online gaming site, suffered a data breach whereby the personal information of 32 million users was exposed. FTC files suit, alleging, *inter alia*:
  - RockYou had misrepresented to its users that it used commercially reasonable safeguards to protect PII of its users
  - RockYou had also collected personal information of over 179,000 children below the age of 13 without parental consent, in violation of COPPA
- RockYou settles with FTC for $250,000 and agrees to other concessions, including maintaining a comprehensive information security program subject to third party audit
- In parallel civil litigation, RockYou settles for $2000 plus $290,000 in attorneys fees and other concessions

Other Examples

- In 2011, the FTC settled with Ceridian and Lookout Services after data breaches occurred to the personal information stored by these companies. The FTC required both companies to, among other things, implement comprehensive security programs and to obtain third party audits every 20 years

- In January 2007, TJX settled with 41 states in a large data breach case. It agreed to pay $9.75 million to settle the dispute

- In 2006, the FTC fined ChoicePoint $10 million after a rather large data breach occurred affecting 160,000 consumer records

A Brief Primer on Federal and State Privacy Laws

- There is no single, comprehensive federal law that governs privacy issues, particularly data privacy issues
  - Sector-based legislature
- State laws offer more comprehensive protection in many instances, but are limited in application to state consumer data
  - Vary by jurisdiction and can be complex
- Generally, Federal and State laws require businesses to maintain adequate data security and destroy data with personally-identifying information

ACC AMERICA
Association of Corporate Counsel
Delaware Valley (DELVACCA) Chapter

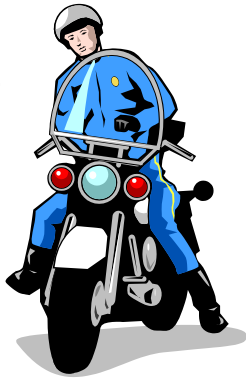
Federal Data Privacy Laws

- Main Federal Laws Governing Data Privacy include:
  - Children's Online Privacy Protection Act (COPPA)
  - Fair Credit Reporting Act (FCRA)
  - Gramm-Leach-Bliley Act (GLBA)
  - Federal Trade Commission Act (FTCA)
  - Health Insurance Portability and Accountability Act (HIPAA)
  - Health Information Technology for Economic and Clinical Health Act (HITECH)

… and others!

Federal Data Privacy Laws

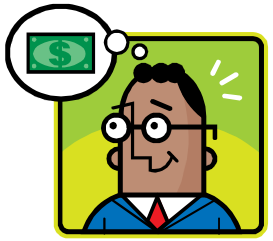
- COPPA
  - Requires any person who operates a commercial web site or online service directed to children under 13 that collects PII from children, or who operates a general audience web site and has actual knowledge of collecting PII from a child, to, *inter alia*:
    - Post a link to a privacy notice regarding its information practices on its home page (with certain information included)
    - Provide notice to parents and request permission to collect such information from a parent
    - Obtain verifiable parental consent from the child's parent before collecting, using or disclosing the child's PII
    - If disclosing to third parties (in most circumstances), obtain a more reliable method of consent



Federal Data Privacy Laws

- COPPA Amendments
  - In September 2011, FTC sought public comment on proposed amendments. These amendments would, *inter alia*,
    - Broaden the definition of "personal information" to include geolocation information and other types of "persistent identifiers" such as tracking cookies
    - Clarify what notice operators must provide parents before collecting the PII of children
    - Add new parental consent mechanisms, such as scanned consent forms, and delete outdated mechanisms such as "email-plus"
    - Strengthen the confidentiality and security provisions of the rule by requiring operators to ensure that third parties or service providers to whom PII is disclosed also implement reasonable procedures to protect this information

Federal Data Privacy Laws



- FCRA
  - Governs privacy requirements for Credit Reporting Agencies (CRAs)
  - Companies must exercise care when destroying consumer reports or information derived therefrom
- GLBA
  - Protects the privacy of consumer information held by financial institutions (defined broadly)
    - Requires financial institutions to protect information collected from individuals and to provide consumers and customers with a privacy notice in certain circumstances
      - Privacy notice must be clear, conspicuous and accurate
      - Must also allow consumers to have a reasonable way to opt out of having information shared with certain third parties
    - Places limits on how third parties can re-disclose non-public financial information

Federal Data Privacy Laws

- FTCA
  - Section 5 prohibits “unfair or deceptive acts or practices in or affecting commerce” and is often used by the FTC as a grounds to enforce an entity’s promises set forth in online privacy policies
  - Businesses must also avoid security practices that create an unreasonable risk of harm to consumer data
  - Examples:
    - Google/Facebook administrative proceedings
    - Chitika case involving advertising network’s alleged deceptive privacy controls
    - Case against W3 Innovations for mobile app violation of COPPA

Federal Data Privacy Laws

- HIPAA
  - Applies to covered entities, namely, health care providers, health plans, and health care clearinghouses generally (exceptions exist) and business associates
  - Addresses the use and disclosure of individuals' identifiable health information
    - Generally prohibits disclosure or use of identifiable health information absent written consent, except in certain circumstances
  - Requires a notice of privacy policy that must meet certain requirements
  - Covered entities must also maintain reasonable and appropriate administrative, technical and physical safeguards on the data
- HITECH
  - Expanded HIPAA's requirements and established security breach notification requirements, among other things

Loss of Laptop Computer Case Study

***Guin v. Brazos Higher Ed. Serv. Corp., Inc.*, 2006 WL 288483 (D. Minn. 2006)**

- Typically, the loss of a laptop containing PII will trigger an inquiry under the Notice of Security Breach Statutes as to whether there is an event that gives rise to notice to consumers
- Facts: Defendant permitted an employee to keep unencrypted nonpublic customer data on a laptop computer that was ultimately stolen from the employee's house
- Defendant was unable to determine which of its customers' information was contained on the laptop
  - Required under California law to give notice to its customers, and sent a notification letter to all of its customers
- Argument: Plaintiff argued that Brazos had breached its security obligations under the GLBA

ACC AMERICA
Association of Corporate Counsel
Delaware Valley (DELVACCA) Chapter

Loss of Laptop Computer Case Study

- Ruling: No liability because:
  - Plaintiff could not show actual loss or damage
  - Even if damage had existed, it would be due to the intervening criminal act of a third party and therefore any damages that resulted would not be foreseeable to Defendant
  - At the time of the burglary Brazos had written security policies, current risk assessment reports and proper safeguards for customers' personal information as required by the GLBA

ACC AMERICA
Association of Corporate Counsel
Delaware Valley (DELVACCA) Chapter

State Privacy Policy Laws

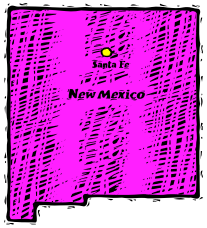
- Vary greatly by state:
  - Certain states require collectors of personal information from such state's residents to adopt and maintain privacy policies. *See, e.g.*, California Business and Professions Code §§ 22575-22579
    - Can vary by type of personal information collected, e.g., social security numbers in Connecticut. *See* Public Act No. 08-167 (requiring any person who collects Social Security numbers in the course of business to create a privacy protection policy that is publicly displayed)
  - Other states adopt more lenient rules. E.g., Pennsylvania makes it a violation for a company to knowingly make a false or misleading statement in a privacy policy, but does not require adoption of a privacy policy *per se*. 8 Pa. Cons. Stat. § 4107
    - Similar to Section 5 of the FTCA

States/Commonwealths/Territories with Data Breach Laws:

Alaska	Louisiana	Ohio
Arizona	Maine	Oklahoma
Arkansas	Maryland	Oregon
California	Massachusetts	Pennsylvania
Colorado	Michigan	Puerto Rico
Connecticut	Mississippi	Rhode Island
Delaware	Missouri	South Carolina
D.C.	Minnesota	Tennessee
Florida	Montana	Texas
Georgia	Nebraska	Utah
Hawaii	Nevada	Vermont
Idaho	New Hampshire	Virginia
Illinois	New Jersey	Washington
Indiana	New York	West Virginia
Iowa	North Carolina	Wisconsin
Kansas	North Dakota	Wyoming

States with No Data Security/Breach Notification Laws

- Alabama
- Kentucky
- New Mexico
- South Dakota



ACC AMERICA
Association of Corporate Counsel
Delaware Valley (DELVACCA) Chapter

State Data Breach Notification Laws

- Generally require written notification to individual(s) in the event of a breach of security
  - Often what matters is where the individual resides, not where the information is stored or outsourced for storage
- States vary in:
  - the definition of what constitutes a breach
  - the definition of personal information (only a few include personal health information)
  - inclusion of a risk of harm standard
  - content requirements for notice
  - authorities that must be notified (and timing)
  - available penalties and private right of action

State Data Breach Notification Laws

- Common Elements Among State Notification Laws
  - Almost all require some form of direct notice unless giving notice would compromise a law enforcement investigation of the security of the system
  - Most also recognize that federal law may preempt these laws in certain industries, particularly the financial industry, and compliance with federal law in many circumstances will be deemed to be compliance with the state laws
  - Many require some form of substitute notice if a company has insufficient contact information for an affected resident. Substitute notice often includes all of the following
    - Sending an email to an affected resident (if a valid email address is known)
    - Posting a notice of the breach on the Company's website
    - Informing statewide media (and/or other agencies) of the breach

Two Examples:

- **California; California Civil Code §§ 1798.80-1798.84**
  - Requires notice sent to individuals if stored, unencrypted PII is compromised
    - Notice requirement is automatic if first name or first initial and last name in combination with certain private information (together) is compromised
      - Private information includes medical and health insurance information
    - If data breach affects over 500 California residents, California Attorney General must be notified
    - Every notice of breach must contain, among other things:
      - A list of the types of personal information subject of a breach
      - The date, estimated date, or date range when breach occurred, if possible to determine
      - A general description of the incident (if available at time notice is provided)

ACC AMERICA
Association of Corporate Counsel
Delaware Valley (DELVACCA) Chapter

Two Examples (cont'd):

- **Pennsylvania; 73 Pa. Stat. Ann. §§ 2302-2308**
  - Requires notice sent to individuals if stored, unencrypted or unredacted PII is compromised
    - Notice requirement is automatic if first name or first initial and last name in combination with certain private information (together) is compromised
      - Private information includes financial information but not medical or health information
    - If data breach affects over 1000 Pennsylvania residents, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis must be notified
    - No statutory requirements for what notice must contain

Exemption for Immaterial Breaches

- Michigan (Mich. Comp. Laws, §§ 445.61 to 445.77)
  - Notification not required if determined that the security breach has not or is not likely to cause substantial injury or result in identity theft
- Louisiana (La. Rev. Stat. Ann. § 51:3074)
  - Notification not required if after a reasonable investigation the entity determines there is no reasonable likelihood of harm to consumers
- *See, e.g.*, Alaska, Iowa, New Jersey, Rhode Island, Vermont

Exemption for Encrypted PII:

Arizona	Minnesota
Arkansas	Montana
California	Nebraska
Colorado	Nevada
Connecticut	New Jersey
Delaware	North Dakota
Florida	Oklahoma
Georgia	Oregon*
Hawaii	Pennsylvania*
Idaho	Rhode Island
Illinois	Tennessee
Indiana*	Vermont
Kansas	Washington
Maine	
Maryland	
Michigan*	

*Exception does not apply if encrypted information is unlawfully taken by a person with access to encryption key

Private Right of Action Available In:

California	New York City
District of Columbia	North Carolina
Hawaii	North Dakota
Illinois	Rhode Island
Louisiana	Tennessee
Maryland	Texas
New Hampshire	Washington

Recent State AG Actions

- In January 2012, Minnesota AG sued Accretive Health, Inc.
  - Stolen laptop containing personal health information
  - Alleges violations of state and federal health privacy laws
- In April 2011, Texas AG and FBI launched a criminal investigation into a data breach that occurred in the Texas comptroller's office
  - Millions of records were posted to a public server
- AG Trends in Remediation
  - Credit Monitoring when not Statutorily Required

Best Practices to Conform to State and Federal Privacy Laws

- Federal Trade Commission recently released a Privacy Framework and Implementation best practices guide
  - Key Recommendations:
    - Incorporate substantive privacy protections into company's practices
    - Maintain comprehensive data management procedures throughout a product's/service's lifecycle
    - Companies do not need to provide choice before collecting and using consumer data for consistent practices
    - For inconsistent practices, companies should offer choice at a time and in a context in which consumer is making a decision about data
      - Obtain consent before using consumer data in a materially different manner
      - Obtain consent before collecting sensitive data for certain purposes
    - Privacy notices should be clear, short and more standardized.
    - Companies should provide reasonable access to data
    - Companies should educate consumers about commercial data privacy

Preventing/Mitigating Liability under Data Breach Laws

- Implement a data security and destruction policy
- Implement a data breach policy and educate employees about it
- Identify applicable federal and state laws
- Identify procedures and practices in event of a breach
  - Have an existing process to monitor whether an incident has taken place
  - Implement internal reporting processes to avoid delays in reporting
- Control access to data.
  - Who has access to data, passwords, etc.?
  - Is there appropriate software and application security?

Preventing/Mitigating Liability under Data Breach Laws

- Test for vulnerabilities to common attacks, or more sophisticated attacks, for high value data
  - Monitor network security
    - Examine network architecture, the monitoring process for intrusions and inappropriate use, assess firewalls, remote access and virus scan policies, etc.
  - Consider screening personnel
- Assess confidentiality agreements/NDAs that are in place, employee training regarding security, and the steps in place to retrieve confidential information
  - Consider physical security (badges, identification documents, etc.)

Preventing/Mitigating Liability under Data Breach Laws

- Adopt a privacy policy that clearly sets forth data breach notification policies and procedures and stick to it
  - Many states have exemptions to data breach notification statutes if a business acts consistently with its own information security policies
- And finally… ENCRYPTION!
  - Encrypt all personal information and securely store encryption keys
    - FTC Safeguards Rule (for the GLBA) requires certain encryption technologies be implemented by financial institutions
    - HIPAA Security Rule requires encryption when certain health information is sent over a network
    - Many state data breach laws only cover loss of unencrypted data (or encrypted data with key)

Best Practices in the Sale or Licensing of Personal Information

- In any contract licensing use of PII:
  - Limit use, sale and disclosure of PII to the extent possible, based on the type of PII at issue
    - i.e., Licensee shall keep confidential and not disclose to any third party Personal Identifiable Information (PII), except as needed to perform its obligations under this Agreement. To the extent Licensee discloses its information to any third party as stated hereunder, Licensee agrees to contractually require (in writing) such third party to protect such PII using at least the same degree of care as Licensee is obligated under this Agreement.

Best Practices in the Sale or Licensing of Personal Information

- Require Licensee to take all commercially reasonable actions to prevent the unauthorized use, disclosure, copying or reproduction of PII
  - Consider requiring Licensee to implement certain specific kinds of data protection policies or technological measures (i.e., hardware/software) or to encrypt the PII
- Require Licensee to notify Licensor immediately when there is a data breach that involves or may involve the PII
- Restrict sublicensing / reproduction of licensed PII

Best Practices in the Sale or Licensing of Personal Information

- Indemnification
  - Be sure to include an indemnification that covers all costs associated with a data breach
    - Make sure that Licensee is also required to extend the indemnification to any third parties to whom Licensee discloses PII
  - Sample Indemnification Language:
    - Licensee hereby agrees to indemnify, defend, and hold harmless Licensor, its officers, directors, employees, and affiliates, from any and all costs, including notification costs, damages, liabilities, fees, including reasonable attorneys fees and costs, expenses and/or penalties associated with (a) any unauthorized disclosure, release or collection of PII licensed to Licensee under this Agreement by Licensee or any third party and (b) any unauthorized disclosure, release or collection of PII in the possession, custody or control of a third party, to the extent Licensee authorized such third party to use, store, maintain, manage, or otherwise possess such PII.

Best Practices in the Sale or Licensing of Personal Information

- Consider including a provision requiring Licensee to comply with any applicable security provisions required by State or Federal law
  - Massachusetts regulations, for example, require licensors to contractually require service providers to comply with data security provisions in certain security breach regulations

- In any contract involving the sale of PII:
  - Ensure that the purchaser agrees to hold seller harmless for any costs associated with any breach of PII that occurs after the sale/transfer of data
    - Make sure seller holds purchaser harmless for any data breaches that occurred prior to sale/transfer of data

Best Practices in the Sale or Licensing of Personal Information

- Be aware that certain laws restrict the sale and/or disclosure of certain information
  - Ex. Sec. 13405 of HITECH Act restricts sale of protected health information in certain circumstances
  - Ex. 18 U.S.C. § 2721 restricts the resale of certain personal information received from a State department of motor vehicles
  - Bankruptcy Code 363(b)(1) restricts the sale of PII if debtor disclosed a policy prohibiting transfer to third parties and policy is still in effect at the time of bankruptcy case
- Purchaser may wish to obligate seller to ensure that seller has destroyed or will destroy all applicable PII, once such data has been transferred to purchaser

Best Practices in the Sale or Licensing of Personal Information

- Consider who is liable for data breach / responsible for notification during any transitional periods of ownership
- Contemplate including a schedule listing any third parties to whom seller licensed or disclosed PII
  - Include any associated agreements
- Make sure seller lists all of the various types of PII collected
  - Need to know what data is in your possession if a breach actually occurs
- Hire counsel to review any such agreement

What to do When a Data Breach Occurs

- Be Prepared!
  - Pre-incident planning and a good crisis management team can drastically alleviate headaches and prevent the “chicken with its head cut off” syndrome
  - Crisis Management Team (CMT) anticipates and plans in advance what may happen in a breach scenario
    - A controlled, internal process is put into place
    - Determine who is impacted, can help solve the problem and who needs to know
    - Recruit these folks onto the CMT
    - Develop response plans internally and drill with external CMT members
    - Hold regular complete drills
    - Compile a master list of experts—either responders or advice givers—determine whether they need to be contacted or contracted with pre-crisis

What to do When a Data Breach Occurs

- Crisis Management (cont'd)
  - Internal
    - Recruit the CMT by both "job description" and current holder of the job. All possible methods of communication should be included. Alternates should be named in case contact is not made. Should anyone else be included?
    - Name the sole spokesperson for all communications. This should be a professional who is skilled at preparing and presenting talking points
      - Internal communication requirements should be determined when the CMT is determined
      - Email distribution lists should be established ahead of time for smooth flow of communications
    - Do not include CEO on the CMT

What to do When a Data Breach Occurs

- Crisis Management (cont'd)
  - External
    - The named spokesperson is the only person who deals with the media!
    - Stakeholder list must be compiled pre-incident
      - Councilperson
      - State Representative
      - Mayor
      - Other Elected Officials
      - Customers
      - Directly Impacted Folks
      - Local, State and Federal Agencies
      - Insurance Brokers and Carriers
      - All the Individuals who have been Drilled
    - How and how often you will need to reach out to people should be determined pre-incident

What to do When a Data Breach Occurs

- Post-Breach
  - Gather Information
    - Data Breach Notification Laws . . . Key is to know the extent of the breach
    - Respond when ready but do not drag your heels
    - Brief a company spokesperson on how to respond
    - Bring in consultants if necessary
      - NDA and other contracts should already be in place
  - Contact Appropriate Stakeholders
    - The fewer surprises, the better
  - Preserve Evidence
    - To determine a root cause analysis at a later date

What to do When a Data Breach Occurs

- Be Ready for Customers' Questions / Preempt their Concerns
  - Adopt an apologetic air, but do not admit liability
  - Be transparent and let customers know the actions you are taking
  - Offer remedial actions to customers (i.e., free credit reports for a year, etc.)
- Attempt to Enforce any Indemnification Provisions (to the extent applicable and available)
  - Don't wait- notify applicable parties immediately
- Quick, Focused Response is Key to Mitigating Costs Associated with a Breach

Questions?