Preparing For and Responding To Data Breaches

A Webinar Presented by Dechert LLP

November 18, 2015

Dechert LLP

Today’s Presenters

Timothy C. Blank

Partner

Boston

timothy.blank@dechert.com

+1 617 728 7154

Hilary Bonaccorsi

Associate

Boston

hilary.bonaccorsi@dechert.com

+1 617 728 7153

Program Overview

- **Before a Data Breach**
  - Know the Law
  - Have a Comprehensive Information Security Program
  - Put Key Relationships in Place
  - Designate an Internal Expert
  - Negotiate Strong Contracts
  - What Will Regulators Really Want to Know?
- **Discovering a Data Breach**
  - Stop the Attack, Activate Team, Escalate Issues to Senior Management as Needed
- **After a Data Breach**
  - Assess Impact and Conduct Forensic Examination
  - Determine Notice Obligations
  - Consider Contractual Obligations and Examine Privacy Notices
  - Prepare an Incident Report
- **Understanding Potential Claims**

Terminology Lesson

- Cybersecurity – refers to protecting the nation's or a corporation's "critical infrastructure" (banking, power, defense, transportation) from attacks by foreign governments, terrorist organizations, or cyber criminal enterprises.

- Data Protection/Data Breach - refers to protecting personally identifiable information ("PII") such as name, address, SSN and/or account numbers.

- Data Privacy – refers to fast growing practice of hundreds of companies that collect highly personal information about you from website and internet use, to use (or to sell to others to use) for marketing additional products and services to you.

  - Online activities
  - Political views
  - Health worries
  - Shopping habits
  - Travel plans

Different Kinds of Data Losses

- By Mistake
  - Most common
  - Mistaken “authorized” access
  - Lost or stolen laptop
  - Lost FedEx package
  - Incorrect email attachment
- By Theft – “money is the goal”
  - Anthem
  - Target
  - Staples
  - JP Morgan
  - Home Depot
  - Sony Playstation
  - BJ’s Wholesale
  - TJ Maxx
  - IRS Refund Scam
- By “Attack”
  - For economic, military or political gain
  - Perpetrated by foreign governments, commercial competitors or terrorist organizations

Before a Breach

Before a Breach: Know the Law

Understand the Scope of the Data Protection and Data Breach Statutes

- **In General:**
  - If you collect "personally identifiable information," you need a privacy program
  - Varies (state by state), but generally consists of first name (or first initial) plus last name, in combination with one or more data elements
    - Social Security Number
    - Driver's License Number
    - Account Number (with access code)
    - Credit card number
    - Medical information
  - Information about a company or other institution, is not "personally identifiable information."
- **Industry – Specific:**
  - Any "financial institution" that obtains "nonpublic personal information" from its "customers" needs a privacy program. (Reg. S-P)
    - Potentially broader in scope
  - HIPAA regulates the use and disclosure of "protected health information" by "covered entities."
  - Others

Before a Breach: Know the Law
Federal Statutes & Regulations (Examples)

- FTC Act Section 5
- Title V of the Gramm-Leach-Bliley Act of 1999
  - SEC's Regulation S-P
  - FTC Privacy of Consumer Financial Information Rule ("FTC Privacy Rule")
  - FTC Standards for Safeguarding Customer Information ("FTC Safeguards Rule")
  - SEC's Regulation S-AM
- Red Flags Rule
- Health Insurance Portability and Accountability Act (HIPAA) of 1996
- Fair and Accurate Credit Transactions Act (FACTA) of 2003
- Fair Credit Reporting Act (FCRA) of 1970

Before a Breach: Know the Law
State Statutes (Examples)

- State Data Protection Laws
  - Massachusetts Standards for the Protection of Personal Information
- State Breach Notification Laws
  - 46 state laws plus the District of Columbia
- State Opt In/Opt Out Laws
- State Disposal Laws
- State Social Security Number Laws
- State Encryption Laws

Before a Breach: Know the Law
Understand the Basis For Liability

- FTC Act Section 5
- SEC/FTC Enforcement Actions
- Litigation
  - With individuals / class actions
  - With credit card issuers
  - With insurance companies
  - With shareholders / investors under securities laws
- State AG Enforcement Actions

Before a Breach:
Have a Comprehensive Information Security Program

- Written Information Security Program
- Incident Response Plan
- Privacy Notice*
- Industry-Specific Policies (*e.g.*, Red Flags Program)*
- Online Privacy Policy*

** Discussed in Dechert's September 29, 2015 Data Privacy and Cybersecurity Group webinar on Designing Privacy Policies and Identifying Privacy Risks for Financial Institutions.*

Before a Breach:
Have a Written Information Security Program ("WISP")

- **Model: Massachusetts Standards for the Protection of Personal Information**
  - Most firms use the Massachusetts statute as the model, but there are other state statutes addressing data security (*e.g.,* California)
- Under Massachusetts law, any company that owns or licenses personal information about a resident of Massachusetts must meet certain minimum standards with respect to the safeguarding of personal information (in both electronic and paper form)
- **Objectives of Statute:**
  - Insure the security and confidentiality of customer information in a manner fully consistent with industry standards
  - Protect against anticipated threats or hazards to the security or integrity of such information
  - Protect against unauthorized access to or use of such information that may result in substantial harm or inconvenience to any consumer

Before a Breach:
Have a Written Information Security Program ("WISP")

- **Model: Massachusetts Standards for the Protection of Personal Information**
- Must develop, implement and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains
  - Administrative;
  - Technical; and
  - Physical safeguards.
- Must be appropriate to:
  - The size, scope and type of business;
  - The amount of resources available;
  - The amount of data stored;
  - The need for security and confidentiality of both consumer and employee information.

Before a Breach:
Have a Written Information Security Program ("WISP")

Administrative Safeguards

- Designate employee to maintain information security program;
  - At least annual review of Program; Monitoring security Program
- Identify and assess reasonably foreseeable internal and external risks;
- Develop security policies for employees accounting for which employees have access to information
- Employee training and employee disciplinary procedures
- Third Party Service Provider Verification
  - Critical component; major source of vulnerability
  - Contracts are often inadequate

Before a Breach:
Have a Written Information Security Program ("WISP")

Technical Safeguards

- Numerous technical requirements including:
  - Secure user IDs and other identifiers;
  - Secure access control measures;
  - Encryption of both (1) laptops, and (2) other portable devices;
  - System monitoring;
  - Firewall protection;
  - Up-to-date patches and virus definitions; and
  - Education and training
- Conduct gap analysis – inventory all current I.T. procedures and identify any deficiencies

Before a Breach: Have an Incident Response Plan

- An incident response plan details, in writing, a concrete plan for what a company will do if it faces a suspected or actual data breach or cyber-attack. The plan should, at a minimum:
  - Identify the company's most vulnerable data;
  - Assign responsibility for each element of the response plan and provide 24-hour contact information for all personnel and back-up personnel, including a rapid response team
  - Explain how to determine whether an incident is actually a breach and whether and how it should be escalated;
  - Indicate that data should be preserved so a forensic investigation can be conducted;
  - Identify who will keep logs and records of all information relating to the incident; and
  - Include procedures for notifying law enforcement and criteria for whether customers or third-parties need to be notified.
- Incident response plans should be tested
  - Personnel need to be trained and know how to respond to a data breach or cyber-attack.

Before a Breach: Industry-Specific Requirements

Red Flags Rule: Triggers

- "Financial Institution" is a bank, credit union, or any other person that holds a "transaction account"
  - "Transaction Account" is generally considered a deposit or account on which the depositor or account holder is permitted to make withdrawals
- "Creditor" is defined broadly as any entity or person who regularly arranges for, extends, renews or continues credit
  - Interpreted expansively; includes any situation in which services or goods are provided prior to receipt of full payment
  - Creditor may include lenders such as banks, brokers, finance companies, auto dealers, mortgage brokers, utility companies, telecommunications companies, and professional services providers
- "Covered Account" is an account primarily for personal, family, or household purposes that is designed to permit multiple payments or transactions; or any other account for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft

Before a Breach: Industry-Specific Requirements
Red Flags Rule: Overview

- The Red Flags Rule requires “financial institutions” and “creditors” to:
  - Establish a written, board approved Identity Theft Program;
  - Identify “red flags” of identity theft – any “pattern, practice, or specific activity that indicates the possible existence of identity theft”;
  - Detect “red flags”;
  - Prevent and mitigate identity theft;
  - Update the Identity Theft Program; and
  - Administer the Program.
- Guidelines suggest oversight of the Program by the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management.

Before a Breach: Make Sure Key Relationships Are in Place

- Form relationships before a breach with:
  - Legal counsel
  - Forensic experts
  - Insurance providers
  - Public relations professionals
  - Human resources experts (if internal)

Before a Breach: Designate an Internal Expert

- Appoint a Chief Information Security Officer (“CISO”) who understands your business, data flows and risks

- Make updates on information security and data incidents a recurring Board Agenda item

Before a Breach: Negotiate Strong Contracts

- Conduct due diligence with regard to vendor selection
- Hold vendors and service providers to the same legal standard
- Require vendors and service providers to provide notice of security breaches
- Supervise and monitor vendors' and service providers' compliance

Before a Breach: Always Have These Questions in Mind:

1. Do you truly understand your firm's cybersecurity infrastructure?

2. Have you enacted policies and internal procedures specifically tailored to your risks?

3. Can you prove - - with documents - - that you adhere to and enforce your own policies?

   Can you detect - - in real time - - any unlawful access to your firm's data networks?

   Are you actively monitoring and minimizing the risks associated with your third party vendors and service providers?

Discovering a Breach

Discovering a Breach

- Stop the attack / intrusion / information loss
- Activate team
  - Preserve critical evidence with proper forensics
  - Ensure proper documentation of investigation
  - Designate primary contacts (internal and external)
- Escalate issues to senior management as needed

After a Breach

After a Breach: Initial Steps

- Alert legal counsel
- Assess impact
  - When did the attack happen? For how long?
  - How did it happen?
  - What data was lost/disclosed? Was it encrypted?
- Forensic snapshot
- Conduct investigation
  - Gather evidence
- Notify cyber insurance carrier

After a Breach: Determine Notice Obligations

- 46 states + D.C. have data breach notification laws.
- Generally, a company must notify the affected consumer when there is a “breach of security.”
- A “breach of security” is ordinarily defined as “an unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information.”
- Each state law is different, and therefore you must analyze each statute to ensure compliance.

After a Breach: Determine Notice Obligations

Differences in State Data Breach Notification Laws

1. Definition of “Personal Information”
2. What is a “triggering event” (numerical thresholds, risk calculation)
3. Timing of notice (“following discovery”, no later than “10 days”, “as soon as practical”)
4. Content of notice
5. Recipients of notice (agencies, individuals, data “owners”)
6. Means of notice (who sends?)
7. Penalties, private right of action

After a Breach: Determine Notice Obligations

Notification Triggers

- "**Personal Information**" is usually defined as an individual's first name or first initial and last name in combination with:
  - Social security number;
  - Driver's license number or state issued identification card number;
  - Account number, credit or debit card number; or
  - Medical information –
- Breadth of Definitions Vary
  - North Dakota requires notice when name + date of birth or mother's maiden name is disclosed
  - Updates include "unique biometric data" and username + password
- Tricky Issues
  - "Partial Social Security Numbers" (also: SSN protection laws)
  - Account numbers, with or without password or PIN code

After a Breach: Determine Notice Obligations

Notice Content

- Required content of notice also varies by state.
- Most states require the consumer notification to include a general description of the data breach.
  - But not all: Massachusetts explicitly prohibits inclusion of such information.
- Some states require information on how to put in place a credit freeze and how to monitor account statements for fraud.
- AG contact information or FTC contact information must sometimes be included.

After a Breach: Determine Notice Obligations
Notice Timing

- Timing of notice varies by state:
  - "following discovery"
  - "the most expedient time possible"
  - "no later than 30 days."

- Some states require notice to be provided to the AG's office before consumers are notified

After a Breach: Determine Notice Obligations

Who to Notify

- Generally, you will provide notice to the consumer
  - But, states do distinguish between entities that “own” data, versus those that “maintain or possess” information
  - Can result in notice to the data “owner”
- States may require notification to the AG, or Office of Consumer Affairs, or State Police, and/or equivalent.
  - Some states use numerical thresholds before mandating notification.
- Some states may require notification to Credit Monitoring Agencies (generally when a numerical threshold is reached)

After a Breach: Determine Notice Obligations
Who Sends the Notice?

- Biggest issue often centers around who sends the notice – the “data owner”

- Clients feel strongly – both ways

After a Breach: Determine Notice Obligations
Look for "Safe Harbors"

- Most states allow for a "risk of harm" analysis to determine whether notice is required
  - "Notice is not required if there is not a reasonable likelihood that harm to consumers has or will result."
  - "The breach must create a substantial risk of identity theft or fraud."
  - Some states require a written determination; may need to be sent to the state AG
- Many states have an "encryption" safe harbor

After a Breach: Notification Obligations
Key Takeaways

- State data breach statutes are constantly changing and definitions of what constitutes “personal information” are evolving
- Each data incident is very fact-specific; important to conduct a careful facts and circumstances analysis of notice obligations for each incident
  - Get guidance on gray areas—sometimes the data breach statutes will not contemplate your set of facts
  - Consider the “value” of the data at issue and the level of risk

After a Breach: Monitor Potential Uniform Federal Law Regarding Notice Obligations

- Faced with a patchwork of 46 state data breach notification laws (plus the District of Colombia) members of Congress have put forth at least 10 federal data breach reporting bills to streamline the process.

- The bills that have received the most attention include:

  - **The Data Security and Breach Notification Act of 2015 ("Blackburn Bill")**
    - Introduced by House Representative Marsha Blackburn April 2015
    - Referred to the Subcommittee on Commerce, Manufacturing, and Trade April 2015
  - **The Personal Data Notification and Protection Act of 2015 ("Obama Bill")**
    - Proposed by the White House, introduced by Representative James Langevin March 2015
    - Referred to the Subcommittee on the Constitution and Civil Justice April 2015
  - **Consumer Privacy Protection Act** ("Leahy Bill")
    - Introduced by Senator Patrick Leahy April 2015
    - Referred to the Committee on the Judiciary April 2015

- These three bills have gained traction, and there are other variations of the bills that are pending

After a Breach: Monitor Notice Obligations

- How are the proposed bills similar?
  - All contemplate a single federal statute to govern data breach reporting
  - All vest enforcement authority in the FTC and state attorneys general
- How are the proposed bills different?
  - The Blackburn Bill would:
    - Trigger a notification requirement for fewer types of personal information than most existing state laws (and would preempt state law)
    - Require companies to notify consumers only if they determine there is a "reasonable risk" of "identity theft, economic loss or economic harm, or financial fraud"
  - The Obama Bill would:
    - Target only businesses that work with the personal information of over 10,000 customers over a 12-month timeframe
    - Define "personal information" more broadly to include, for example, unique biometric data and account identifiers
  - The Leahy Bill would:
    - Require disclosure for breaches that impact social networks and cloud email services
    - Create seven new categories of "protected information," including health information, geolocation data, and password-protected private videos and photos

After a Breach: Consider Contractual Obligations

- Even if a company is not required to notify consumers under the state data breach notification statutes, it may still be required to notify other parties with whom it has contractual agreements

- **Notice Provisions.** If a party to this Agreement becomes aware of any **actual or suspected loss** of, unauthorized access to, or unauthorized use or disclosure of any Confidential Information of the other party, including any Personal Information covered by this Agreement, **such party promptly shall, at its expense: (a) notify the other party in writing; (b) investigate the circumstances relating to such actual or suspected loss or unauthorized access, use or disclosure;** (c) take commercially reasonable steps to mitigate the effects of such loss or unauthorized access, use or disclosure and to prevent any reoccurrence; (d) provide to the Owner such information regarding such loss or unauthorized access, use or disclosure as is reasonably required for the Owner to evaluate the likely consequences and any regulatory or legal requirements arising out of such loss or unauthorized access, use or disclosure; and **(e) cooperate with the Owner to further comply with all relevant laws, rules and regulations**

After a Breach: Consider Contractual Obligations

- Companies should review their agreements for privacy clauses to determine the full scope of their exposure and obligations

- **Privacy Clauses / Compliance Provisions**

  - Each party agrees to **comply with the requirements of Title V of the Gramm-Leach-Bliley Act** and any regulations adopted thereto, as well as any other applicable federal or state privacy laws and regulations. **Each party agrees that it will not disclose nonpublic personal information received in connection with this Agreement to any other party**, except to the extent required to carry out the services in this Agreement.

- **Indemnity Provisions**

  - If you agree to comply with applicable privacy laws, some types of data losses (for example, mistaken authorized access) could mean you're liable for the costs associated with the breach.

After a Breach: Examine Privacy Notices

- Privacy notices may be construed as “promises” to consumers

- Among **our top priorities is keeping your Personal Information secure**. We use Secure Sockets Layer (SSL) technology to **encrypt all of your Personal Information** before it is transmitted to us so that it can be safeguarded as much as possible from being read or recorded as it travels over the Internet. **The computers that store your Personal Information are located in a separate facility which employs firewall and security technology.** We employ these procedures to protect your Personal Information from unauthorized access, destruction, use, modification or disclosure.

- **We screen and reasonably determine to be reputable any third party to whom we disclose such information and we require such third parties to agree to use the Personal Information only for such specified purposes.** Each of our partners must agree to implement and maintain reasonable security procedures and practices appropriate to the nature of your Personal Information in order to protect your Personal Information from unauthorized access, destruction, use, modification or disclosure.

- We **share** your personal information **only with our affiliates.**

After a Breach: Prepare an Incident Report

- The incident report should be prepared in consultation with legal counsel
- The incident report should:
  - Describe the incident, including specific dates & times
  - Categorize the types of people impacted (consumers, employees)
  - Explain who investigated the incident and the results of the investigation (with supporting documentation)
  - List all root causes of the incident
  - Identify the business, legal and regulatory risks
  - Address whether notifications were sent
  - Set forth “lessons learned” and plans for remediation

After a Breach: Examine Materiality

October 2011: SEC Issues Guidance on Cyber Attack Disclosure Obligations of Public Companies

- Guidance makes clear that disclosure of "cyber security risks" and "cyber incidents" may be required if "material"
  - Risk Factors
  - MD&A
  - Description of Business
  - Legal Proceedings
  - Financial Statements
- Disclosure obligations apply both "prior to" and "during and after" a cyber incident
- Give thought to how much detail you want to include
  - Too much detail can essentially provide a "roadmap" to hackers of your vulnerabilities

After a Breach: Consider Sharing Threat Information

- The Cybersecurity Information Sharing Act of 2015 ("CISA")

- Encourages the sharing of cybersecurity threat information among private companies and between the private sector and the government
  - Provides companies with protections, including immunity from lawsuits, as an incentive to share information

- Update:
  - The Bill passed in the Senate and corresponding legislation was passed by the House
  - Differences between the House and Senate bills must be ironed out before final conference passage
  - President Obama has endorsed and is expected to sign the final bill

Understanding Potential Claims

Understanding Potential Claims
FTC Actions

- Section 5 of the FTC Act prohibits “unfair or deceptive acts or practices in or affecting commerce.”
- FTC punishments vary and can include:
  - Implementation of comprehensive information security programs;
  - Audits conducted by independent third-party security professionals for an extended term;
  - Large monetary civil penalties;
  - Large “consumer redress” penalties;
  - Record keeping provisions; and
  - Reporting provisions to allow the FTC to monitor compliance.

Understanding Potential Claims

SEC Charges Investment Adviser with Failing to Adopt Proper Cybersecurity Policies and Procedures Prior to Breach

- SEC released an Order regarding a settlement with R. T. Jones in connection with its alleged violation of Rule 30(a) of Regulation S-P (the "Safeguards Rule").
- **Alleged Facts:**
  - For approximately 4 years, R. T. Jones—an SEC-registered investment adviser with 8,400 client accounts and $480 million in assets under management–stored sensitive personally identifiable information ("PII") of clients and other persons on its third party-hosted web server.
  - R.T. Jones did not adopt written policies and procedures regarding the security and confidentiality of that information and the protection of that information from anticipated threats or unauthorized access.
  - In July 2013, the firm's web server was hacked and the PII over more than 100,000 individuals, including thousands of R.T. Jones's clients, was left vulnerable to theft.
  - R.T Jones retained more than one cybersecurity consulting firm to confirm and assess the attack. Neither could confirm whether the PII stored on the server had been accessed or compromised.
  - R.T. Jones notified the affected individuals and provided free identity monitoring.
  - At the time of the Order, there was no indication that any client has suffered actual financial harm as a result of the breach.
- **SEC Findings:**
  - R.T. Jones failed to adopt any written policies and procedures reasonably designed to safeguard its clients' PII as required by the Safeguards Rule. R. T. Jones's policies and procedures did not include, for example:
    - Conducting periodic risk assessments;
    - Employing a firewall to protect the web server containing client PII;
    - Establishing procedures to respond to a cybersecurity incident; or
    - Encrypting client PII.

Understanding Potential Claims

Remijas v. Neiman Marcus Group, LLC

- In 2013, hackers attacked Neiman Marcus. Approximately 350,000 credit cards were exposed to the malware. Some customers found fraudulent charges on their cards.
- Several customers filed class-action complaints, alleging negligence, breach of implied contract, unjust enrichment, unfair and deceptive business practices, invasion of privacy and violation of multiple state data breach laws.
- The federal district court (N.D. Ill.) dismissed for lack of Article III standing.
- Seventh Circuit held the plaintiffs did have standing because they suffered injuries associated with resolving fraudulent charges and protecting against future identity theft.
- The court explicitly refrained from deciding whether the mere loss of private information sufficed as an Article III injury.

Understanding Potential Claims

In re: Target Corporation Customer Data Security Breach Litigation

- In 2013, Target experienced a data breach that impacted payment card information of tens of millions of shoppers.
- The lawsuits regarding the Target breach were separated into two “tracks”: one for consumers and one for financial institutions.
  - Earlier in 2015, the consumer action settled.
  - The financial institution action continues.
    - These were institutions that issued payment cards to customers who had been victims of the breach.
    - They sued to recover losses suffered in remediating the damage experienced by their cardholders (*e.g.*, reimbursing for fraudulent charges and reissuing cards).
- In September 2015, the US District Court in Minnesota certified a class.

Q&A Session

Additional Resources: Dechert OnPoints

- September 28, 2015: SEC Cybersecurity Examinations and Enforcement: What Broker-Dealers and Investment Advisers Need to Know
- May 15, 2015: U.S. SEC Division of Investment Management Issues Cybersecurity Guidance
- April 6, 2015: President Obama Issues New Executive Order Authorizing Sanctions Against Cyber Attackers
- March 26, 2015: The Evolving U.S. Cybersecurity Landscape – What Firms Want to Know
- April 22, 2014: SEC Staff to Conduct Broker-Dealer and Investment Adviser Examinations Focused on Cybersecurity
- April 23, 2013: SEC and CFTC Issue Identity Theft Red Flags Rules Applicable to Institutions and Creditors

Thank You

For further information, visit our website at **dechert.com** or contact any of today's presenters.

Dechert LLP