Security Breaches: Best Practices/Lessons Learned

Peter McLaughlin, Foley & Lardner LLP
Tim Olson, Experian
Andrew Serwin, Foley & Lardner LLP
John Tucker, Foley & Lardner LLP

April 16, 2009
9:00 a.m. – 10:00 a.m. PT

Housekeeping

- We will take questions throughout the program via the Q & A tab located on your menu bar at the top of your screen and live questions at the end of the program.

- Foley will apply for CLE credit after the Web conference. If you did not supply your CLE information upon registration, please e-mail it to mlopez@foley.com.

- Today’s program is being recorded and will be available on our Web site.

- For audio assistance please press *0.

- For full screen mode, go to “View” on your toolbar and select “Full Screen” or press F5 on your keyboard.

- Materials can be found on our Web site at www.foley.com/fridayfocus or by clicking the printer icon on the bottom right hand side of your screen.
Agenda

- Defining the Problem
- Challenges to Effective Responses
- Prevention and Mitigation
- What’s on the Horizon
Defining the Problem

- Legal Issues: addressing statutory requirements, privacy rights and potential lawsuits

- Business Issues: often times at least as critical as the legal issues with concerns re impact on business reputation, processes, customer relations, etc.
Why do These Incidents Occur?

- Sometimes completely accidental

- Sometimes related to identity theft -- the fastest growing crime in the United States
  - Stolen or fraudulently-acquired personal information enables identity theft
  - Black market for identity theft
  - Most sensitive data is social security number, financial information (including credit card #s), health information, passwords, pin numbers, etc.
How Much in Losses are We Really Talking About?

- To an individual

- To a company, one example is:
  - A bank that issues a credit card may be compelled to monitor, cancel, and reissue that card
  - Estimates range between $10 and $50 per card
  - Multiply by number of cards involved

What Type of Data Presents Privacy and Security Issues?

- Confidential Information

- Intellectual Property

- Personally Identifiable Information
  - Health
  - Financial
  - Other data that reveals sensitive information about individuals by itself or if combined with other information
**Notable Examples: ChoicePoint**

- February 2005 allegation: Identity thieves posed as legitimate customers to access company’s extensive consumer profile database
- FTC reportedly investigated company’s compliance with federal law
- SEC reportedly investigated insider trading and adequacy of disclosures
- Secret Service, FBI and U.S. Postal Service involved
- Six class-action lawsuits filed in CA and GA

---

**Notable Examples: DSW Shoe Warehouse**

- March 2005 Allegation: Data from 1.4 million credit cards used in 108 stores was reportedly stolen between November 2004 and February 2005
- Federal authorities, including Secret Service, investigated
- DSW established special help line for its customers
- Parent company disclosed the matter in a 10-K/A and 8-K filed in April 2005
- Disclosures occurred in the midst of parent’s planning for the IPO of DSW
- Head of FTC, Deborah Platt Majoras, was among affected DSW customers
Notable Examples: Heartland

- Late 2008: 100 million card transactions/month for 175,000 merchants
- Attack occurred while PCI review under way
- Heartland uncovered malware (the data-sniffing kind) that allowed thieves to capture credit or debit-card numbers, expiration dates, and in some cases the cardholder’s name.

Not Just U.S. —

- Undercover reporter for British Tabloid, Sun Newspaper, alleged Indian call center employee of Infinity eSearch sold personal data on 1,000 British customers for $5.40 apiece. (June 2005)
- Australian Television Program, Four Corners, reported on “black market in information held by Indian call centres” with information available at $10 apiece
- UK & Germany
Challenges to Effective Responses

Challenge #1

When must notice be given?
Security Breach Notification Laws

- Enacted in 44 States (including NY, FL, PA, CA and IL)
- Generally, requires notice to affected individuals in the event of a breach in the security, confidentiality, or integrity of computerized personal information
- Typically does not apply to encrypted information (unless encryption key is compromised)
- Applies even if there is simply a reasonable belief that there was an acquisition of data

State Identity Theft Laws

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

- What good is encryption?

- Electronic v. non-electronic
  - North Carolina’s law applies to non-electronic

- Is there a general duty?

- Is notice required if there is no likelihood of identity theft?

Challenge #2

How quickly must notice be given?
Challenge #3

Who must be notified?

Who Must be Notified

- Affected individuals
  - Standard
  - Employees?

- Government / law enforcement?
  - Federal
  - State

- Business partners?
  - Pennsylvania: Specifically states that service provider to provide notice to its customer who in turn notifies individuals
  - Florida: Requires notice to business partners for which you maintain personal information

- Credit bureaus?

- Insurance company?
Challenge #4

What form of notice must be given?

Notice and More

- Letter via US First Class mail

- Many AGs, Consumer Groups, and Class Action Litigators pressure for more than just notice
  - Two or more years of credit monitoring are a typical requirement
  - Going beyond the minimum notification requirement is a good step to ward off class action and AG scrutiny
Prevention and Mitigation

Potentially Relevant Policies

- Privacy policies
- Employee policies
- Business partner policies (e.g., contract policies)
- Document retention policies (e.g., destruction of records containing sensitive personal information)
- Incident response policies
Prevention

- Technologically
  - Protect your systems
  - Work with (certified) vendors and other parties like Visa
    - Visa’s information security standards
    - ISO 17799 Information Security Programs

- Contractually
  - Two key contracts are merchant bank and POS vendor
  - Require certifications as a condition

- Internally
  - Implement appropriate policies
  - Educate employees about handling inquiries

What is “Reasonable Security”?  

- Legislative history says there are no specific mandates; no bright lines
  - States there will be “compliance uncertainty”
  - Goal is to allow industry to exercise its own judgment

- “Reasonable” measures must be “appropriate to the nature of the information”

- This obligation expressly applies to contracts involving data sharing
The FTC & States

- FTC Enforcement Actions reflect the FTC’s view of “reasonable security”

- California, Massachusetts, others...

Service Providers & Outsourcing

- Many outsourcing relationships involve the sharing of sensitive data

- An increasingly important issue for customers
  - Differentiating factor
  - Qualifying factor
  - Willingness to pay for improved security?

- Offshoring data security a particularly sensitive issue
Rely on Contract Remedies?

- Security/privacy problems can create a host of business and legal problems
  - Financial loss
  - Harm to reputation
  - Bad publicity
  - Regulatory actions
  - Civil litigation

- To what extent will a contract adequately protect your company from these risks?

Agreements: Due Diligence

- Prudent business practice
  - FTC recommends it

- Scope
  - Counterparty’s security policies, capabilities, key personnel, and track record

- Method
  - Inspection?
  - Independent audit?
  - Check references
  - Media/litigation searches
Agreements: Core Issues

- Information rights
  - Reporting obligations
  - Record-keeping obligations
  - Audit rights
    - Third-party
    - Corrective actions

- Allocation of risk
  - Limitations on liability
  - Exclusions
  - Insurance

- Compliance with laws
  - What if laws change
  - Increased costs?

- Risk of security breach
  - Preventive actions / security
  - Monitoring and detection obligations
  - If breach occurs
    - Obligation to notify counter-party
    - Cooperation obligations?
    - Inspection rights?
    - Obligation to notify third parties
    - Who pays for notices?
    - Who is liable for third-party claims?
    - Preservation and evidentiary issues
What’s on the Horizon

- HIPAA modifications
- Breach-Notice expanding internationally
- Litigation

Amendments to HIPAA

- New EHR requirements
- New privacy requirements, including notice of security breach requirements
- HITECH Act
Breach – Notice Expands

- Europe
- Canada
- Australia

All are considering formal breach-notice requirements although the spirit of existing laws might indicate an obligation to notify individuals.

Privacy Litigation

- Airlines cases

- Laptop case

- No standing/no damages

- Ruiz v. Gap (April 13, 2009)
  - Increased Risk of ID Theft Not Damages
California’s Identity Theft Law - Remedial Measures

- California permits a person that has been a victim of identity theft to initiate a law enforcement investigation and obtain a police report.
- Expedited judicial review of convictions is also permitted for victims of identity theft.
- There are disclosure requirements regarding consumer reports and credit information if a person has had a credit application made in his name.

Practice Tips for Breach Issues

- Adopt plan.
- Pay attention to suspicious activity or complaints.
- Address these issues with your business partners.
- Realize that multiple parties may have duty to disclose same incident.
- Implement escalation procedures.
- Comply with highest legal standard.
Privacy Takeaways

- Assess what information is being collected
- Think through the types of data you are collecting
- Determine what laws apply to your company based upon the information it collects, where it does business and the identity of its customers

Questions and Answers