Data Breaches:
Security and Privacy Lessons Learned

Sue Glueck
Senior Privacy Attorney

Adam Shostack
Program Manager, Security Engineering & Community

Microsoft Corporation
August 20, 2008
CONTEXT
What are breaches?

• Problems with PII data governance
• Usually (but not always) reported after CA SB 1386
• Cataloged and available for study
How bad is it out there?

- In a new study based on interviews with 50 U.S. retailers, Gartner found that 21 of them were certain they had had a data breach
  - Just three of the retailers had disclosed the incident to the public
  - Might indicate 1/7 US breaches reported
    - [http://www.csoonline.com.au/index.php/id;1397175505;fp;4;fpid;959002](http://www.csoonline.com.au/index.php/id;1397175505;fp;4;fpid;959002)
How bad is it out there?

- DOJ indicted 11 individuals in retail hacking scheme
- Companies targeted included TJX, BJ’s Wholesale Club, DSW Inc., Dave and Buster’s Inc., Barnes & Noble, Sports Authority Inc., Boston Market Corp, Forever 21 Inc., OfficeMax
  - Boston Market Corp, Forever 21 Inc. did not notify customers because data loss was not confirmed
  - No comment from OfficeMax, Barnes & Noble and Sports Authority
WHY DISCLOSE BREACHES?
State Breach Notification Laws

• 44 states have breach notification laws
• Most recently Alaska - Alaska Stat. § 45.48.010 et seq.
  – Breach notification requirements
    • But not required if after investigation and written notice to Alaska’s AG, no reasonable likelihood that harm to consumers has or will result from the breach
  – Restrictions on use of SSN
  – Security freezes
State Breach Notification Laws

• Varying provisions
  – Computerized vs. paper data
  – Definition of personal information
  – Some laws require notifying state agencies and/or credit bureaus
  – Timing of notifications
  – Harm threshold
  – Content of the notification letter
  – Private right of action
Federal Laws

- **Gramm-Leach-Bliley (GLB) Act**
  - Safeguards Rule: Each financial institution must develop, implement and maintain a comprehensive information security program that is written in one or more readily accessible parts

- **Fair Credit Reporting Act, as amended by the Fair and Accurate Credit Transactions (FACT) Act**
  - Disposal Rule: Requires businesses to take reasonable and appropriate measures to prevent the unauthorized access to — or use of — information in a consumer report when disposing of records

- **Section 5 of the FTC Act (15 U.S.C. §§ 41-58) prohibits unfair or deceptive practices**
  - Unfair trade practice to misrepresent your privacy practices
  - You have an obligation to do what you say
  - However, most recent rulings indicate that you have an obligation to keep personal information secure regardless of what you say in your privacy statement
Outside the U.S.

- Japan
- EU proposal to amend the Directive 2002/58/EC on Privacy and Electronic Communications ("the ePrivacy Directive")
  - Scope issues
- UK
  - Recent breaches
  - ICO guidance on “voluntary notification”
- Other countries
WHAT ARE THE IMPACTS OF DISCLOSURE?
Impact on stock price

• Stock price study by Acquisti, Friedman and Telang

“there exists a negative and statistically significant impact of data breaches on a company’s market value on the announcement day for the breach. The cumulative effect increases in magnitudes over day following the breach announcement, but then decreases and loses statistical significance.”

<table>
<thead>
<tr>
<th>Day</th>
<th>-1</th>
<th>0</th>
<th>0 to 1</th>
<th>0 to 2</th>
<th>0 to 5</th>
<th>0 to 10</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAR</td>
<td>0.03</td>
<td>-0.41**</td>
<td>-0.58**</td>
<td>-0.46</td>
<td>0.21</td>
<td>1.3</td>
</tr>
</tbody>
</table>

Impact of legislation

- Carnegie Mellon study analyzed states that had passed data breach notification legislation 2002 to 2006, using FTC data on identity theft
  - “We [found] no statistically significant effect that laws reduce identity theft, even after considering income, urbanization, strictness of law and interstate commerce.”
  - “The lack of a significant negative effect may be due to breaches accounting for a small enough percentage of total identity thefts, dwarfing any actual crime reduction by more common causes such as lost or stolen wallet"
- Note that study looks for reduction in incidents; CA SB1386 aimed to reduce impact
- Issues with data quality and reporting bias
Litigation

• Data breach litigation typically class actions alleging:
  – Negligence/gross negligence
  – Breach of fiduciary duty
  – Breach of contract
  – Invasion of privacy
  – Emotional distress
  – State consumer protection acts
  – Unfair trade practices acts
  – State data breach notification law

• Seeking actual and speculative damages for:
  – Fraudulent charges
  – Credit monitoring costs
  – Identity theft insurance costs
  – Credit report costs
  – Emotional distress from fear of fraud
Litigation

• Pisciotta v. Old Nat’l Bancorp, 499 F.3d 629 (7th Cir. 2007)
  – Plaintiffs sought compensation for past and future credit monitoring services, compensation for economic and emotional damages; breach of contract
    • No allegations of completed direct financial loss to their accounts
    • No victims of identity theft
  – 7th Cir affirmed district court dismissal
    • “Without more than allegations of increased risk of future identity theft, the plaintiffs have not suffered a harm that the law is prepared to remedy”
Litigation

• Other class actions:
    • Plaintiff lacked standing to sue because no actual damages, no recognized injury
    • Broad interpretation of what is included in actual damages

• But...class action attorneys are still hard at work

• Regulatory action
  • ChoicePoint, DSW, BJ’s Wholesale Club, Petco, Guess, Tower Records, Barnes & Noble.com, Card Systems
More litigation

- In 2005-06, hackers stole 45.7+ million customers’ credit card data, drivers’ license numbers and other data on 450,000 customers
- Has spent $202 million in expenses related to the breach
- Multiple class-action lawsuits and investigations
  - FTC investigation and settlement
  - Mastercard-issuing banks settlement - $24 million
  - Visa-issuing banks - $40.9 million
  - Class action suits by consumers in various states under security breach notification laws
    - Customers vouchers of $30-$80 and 3-day sale
    - For 450,000 customers who also provided drivers license: credit monitoring, ID theft insurance, reimbursement for identity theft
- TJX announced Aug, 2008, that its 2nd quarter profit more than tripled
What about cost?

- 2007 Annual US Cost of a Data Breach (Ponemon Institute)
- Headline: “Cost increases to $197 per record”
- Breakdown:
  - Cost of lost business $128/record, 65% of costs
  - Other costs down 15%
  - (3rd party breaches more expensive)

“Following a data breach, organizations suffered an average increased customer churn rate of 2.67 percent, up from 2.01 percent in 2006.”

“The survey design relied on a “shadow costing method” used in applied economic research. This method does not require subjects to provide actual accounting results, but instead relies on broad estimates based on the experience of the subject.”
WHAT WE CAN LEARN FROM BREACHES
Many breaches...

• 1078 incidents in Open Security Foundation’s Dataloss DB (as of Aug 15, 2008)
• Approximate number of records compromised in the U.S. due to security breaches since Jan, 2005: 236,543,778 (Privacy Rights Clearinghouse)
What’s really going wrong?

**Figure 15.** Security breach incidents by type, 2000–1H07, and 2H07 alone, expressed as percentages of the total.
Where to get data

• Privacy Rights ClearingHouse
• Ponemon institute studies
• Ontario Privacy Commissioner’s Health orders
Lessons Learned

• Have a plan
  – Use the data to understand the risks
  – Get buy-in at high levels and low
  – Part of overall privacy incident process
• An ounce of prevention...
  – Find sensitive PII
  – Eliminate where possible (pesky employee laptops, for example)
  – Provide training to data handlers
  – Manage 3rd parties
  – Conduct assessments and audits
Lessons Learned

• In the event of a breach...
  – Follow your plan
  – Carefully assess the incident, including forensic analysis
  – Get legal advice
  – Consider help for victims (credit monitoring vs. identity theft protection services, coupons, vouchers)
  – Prepare call center to respond to questions
  – Proactive-reactive PR
Lessons Learned

• After a breach...
  – Post-mortem
    • What caused the breach?
    • What could have gone better in handling the crisis?
    • But beware smoking gun documents
  – Take corrective action
    • Update your plan if necessary
    • Training
    • Encryption
    • Inventory data
    • Other security measures
Key Takeaways

• We’re constantly learning from each other’s mistakes and successes
• More communication
QUESTIONS?