Dealing with the Reality of a Privacy Breach:
Civil Litigation, Regulatory Response, and Minimizing Your Risks

HCAA North Central Regional Annual Conference | October 3, 2011
Overview

- The challenge of protecting business data
- Addressing a breach and its aftermath
- Recommendations for minimizing risk
- Questions
Some Interesting Statistics

The United States of Shame

Highest ID theft reported in Florida, followed by Arizona and California
Privacy and Security Landscape

- Increasing electronic storage of data
- Privacy laws in 85+ countries.
- Increasingly sophisticated malware
- Increasing enforcement
- Increasing expectations for accountability
- Sophistication of professional hackers
Staggering Amount of Electronic Data

- Over 281,000,000,000 gigabites of stored information
- Over 210,000,000,000 email messages sent in 2008
- Over 58,000,000,000,000 spam messages
What Would This Look Like Printed Out?

10.5++ billion miles
of file cabinets stored end to end
Identity Theft – Key Pieces of Information
Scope of the Problem

- At least one out of three Americans
- Now an issue in almost all countries
- At least one out of five Internet users
- At least one child in every classroom
- Not just a financial issue
What Are The Thieves Doing With Stolen Identities Besides Making Credit Card Purchases?
Examples of Publicized Breaches
Many Unsuspecting ATM Users Fall Prey to Skimming Hardware
Pain at the Pump
Identity Theft at Gas Stations

- Thieves attach an external skimmer
- Sometimes hard to detect
- Some pumps now protected w/ sticker
71% of Fraud Happens Within a Week of Stealing a Victim’s Personal Data
Example of the Challenges
Collection and Processing of Protected Health Information

- Physicians in hospital
- External physicians
- Nurses, other HCPs
- Local IT support
- Remote IT support
- Billing support
- Auditors
- Consultants

Multiple sources for data access

Patient Data Storage
- EMR, back-ups, legacy databases, Research databases,

Other Personal Data Storage (e.g., employees)
- Employee and temporary employee management

Data Security
- Security Layers
- Gate keepers
- Audit Trail
- Encrypted data
- Cloud computing

Business Associate management
- Business associate agreements
- Pre-screening of vendors
- Auditing

HIPAA Privacy Rule Guidance Docs
HIPAA Security Rule Guidance Docs
State privacy laws, Disposal laws

FTC Requirements
Credit Card Data Requirements
Records Retention/E-discovery
Litigation risk reduction

Integration of multiple entities
- Off-site storage
- Unencrypted back-up tapes
- Remote access
- Portable devices
- Use of personal devices
- Long retention times
- Obsolete equipment
How Do Breaches Occur at Organizations? Examples

- Vendors
- Human error
- Unforeseen glitches

- Insufficient training
- New employees
- Untrained contractors

- Disgruntled employees
- Internal sabotage
- Curiosity/gossip

- New security threats
- Network vulnerabilities
- Social media
More Than Two-thirds Of Social Network Users Experienced Some Abuse

- 40% of social networking users quizzed have been sent malware such as worms via social networking sites, a 90% increase since April 2009.

- Two thirds (67%) say they have been spammed via social networking sites, more than double the proportion less than two years ago.

- 43% have been on the receiving end of phishing attacks, more than double the figure since April 2009.

What is the impact on your organization of employees using social networking sites via company-provided equipment?
Progression of Security Breach Laws and Enforcement

1990's
Component of existing data protection laws in certain EU countries

2001/2003
California S.B. 1386

2006
Canada (Guidance)

2008
44 US States, D.C., Puerto Rico, Virgin Islands

2/2009
American Recovery and Reinvestment Act of 2009

9-10/2009
HITECH (final) regulation and FTC breach reporting regulations

2010/2011
46 states with notification laws, plus HITECH. Some states adding additional requirements. Significant increase in federal and state enforcement. New federal legislation.
State Security Breach Notification Laws

- **Organizations**
  - Usually, all
  - Database owner notifies

- **Format**
  - Computerized only
    - (most states)
    - Broadly defined

- **Data**
  - First initial, last name, or
  - First and last name, plus
  - Social Security number,
  - Credit/debit card number
  - Account number
  - Driver’s license number
  - Exceptions: a few add some

- **Notification**
  - Without unreasonable delay (most)
  - Specific deadlines (a few)
  - Law enforcement delay ok (most)
  - Specific elements, forms (a few)
  - Also report to gov’t agencies (some)

- **Exceptions**
  - Encrypted data (exemption)
  - Redacted (exemption)
  - Risk-based assessment (some)
  - Other reporting obligation

- **Public Posting**
  - A few states
  - Some public sites
  - Media attention

- **Enforcement**
  - Investigation file opened
  - Respond
  - Coordination with AG’s
  - Coordination with federal

- **Expectations**
  - Transparency
  - Good faith
  - Remediation
  - Policies and procedures
  - Training
HITECH Act

- Does not preempt state law notification requirements
- Covered entity responsible for reporting the breach
- HHS notification requirements
- Media notification requirements
- Content of notification letter
- Mailing requirements
- Call center
- HHS and State Attorney General enforcement
Likely Impact of a Substantial Breach

- Reputational damage
- Loss of customer confidence
- Plummeting stock price
- Regulator fines and enforcement
- Class action lawsuits
- Adverse media attention
- Loss of customers
- Loss of employee productivity
US Federal Trade Commission

- FTC Act – Section 5
- Deceptive and Unfair Trade Practices
- 20-year consent decrees
- Substantial fines
- HITECH Act– broadens FTC authority

Examples:
- Eli Lilly
- Guess Jeans
- Victoria’s Secret
- TJ Maxx
- Choicepoint
- B.J.’s Wholesale Club
- DSW
Effects of a Privacy/Security Breach
Customer Trust Study

Average 4% Permanent Loss Of Customers By Healthcare Providers Following A Well Publicized Breach

Customer trust is significantly impacted by public notification of a privacy/security breach. This is the case even when the company had a higher than average customer trust score prior to the breach.
Cost of a Breach

• Current estimate: about $305 per record
• Rising every year
• New laws and regulations add much more exposure:
  – Additional state requirements
  – HITECH Act of 2009
  – Federal legislation (introduced – again!)
  – Ex-US legislation (increasing)
• Privacy litigation on the rise
When Does The Time Period to Notify Affected Individuals Begin?

What You Don’t Know CAN Hurt You
Dumpster Diving: Is What is in Your Trash Valuable to Identity Thieves?

Use a shredder? Now those documents can be put back together.
Recommendations For Reducing Risk

- Overall risk assessment and data lifecycle management plan

- Data Collection
  - Business need
  - Security
  - Notice/consent
  - Consent
  - Process
  - Policies/procedures
  - Training

- Data Use
  - Clear practices
  - Int’l transfers
  - Enforcement
  - Red Flags Rule

- Data Access
  - File encryption
  - Access log
  - Disaster recovery
  - Remote access
  - Vulnerability testing
  - Firewalls
  - Internal threats
  - Website security

- Security
  - Vendor management
  - New obligations
  - Return of data

- Sharing
  - File encryption
  - Access log
  - Disaster recovery
  - Remote access
  - Vulnerability testing
  - Firewalls
  - Internal threats
  - Cloud computing

- Storage
  - Records management
  - E-mail management
  - Irreversible destruction
  - e-discovery

- Retention / Disposal
  - Litigation holds

26
Take-Away Tips

• MUCH easier to address the issue before a breach occurs
• You are only as good as your weakest link
• Privacy by design approach
• Don’t overlook social media aspects
• Integrated compliance approach
• Requires ongoing vigilance, expertise
• Do not get taken by overpriced, under-qualified vendors
• Create self-sufficiency within your own organization
• Don’t overlook the records management and litigation aspects!
Thank You

Joan Antokol, Esq.
Partner
Park Legal LLC
10401 North Meridian St., Suite 350
Indianapolis, IN 46290
317.616.3350 (office)
Joan.antokol@parkintl.com