crowell moring

Breach Response and Litigation Involving Personally Identifiable Information

Jeffrey L. Poston
Robin Campbell

CONSEQUENCES OF A BREACH OF PII

- LEGAL LIABILITY
  - Government Enforcement Action
  - Class Actions
  - Individual Actions
- REPUTATIONAL EXPOSURE
- BUSINESS CONSEQUENCES
- SEC/SHAREHOLDER ISSUES
- EMPLOYEE/CUSTOMER ISSUES
- TYPICAL BREACH COSTS $MILLIONS
  - Forensics
  - Outside Counsel
  - Credit Monitoring
  - Security & Technology upgrades
  - Defense costs
  - Fines
  - Settlements

TYPES OF INCIDENTS

- Cyber-Hacking
- Employee/Vendor Negligence
  - Lost laptop
  - Inadvertent transmission
- Employee/Vendor Theft

EVERY INDUSTRY AFFECTED

- Healthcare
- Financial Services
  - Banks
  - Credit Card Companies
  - Insurance Companies
  - Mortgage Companies
- Technology
- Education
- Retail
- Government

Can involve Employee or Consumer Data

MULTIPLE FEDERAL LAWS IMPLICATED, E.G.

- HIPAA
- GRAMM LEACH BLILEY
- FTCA
- FERPA
- FCRA/FACTA

STATE BREACH NOTIFICATION LAWS

- If PII is potentially comprised, must comply with State Breach Notification laws
  - States plus D.C., Puerto Rico and Virgin Islands
  - 46 Different standards some involving "risk of harm"
  - AGs Have Enforcement Authority
  - Timing: "in the most expedient time possible," "without unreasonable delay"

DEFINITION OF PERSONAL INFORMATION

- Generally defined as combination of first and last name PLUS any one of the following:
  - SSN
  - Drivers License No.
  - Account No.
  - Credit Card No.
  - Medical Information

- Personal Information
  - Consumer data
  - Employee data
  - Member data

ENFORCEMENT ACTIONS

- FTC:
  - Major Internet Company for $22 million
  - Sues major hotel chain for $10 million
  - $10 million fine against Data Aggregator
  - 20 years of security audits for Blood Bank
- HHS:
  - National Health Insurer fined $4.3 million
  - State Health Agency fined $1.7 million

<u>STATES</u>

- Penalties available under state breach laws ($10k to $500k but can go higher), also separate penalties under state insurance and DTPA laws
- CA & MD have established special privacy enforcement units

CASE STUDIES
INSURANCE COMPANY VENDOR

- Could Not Account for 6 Disk Drives
  - Data of 2 million members
    - PHI
    - SSNs
    - Credit Card Numbers
    - Not Encrypted
  - 11 Class Actions
  - Multiple State and Federal Investigations

DEFENSE CONTRACTOR HACKING

- Defense Contractor cyber-hacked from Asia
  - Target was Military Plans
  - Hackers access server with data involving 20,000 employees (SSNs, Names, DOBs)
    - Data Not Encrypted
    - Notified Affected Employees
    - State AG investigation

DATA MANAGEMENT COMPANY

- Inadvertently sent Data from 48 Universities to wrong University
  - Not encrypted
  - Data regarding millions of students
  - No SSNs
  - No Notification
  - No Enforcement Action
  - No Class Actions

HOW TO MANAGE CRISIS WHEN PII COMPROMISED

1. DO NOT SWEEP UNDER THE RUG
2. BE PREPARED
   - Breach Response Plan
     - GC's Office
     - Privacy Office
     - IT
     - Media Relations
   - Anticipate Litigation/Investigations
3. INVOLVE IN-HOUSE/OUTSIDE COUNSEL IMMEDIATELY
   - If beyond de minimis expect further scrutiny
   - Can assert privilege to maximum extent possible
   - Assert privilege over outside consultants
   - Use counsel to conduct employee interviews
   - Maintain chain of custody over documents to prevent spoliation
4. INVESTIGATE
   - Physical
   - Forensics
   - What Data?
   - Whose Data?

HOW TO MANAGE CRISIS WHEN PII COMPROMISED (cont'd)

5. MITIGATE/REMEDIATE

6. FIRST 24-48 HOURS CRITICAL
   - Can you recover data?
   - Can you forensically prove data not accessed?
     - University example

7. INVOLVE IN-HOUSE/OUTSIDE COUNSEL IMMEDIATELY
   - If beyond de minimis expect further scrutiny
   - Can assert privilege to maximum extent possible
   - Assert privilege over outside consultants
   - Use counsel to conduct employee interviews
   - Maintain chain of custody over documents to prevent spoliation

8. FIRST 24-48 HOURS CRITICAL
   - Can you recover data?
   - Can you forensically prove data not accessed?

HOW TO MANAGE CRISIS WHEN PII COMPROMISED (cont'd)

9. If Data Missing Or Possibly Accessed
   - Be Proactive with Regulators
   - Establish Relationship/Bring them in the loop

10. Involve Corporate Communications Office
   - States Require Certain Content in Notification Letters
   - Speak with one consistent voice

11. Consider Potential Litigation When Remediating Breach
   - Take steps to preserve indemnification rights
   - Present a united front with vendors
   - Early offering of services may prevent litigation
   - BUT may reduce options at later settlement

Emerging Litigation Issues

- Typical Claims
  - Negligence
  - Breach of Contract
  - Unfair Trade Practices
  - Breach of Privacy
  - State Statutes
- Threshold issues
  - Standing to sue (Federal Court)
  - Actual injury or harm (common law claims)

Emerging Litigation Issues (cont'd)

- Class Certification Issues
  - Rare (Dismissal or Settlement)
  - Claims often turn on individualized issues or causation and damages
  - Thus common questions of law & facts do not predominate over questions affecting individual members.
- Damages
  - Aggregate exposure to nominal damages
  - Due process violation?

TYPICAL SETTLEMENTS

- Non-monetary relief (e.g., credit monitoring)
- Monetary payments to privacy non profits (e.g. Privacy Rights Clearinghouse)
- Consent Decree requiring security improvements
- Attorneys fees to Plaintiffs' counsel
- Capped individual payments to Plaintiffs who can prove causation

SUMMARY

- Security incidents are inevitable/litigation is not

When a breach hits:

- Do the right thing
  - Protect your company
  - Protect your customers/employees/members
  - Protect your data
  - Not mutually exclusive
- Respond quickly and aggressively to:
  - Mitigate Damage
  - Lessen likelihood of litigation/investigation
  - Protect yourself if they do arise