

Cutting Edge Issues in Technology Law
Seattle December 7-8, 2006

Privacy & Security Recent Developments

Francoise Gilbert
CEO - IT Law Group
www.itlawgroup.com
Palo Alto, California

IT LAW GROUP

© 2006 IT Law Group

QUIZ: What is this number?

97,148,596

IT LAW GROUP

2

ANSWER

- **97,148,596** is the number of records containing sensitive personal information (SSN number, credit card numbers, drivers license numbers, etc.) involved in security breaches between February 15, 2005 and November 3, 2006

- Source: Privacy Rights Clearinghouse

Your company or client name could be here

Wells Fargo	Polo Ralf Lauren	Verizon	TransUnion	Eastman Kodak
GMAC Financial	Starbucks	Nikon	H&R Block	Toyota
Intuit	Bananas.com	ADP	FedEx	Chevron
Bank of America	Gymboree	EDS	Ernst & Young	Kaiser Permanente
Card Systems	Williams Sonoma	Allstate	Deloitte	Circuit City

QUIZ: How did it happen?

- 426 security breaches reported in 21 months
- And more probably not reported
- this means about 20 per month, or at least one each business day
- How did these 426 reported security breaches occur?

CAUSES FOR DATA LOSS

- What happens:
 - Lost item
 - Theft or burglary
 - Dishonest insider
 - Hacker (outsider)
- How it happens:
 - Most frequent: *Negligence, laziness, no common sense*
 - In most cases, the breach of security and loss of data is *not* caused by cyber crimes

EXAMPLE

- SSN number exposed on mailing labels
 - H&R Block
 - Blue Cross / Blue Shield (600 records)
- Credit/debit card information printed on paper that was recycled and used in wrapping newspaper bundles for distribution
 - Boston Globe
- SSN numbers provided in response to FOIA request
 - Dept of Agriculture (350,000 records)

EXAMPLE

- Instructor posted class roster with SSN number to website:
 - Old Dominion University (601 records)
- SSN, date of birth, etc. routinely posted on website as part of standard business practice
 - Ohio Secretary of State's Office
 - Georgia County Clerk of Courts' website
- SSN numbers posted on website, for commercial purpose
 - Lexis-Nexis Internet Database Service posted SSN of Tuscarawas and Warren counties

EXAMPLE

- Computer with **unencrypted** names, social security numbers, birthdates, etc. **lost or stolen**
 - University of Pittsburg Medical Center
 - California Army National Guard
 - Fidelity Investments (196,000 records)
 - Starbucks
 - Gymboree (20,000 employee records)

EXAMPLE

- **Unencrypted** media or computer tape containing names, addresses, SSN **lost or stolen**
 - People's bank (90,000 records)
 - Providence Home Services (365,000 records)
 - Ernst & Young (38,000 records)
 - Affiliated Computer Services (1.4 million records)
- This includes the laptop "stolen" from someone's car left with all doors unlocked, the engine running, and laptop on the passenger seat...

EXAMPLE

- Dishonest employee accessed customer files
 - City of San Diego Water & Sewer Dep't.
 - Swedish Medical Center Seattle (1,000 records)

EXAMPLE

- Computer purchased at second-hand store contained the names, SSN numbers, employment records, and other personal information of employees
 - Intermountain Healthcare (6,244 records)
- Employee records found scattered on a city street
 - City of Visalia (200 records)

EXAMPLE

- Hackers obtained credit card information, in conjunction with names and addresses from website
 - State of Rhode Island website (4,117 records)
 - Honeywell International (19,000 records)
 - Akron Children's Hospital (200,000+ records)

BEWARE OF SUBCONTRACTORS

- Security problems can occur both
 - While data is on the organization's premises (or website); and
 - While the data is in the custody of subcontractors, vendors, outsourcers, or offshore service providers
- Example:
 - Card Systems hacking exposed name, account and verification codes of customers of MasterCard, Visa, Discover and Amex Cards

OFFSHORING

- *An Australian reporter, working undercover, was able to purchase the personal information of Australian customers from a call center in India*
- *These included birth certificate information, Medicare number, driver's license number, ATM card number*
- *Source: www.news.com August 16, 2005*

OFFSHORING

- *In New Delhi, police arrested a call center worker for alleged theft of personal customer information that the firm was handling for its clients. The employer found the worker copying customer information on a CD, and reported the matter to the police*
- *Source: www.news.com September 2005*

THE RECORD TO DATE

- Card Systems: **40 million**
 - Hacking exposed name, account and verification codes of customers of MasterCard, Visa, Discover and Amex Cards (June 2005)
- Dep't of Veteran Affairs: **28.6 million**
 - Laptop stolen from home of employee of VA Adm, contained data of all veterans discharged since 1975 (May 2006)

WHAT HAPPENS NEXT?

- Consequences of loss of sensitive personal data:
 - Legal:
 - Class action litigation
 - FTC or State Attorney General scrutiny and supervision for the next 20 years
 - Financial
 - PR disaster
 - Bankruptcy: Card Systems assets sold to Pay By Touch
 - Stock value slashed: Choicepoint stock was \$46 before disclosure of breach, it is now \$37; i.e., loss of 25% of value

SECURITY TODAY

- Significant expansion of corporate obligations to ensure the security of electronic information
 - Personal Information
 - Customers (and other outsiders)
 - Employees
 - Company Information
 - Reporting requirements (e.g., SOX)
 - Record keeping requirements (e.g., evidence, tax)

SECURITY TODAY

- **Duty to Protect:** Provide reasonable security for corporate and personal data, and information systems
 - Duty to prevent breaches
 - Duty to destroy data
 - Duty to ensure security of e-transactions
- **Duty to Disclose:** Disclose security breach
 - To those who may be adversely affected by such breaches
 - To others (AG, Consumer Protection Board, State Office of Cybersecurity, Consumer Reporting Agencies)

DUTY TO PROTECT

- Corporate Governance Legislation
 - Sarbanes Oxley Act Sect. 302 and 404 require significant security measures to ensure that adequate internal control structures and procedures for financial reporting are in place
 - CEO and CFO are responsible for ensuring security and quality of corporate information

DUTY TO PROTECT

- Privacy / Security Laws, Regulations
 - Require companies to implement information security measures to protect personal data they maintain
 - GLBA places responsibility for security with the Board of Directors. The Board is required to approve the written security program
 - HIPAA, COPPA
 - State laws require companies to **implement reasonable security measures** (California, Arkansas, Nevada, Rhode Island, Texas, Utah)

DUTY TO PROTECT

- Authentication, integrity, retention
 - E-Sign and UETA require all companies to provide security for storage of electronic records relating to online transactions
 - IRS regulations require companies to implement information security to protect electronic tax records
- Data destruction laws
 - FACTA Document Destruction Regulations
 - State laws

DUTY TO PROTECT

- FTC and State Attorneys General
 - Have prosecuted companies for alleged failure to provide adequate security
 - Asserted that the failure to provide appropriate information security was an [unfair trade practice](#) under Section 5 of the FTC Act, even in the absence of any false representation by the defendant as to the state of its security
 - Consent decrees require implementation of security measures and appointment of an identified Privacy / Security official responsible for compliance

RECENT CASES

- Guidance Software (November 06)
- DSW (March 06)
- CardSystems Solutions (February 06)
- ChoicePoint Inc. (January 06)
- BJ Wholesale Club (June 05)

FTC v. CHOICEPOINT

- ChoicePoint provided third party's personal information to subscribers who had inadequate credentials
- ChoicePoint did not have reasonable procedures to screen prospective subscribers, and turned over consumer information to subscribers whose application raised obvious redflags
- ChoicePoint received subpoenas from law enforcement authorities in 2001 alerting CP of the fraudulent activities

- Source: Federal Trade Commission

FTC v. CHOICEPOINT

- Settlement January 2006
 - **\$10 million** in civil penalties (the largest civil penalty in FTC history)
 - **\$5 million** for consumer redress
 - Establish, implement and maintain comprehensive information security program
 - Obtain every 2 years, for the next 20 years, an audit from a 3rd party
 - Record-keeping and reporting provisions to allow FTC to monitor compliance

DUTY TO PROTECT

- **Abroad and International**
 - **Foreign Data Protection Laws:** EU Member States, Canada, Australia, Argentina, require companies to implement security measures
 - **Safe Harbor:** Companies self-certifying under the Safe Harbor commit to take reasonable precautions to protect personal information from loss, misuse, unauthorized access, disclosure, alteration and destruction
 - **Model contracts and BCRs:** also include a requirement for security

CLASS ACTIONS

- Example: ChoicePoint
 - Class actions brought on behalf of individuals whose personal data were compromised by the security breaches disclosed in February 2005
 - Class actions brought on behalf of shareholders, who allege that ChoicePoint management failed to disclose to shareholders and potential investors that the company's security measures were inadequate and ineffective

CLASS ACTIONS

- Sony BMG: spyware (rootkit) and breach of privacy
- Visa, MasterCard: failure to protect credit card system from breach
- Wells Fargo

COMPLIANCE REQUIRED

- Entities that are regulated by specific sectoral laws that outline the security measures to be taken (e.g., financial and healthcare institutions) should comply with these **laws and regulations**
- Organizations that are not currently regulated should take into account the **FTC rulings** because they define a **de facto standard**

FEDERAL TRADE COMMISSION

- Current FTC rulings require:
 - Designation of appropriate personnel to oversee privacy / security program (e.g., CPO, CSO, CISO)
 - Identifying reasonable, foreseeable internal and external risks to security, confidentiality, and integrity of personal information
 - Conducting an annual written review by qualified persons
 - Adjusting program to fit findings from reviews, monitoring, operational changes.

SEVEN PART PROGRAM

- In order to address security, companies must implement an Enterprise Security Program:
 - 1. *Asset assessment*
 - 2. *Risk assessment*
 - 3. *Security policies and procedures*
 - 4. *Education and training*
 - 5. *Monitoring and testing*
 - 6. *Review and upgrade*
 - 7. *Same as above for third party relationships*

DEALING WITH THIRD PARTIES

- Conduct thorough *due diligence* of service provider before entering into a contract
- Evaluate privacy and security *policies, incident response, enforcement*
- Ensure *contract* provides for data use restrictions, security procedures, disclosure of security breaches
- Conduct periodic *audits* during performance of the contract

DEALING WITH THIRD PARTIES

- Remember that:
 - China, India, the Philippines and other offshoring countries *do not have data protection laws, or information security laws, and may have a deficient judicial system*
 - Some countries that do have data protection laws *do not have a data protection culture. Privacy is also a cultural issue*

ATTORNEY'S ROLE

- Attorneys play an important role in the development and implementation of an Enterprise Security Program:
 - Develop plan, define goals and budget
 - Assess data flows, and evaluate risks
 - Understand (and communicate) compliance requirements and applicable laws
 - Create policies (high level) and procedures (daily use)
 - Provide training, and disseminate policy
 - Monitor application and revise policy as necessary
 - Establish process for enforcement, discipline of the infringers

STATE NOTIFICATION LAWS

Alabama	Hawaii	Massachusetts	New Hampshire	S. Dakota
Alaska	Idaho	Michigan	New Jersey	Tennessee
Arizona	Illinois	Minnesota	New Mexico	Texas
Arkansas	Indiana	Mississippi	New York	Utah
California	Iowa	Missouri	Ohio	Virginia
Colorado	Kansas	Montana	Oklahoma	Vermont
Connecticut	Kentucky	N. Carolina	Oregon	W. Virginia
Delaware	Louisiana	N. Dakota	Pennsylvania	Washington
Florida	Maine	Nebraska	Rhode Island	Wisconsin
Georgia	Maryland	Nevada	S. Carolina	Wyoming

IT LAW GROUP

37

DUTY TO DISCLOSE

- 34 States have enacted Security Breach Disclosure Laws; there are discrepancies between these laws
- Covered entities:
 - Entities that own or license personal information (data collectors)
 - Entities that maintain third party information (service providers)
- Breach:
 - Unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of protected personal information

IT LAW GROUP

38

DUTY TO DISCLOSE

- Protected information:
 - Individuals' name (or signature, phone number, address) in combination with
 - (a) SSN number; or (b) Driver's license number; or (c) account number, debit or credit card number and access code (or insurance policy number, passport number, medical information)
- Failure to notify:
 - Injunction
 - Injured customer may (or may not) institute civil action to recover damages
 - Cumulative rights and remedies; treble damages

IT LAW GROUP

39

FIRE DRILL

- Given the urgency requirements in making the disclosures, and the discrepancies between applicable laws, organizations should be prepared to respond to a security breach ahead of time
- Draft and implement **Incident Response Plan**
 - *How security incident is reported internally, to whom*
 - *Core team (representatives from Privacy, Legal, IT, Security, Communications groups)*
 - *Decision makers*
 - *Phased approach: information collection; initial assessment, etc.*
 - *Collect information to allow determination of whether notices to individuals, governments, or credit bureaus are required or recommended*
 - *Establish relationship w. law enforcement agencies, credit monitoring services*

IT LAW GROUP

40

ACTION ITEMS

- Ensure appropriate measures are in place to protect personal information (*Enterprise Security Plan, Incident Response Plan*, as well as Disaster Recovery, Business Continuity plans)
- Weave privacy and security into M&A and corporate agreements
- Protect *information held or accessible by third parties*, subcontractors, outsourcing providers
 - Obligation to have adequate security measures
 - Obligation to immediately disclose security breach
 - Periodic audits
- Review insurance coverage

SUMMARY

- How a company handles information (personal or corporate) is *critical to the balance sheet and share value*
- Any mistake will dramatically affect individuals who may be facing identity theft
- PR disaster will sink the company
- *Numerous laws, regulations, standards* control the collection, use, and transfer of PII
- Compliance with data protection and information security laws must be addressed at the *C-Level*
- Compliance requires the *development, implementation and maintenance of an Enterprise Security Program*

FOR MORE INFORMATION...

fgilbert@itlawgroup.com

650-804-1235

*IT Law Group
555 Bryant Street # 603
Palo Alto, CA 94301*

IT LAW GROUP

43