

Developments in Security & Privacy Law

2007-2008



Agenda

- Overview of security and privacy legal developments over the past year, including:
 - Promulgation by Federal Agencies of Rules Pertaining to Security
 - New and Recent Updates to Federal Legislation
 - Proposed Federal Legislation
 - State Legislative Activities
 - Agency Enforcement Actions and
 - Private and Security Litigation



Universe of Legal Requirements

- **Federal**
 - GLBA
 - FTCA
 - SOX
 - FCRA/FACTA
 - HIPAA
 - FISMA
 - FERPA
 - 21 C.F.R. Part 11 (FDA Regulations)
- **State**
 - Notice of Security Breach
 - Other State Laws
- **International**
 - EU Data Protection Directive
 - Member Country Legislation
 - Binding Corporate Rules, etc.
 - US Safe Harbor –
 - Canada PIPEDA
 - Others (e.g., Japan, Australia)
- **Private Contractual Requirements**
 - PCI DSS
 - Business Associate Agreements
 - Service Provider Agreements

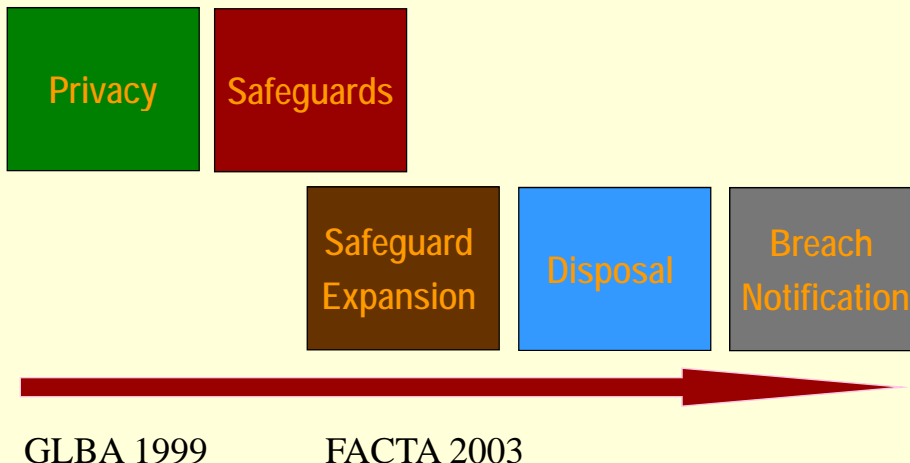


New or Proposed Federal Agency Rules and Guidelines

Security, Privacy, Identity Theft



GLBA Scope and Amendments



Proposed Amendments to Regulation S-P

- GLBA/FACTA
- Applies to brokers, dealers, registered investments advisers, investment companies and transfer agents
- Broadens Safeguards
- Disposal Rule
- Notice of Breach Rule
- Contains new exception to opt-out of information sharing

73 Fed. Reg. 13692 (March 13, 2008)



FISMA: Federal Information Security Management Act of 2002

- Requires compliance with a set of standards federal government information security
 - Federal Information Processing Standards (FIPS)
 - National Institute of Standards and Technology (NIST) SP 800 Standards
- Applies to Federal information System
 - An information system used or operated by an executive agency, or by another organization on behalf of an executive agency
- Is applicable to contractors handling certain sensitive Info
 - Through government contracts
 - Also, some federal agencies (e.g., DOL) are beginning to hold fund recipients to these standards.



Recent FISMA Developments

- December 2007 NIST released a final public draft of guidance for federal agencies to follow when conducting data security assessments.
<http://csrc.nist.gov/publications/drafts/800-53A/draft-SP800-53A-fpd-sz.pdf> (Final Public Draft, Special Publication 800-53A, December 2007).
- Federal agencies required to submit more detailed information on their privacy policies and their handling of privacy reviews of their programs to the OMB as part of the fiscal year 2008 annual FISMA compliance review
 - <http://www.whitehouse.gov/omb/memoranda/fy2008/m08-09.pdf>



REAL ID ACT

- **REAL ID Act of 2005, Public Law 109-13, 119 Stat. 231, 302 (May 11, 2005) (codified at 49 U.S.C. §30301)**
 - Tighten requirements for identification cards acceptable to the federal government
- **Final Rule Issued on January 29, 2008**
 - **Includes:**
 - information and security features that must be incorporated into each card;
 - proof of identity and U.S. citizenship or legal status of an applicant;
 - verification of the source documents provided by an applicant; and
 - security standards for the offices that issue licenses and identification cards

73 Fed. Reg. 5272 (January 29, 2008), to be codified at 6 C.F.R. Part 37



Practices to Address Security and Privacy

REAL ID ACT

- **Requires States (DMV) to:**
 - provide a clear and understandable privacy policy to each card holder;
 - provide individual access and correction rights for card holders;
 - specify the purpose for collecting personally identifiable information in the privacy policy and limitation of the use to those purposes;
 - limit the information collected for those purposes;
 - limit disclosure of the information except to a governmental agency engaged in the performance of official responsibilities pertaining to law enforcement, the verification of personal identity, or highway and motor vehicle safety, or a third party as authorized under the Driver's Privacy Protection Act.



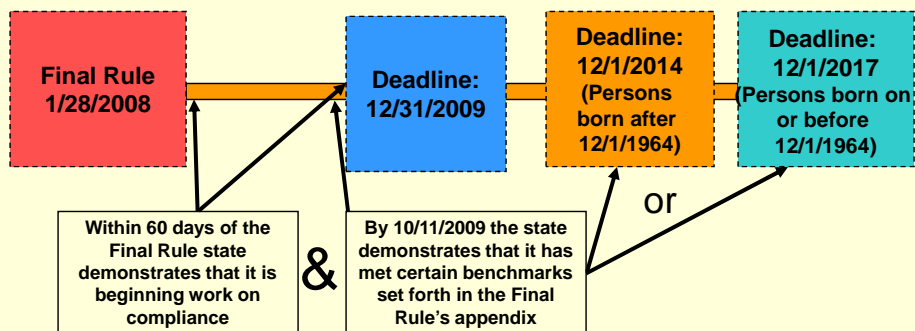
Practices to Address Security and Privacy (cont'd)

REAL ID ACT

- require data quality standards and security safeguards to protect against loss or unauthorized access, destruction, misuse, modification, or disclosure;
- perform a Privacy Impact Assessment (PIA) to identify and analyze how personally identifiable information related to implementation of the REAL ID Act is collected, used, maintained, and protected; and
- establish accountability for compliance with the State's privacy and security policies to ensure that these best practices are fully implemented



REAL ID ACT Deadlines



DHS is making approximately \$360 million available to assist states with REAL ID implementation - \$80 million in dedicated REAL ID grants and another \$280 million in general funding as part of the Homeland Security Grant Program

This is an estimated 73 percent cost reduction – from an original estimate of \$14.6 billion to approximately \$3.9 billion



OMB Memorandum on Security Incidents

- 2007 memo orders federal agencies to
 - Implement Plans for Breach Notice
 - Place Limits on use of SSN
 - Review and reduce volume of Personally Identifiable Information
 - Reduce the use of SSNS
- Incident Reporting and Handling
 - Internal
 - External

"Safeguarding Against and Responding to the Breach of Personally Identifiable information" (M-07-16), is available at <http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf>



Existing Requirements

OMB Memorandum

- When creating a plan, Agencies must follow existing requirements under FISMA
 - Implement procedures for detecting, reporting and responding to security incidents/mitigating risks
 - Notify and consult with
 - Federal security incident center
 - Law enforcement agencies and Inspector Generals
 - Offices designated by the President for an incident involving a national security system
 - Any other agency or office as directed by the President
 - Implement NIST guidance and standards



External Reporting

OMB Memorandum

- Six Elements for Policy and Plan
 1. Whether the breach notification is required
 2. Timeliness of the notification
 3. Source of the notification
 4. Means of providing the notification
 5. Contents of notification
 6. Who receives the notification: public outreach in response to a breach



Reporting and Routine Use

OMB Memorandum

- Requires agencies to report all incidents involving PII to US-CERT within 1 hour of detection
- Disclosures of PII security incident reporting and response are to be designated a “routine use” for purposes of the Privacy Act of 1974



Housing and Urban Development (HUD)

1. HUD suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised;
2. HUD has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the HUD or another agency or entity) that rely upon the compromised information; and
3. the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the HUD's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

72 Fed. Reg. 52572 (September 14, 2007) Comment period closed on 10/15/07



SOX Filing Extensions for Smaller Companies

- Section 404 requires the management of public companies annually to assess and report on a firm's internal controls, including data security, and provide an auditor's attestation of that assessment
- On January 31, 2008 the SEC proposed a one-year extension of the SOX Section 404(b) auditor attestation requirement for smaller companies – *i.e.*, non-accelerated filers--smaller public companies with a public float of less than \$75 million
- Under the proposed extension, Section 404(b) requirements would apply to smaller public companies beginning with fiscal years ending on or after Dec. 15, 2009



FACT Act Red Flags Regulations

- **October 31, 2007 a joint final rule* was released implementing sections 114 and 315 of the FACT Act (FACTA)**
- The rule, referred to the "Red Flag Rule," establishes interagency regulations requiring financial institutions and creditors to implement measures to create identity theft prevention program:
 - require financial institutions and creditors to develop and implement written identity theft prevention programs;
 - describe the factors that financial institutions should address in their programs' policies and procedures;
 - require credit and debit card issuers to assess the validity of a request for a change of address under certain circumstances; and
 - set forth reasonable policies and procedures that a user of consumer reports should employ upon receiving a notice of address discrepancy from a consumer reporting agency.
- **Compliance is due on November 1, 2008,**
<http://www.ftc.gov/os/2007/10/r611019redflagsfrn.pdf>

*Also approved was a joint final rule for creation of programs that assure consumers will be notified and given the opportunity to opt-out of certain marketing conducted by affiliated financial institutions



ID Theft Prevention Program

- Requires reasonable policies and procedures to:
 1. identify relevant patterns, practices, and specific forms of activity that are "red flags" signaling possible identity theft and incorporate those red flags into the program;
 2. detect red flags that have been incorporated into the program;
 3. respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and
 4. ensure the program is updated periodically to reflect changes in risks from identity theft

*Red flags are sets of condition that could point to ID theft, such as an atypical spending pattern, or receipt of a change of address notice followed immediately by multiple credit and/or debit card requests.



FCC Pretexting

- **April 2, 2007, Federal Communications Commission (FCC) released a regulatory package to address "pretexting"**
 - strengthens protection of customer phone records, including measures to prevent unauthorized access to call data and notification of customers when their call data is breached
 - Requires opt-in consent from customers for releases made to joint venture partners or independent contractors for marketing purposes
 - password required before carriers may release a customer's phone call records to a customer, except the carriers may release the customer's phone call record by sending it to an address of record, or if the carrier calls the customer at the telephone of record.
 - Includes notice of breach procedures
- **The FCC policy was issued as part of a larger regulatory package designed to protect "customer proprietary network information" (CPNI) held by carriers**



Security under FCC Rule

- Carriers are required to take "reasonable measures" to discover and protect against "pretexting," whereby someone attempts to fraudulently obtain a customer's phone records without the individual's knowledge or permission.
- The commission said it will infer from evidence of unauthorized disclosures that reasonable precautions were not taken, which could lead to enforcement action
- A coalition of small telecommunications companies Aug. 6, 2007, filed a petition with the Federal Communications Commission seeking reconsideration of the foregoing security rules that could make them automatically liable for security breaches involving customer records
- Even before the new rule FCC required annual certification that they have security in place to protect the privacy of customer records.
 - In 2006 AT&T paid 550,000 in July 2006
 - In march 2007, the FCC fined three telecoms a total of \$100,000 for failing to provide a certification



FERPA

- Family Educational Rights and Privacy Act of 1974 (FERPA) NPRM for amendments resulting from:
 - the USA Patriot Act (Pub. L. 107-56),
 - the Campus Sex Crimes Prevention Act, and section 1601(d) of the Victims of Trafficking and
 - Violence Protection Act of 2000 (Pub. L. 106-386)
 - U.S. Supreme Court decisions interpreting FERPA and make other necessary changes regarding permissible disclosures of education records, permissible redisclosures of education records by State and Federal officials, and investigation and enforcement procedures
- Status: Not Released



Proposed, Pending or Passed Federal Legislation



Leading Federal Notice of Security Breach Bills: Senate

- **Nine data security bills, including S. 1178 and S. 495, are before Congress. All of the measures would preempt state breach notice law**
 - **S. 495, Personal Data Privacy and Security Act of 2007**, Leahy-Specter Bill
 - would require notification any time there is a breach, unless a risk assessment concludes there is "no significant risk" of harm to consumers and risk assessment is provided to Secret Service
 - Includes notice provisions and requires information safeguards to be implemented
 - Passed Judiciary Committee 5/3/07
 - **S. 1178, Identity Theft Prevention Act**, Gordon H. Smith Bill
 - Would require companies and federal agencies to safeguard consumers' sensitive information,
 - Requires notification to individuals if their personal information in any format is breached, prohibits companies from purchasing or selling Social Security numbers and allows individuals to place security freezes on their consumer credit reports



Leading Federal Notice of Security Breach Bills: House

- **H.R. 958, the Data Accountability and Trust Act, introduced by Reps. Bobby Rush (D-IL) and Cliff Stearns (R-FL).**
 - requires companies to implement data security programs and to notify individuals affected by a data security breach, unless there is "no reasonable risk of identity theft, fraud, or other unlawful conduct"
 - awaiting action by the House Energy and Commerce Committee since February 2007
- **H.R. 4175, the Cybercrime Enforcement Act of 2007 introduced by Reps. John Conyers (D-MI) and Lamar Smith (R-TX)**
 - requires companies to notify law enforcement agencies about data security breaches involving sensitive data and to provide criminal penalties for individuals who knowingly fail to provide such notice



Cybercrime Bills

- S. 2168, Identity Theft Enforcement and Restitution Act of 2007, Introduced 10/16/07 by Leahy (D-VT) and Specter (R-PA), Approved by Senate 11/15/07
 - Removes \$5,000 damage threshold
 - Makes it clear that threatening to obtain or release information from a computer for extortion purposes constitutes a cybercrime
 - It eliminate the jurisdictional requirement that a computer's information must be stolen through an interstate or foreign communication in order to federally prosecute the crime
- H.R. 2290, Cyber-Security Enhancement Act of 2007, Introduced 5/14/07 by Reps. Adam Schiff (D-CA) and Steve Chabot (R-OH)
 - Provisions similar to S. 2168



Health Information Bills

- Wired for Health Care Quality Act (S. 1693) introduced by Kennedy (D-MA), Enzi (R-WY) Clinton (D-NY) and Hatch (R-UT):
 - Contains a section on privacy and security of health care records
 - There is some concern that it does not provide enough protections EHR
- Passed the House and awaiting action in the Senate
 - In the meantime, several state legislatures are considering legislation to encourage the use of electronic health files



Federal Trade Commission Reauthorization Act of 2008" (S. 2831)

- would allow the FTC:
 - for the first time to seek civil penalties against companies for violations of any of the laws it enforces--including Section 5 of the FTC Act
 - to file enforcement lawsuits in federal court, including Section 5 cases, on its own rather than asking the Justice Department to file such suits on behalf of the FTC
 - to conduct rulemaking procedures through Section 553 of the Administrative Procedures Act



State Legislative Action

**When Congress Doesn't Act,
States Fill in the Gaps**



State Breach Notice Laws Continue to Proliferate

- Arizona (Ariz. Rev. Stat. §44-7501)
- Arkansas (Ark. Code §4-110-101 et seq.)
- California (Cal. Civ. Code §1798.82)
- Colorado (Col. Rev. Stat. §6-1-716)
- Connecticut (Conn. Gen Stat. 36A-701(b))
- Delaware (De. Code tit. 6, §12B-101 et seq.)
- District of Columbia (B16-810)
- Florida (Fla. Stat. §817.5681)
- Georgia (Ga. Code §10-1-910 et seq.)
- Hawaii (Hawaii Rev. Stat. §487N-2)
- Idaho (Id. Code §§28-51-104 to 28-51-107)
- Illinois (815 Ill. Comp. Stat. 530/1 et seq.)
- Indiana (Ind. Code §24-4.9)
- Kansas (Kansas Stat. 50-7a01, 50-7a02 (2006 S.B. 196, Chapter 149))
- Louisiana (La. Rev. Stat. §51:3071 et seq.)
- Maine (Me. Rev. Stat. tit. 10 §§1347 et seq.)



...with 4 More Enacted in 2007...

- **Maryland (HB 208, S 194)**
- **Massachusetts (HB 4775)**
- **Michigan (SB 309, Public Act 566)**
- Minnesota (Minn. Stat. §325E.61, §609.891)
- Montana (Mont. Code §30-14-1701 et seq.)
- Nebraska (Neb. Rev Stat 87-801 et. seq.)
- Nevada (Nev. Rev. Stat. 603A.010 et seq.)
- New Hampshire (N.H. RS 359-C:19 et seq.)
- New Jersey (NJ Stat. 56:8-163)
- New York (N.Y. Bus. Law §899-aa)
- North Carolina (N.C. Gen. Stat §75-65)
- North Dakota (N.D. Cent. Code §51-30-01 et seq.)



...and with 3 this year, they now total 43...

- Ohio (Ohio Rev. Code §1349.19, §1347 et seq.)
- Oklahoma (Okla. Stat. §74-3113.1)
- **Oregon (SB 583)**
- Pennsylvania (73 Pa. Cons. Stat. §2303)
- Rhode Island (R.I. Gen. Laws §11-49.2-1 et seq.)
- **S. Carolina (S 453)**
- Tennessee (Tenn. Code §47-18-2107)
- Texas (Tex. Bus. & Com. Code §48.001 et seq.)
- Utah (Utah Code §13-44-101 et seq.)
- **Virginia (SB 307)**
- Vermont (Vt. Stat. Tit. 9 §2430 et seq.)
- Washington (Wash. Rev. Code §19.255.010)
- **West Virginia (SB 340)**
- Wisconsin (Wis. Stat. §895.507)
- Wyoming (SF 53)



...With 6 More in Process...

1. Alabama (SB 382, S.B. 489, S.B. 544)
2. Alaska (SB 21)
3. Iowa (SSB 3183)
4. Kentucky (HB 553)
5. Missouri (HB 2130)
6. Mississippi (HB 1408)

This Leaves only the following 2:

1. New Mexico, and
2. South Dakota



Inconsistent Breach Notice Laws

- **Personal Information** At a minimum, define "personal information"--as a name, in combination with a Social Security number, driver's license or state identification number, or financial account or debit card number plus an access code --the breach of which triggers the need to notify consumers
 - Some include passports or other forms of federal identification
- **Breach** Most apply only to breaches of unencrypted electronic personal information, and require written notification after a breach is discovered
 - Some require notice of encryption key is breached along with unencrypted data
- **Notification** Most require notification if there has been, or there is a reasonable basis to believe that, unauthorized access that compromises electronic has occurred
- **Risk of Harm** In some states, entities need not notify individuals of a breach if an investigation by the covered entity (sometimes in conjunction with law enforcement) finds no significant possibility that the breached data will be misused to do harm to the individual



Inconsistent Breach Laws (cont'd)

- **Enforcement Authority** Most give state's Attorney General enforcement authority.
 - A few provide a private cause of action
- **Law Enforcement Delay** Most allow for a delay in notification if a disclosure would compromise a law enforcement investigation, except Illinois
- **Substitute Notice** Most allow substitute notice to affected individuals via announcements in statewide media and on a Web site if more than 500,000 people are affected or the cost of notification would exceed \$250,000 -- RI, DE, NE, OH set lower thresholds
- **Security and Privacy Programs** Some require implementation of safeguards to protect information security and privacy (e.g., MD)
- **Safe Harbor** Some provide a "safe harbor" for covered entities that maintain internal data security policies that include breach notification provisions consistent with state law or federal law such as HIPAA and GLBA. (e.g., OH, MD)
- **Disposal** Some Require Proper Disposal of PI (e.g., MD, MA, OR)



2007 “SB 1386” Amendment

- Includes medical and health information in the definition of "personal information"
 - Such information can include medical history, diagnosis, policy number, subscriber number, an application, claims history, and appeals history
- Expands the state's Confidentiality of Medical Information Act to include in its scope businesses that handle or maintain medical information even if the business is not primarily engaged in maintaining medical records.
- Expands the scope of information required in breach notices to consumers which now must include:
 - who had the data;
 - when the breach occurred (date or estimated date),
 - a description of the categories of information involved,
 - A toll-free numbers to contact the responsible entity and the credit bureaus.



MN Plastic Card Security Act (Security Provisions)

Merchant Security

- HF 1758, amends Minnesota’s data breach notification law and contains security and liability provisions.
- The security provisions took effect August 1, 2007 and apply to any “person or entity conducting business in Minnesota” that accepts credit cards, debit cards, stored value cards or similar cards “issued by a financial institution.”
- Such companies are prohibited from retaining the following card data after authorization of a transaction:
 - “the full contents of a track of magnetic stripe data” (which encompasses the “card verification value” or CVV – a unique authentication code embedded on the magnetic stripe);
 - the three to four digit security code on the back of the card by the signature block (also known as CVV2); and
 - any PIN verification code number (If a *debit card* with PIN is used, a company is prohibited from retaining the data more than 48 hours after authorization of the transaction)



MN Plastic Card Security Act (Liability Provisions)

Merchant Liability

- For data breaches occurring after August 1, 2008, HF 1758 provides:
 - Authorize banks to file lawsuits to recover from the merchant "the cost of reasonable actions undertaken" to respond to the breach
 - Entitle banks to seek the costs of canceling and reissuing credit cards, closing and/or reopening accounts affected by a breach, stop payment actions, unauthorized transaction reimbursements and the providing of breach notice to affected individuals if a merchant retains such data in violation of the proposed law and there was a breach of that information.



Proposed Merchant Liability Laws

- **Iowa (SSB 3183)**, Intro. 2/14/08
 - **Would Require PCIDSS Compliance**
 - Failure to comply permits financial institutions to bring law suits (card replacement costs and actual damages) against merchants that do not comply
- **Washington (HB 2838)**, Intro 2/15/08
 - **Does not mention PCIDSS**. Would exempt a business from liability if it "met industry standards for the handling, processing, and storage of personal information
 - Would make merchants liable to banks for costs related to a breach of credit or debit card information
 - Liability. Any business that faced a breach incident in which 5,000 or more individual names or account numbers were compromised would be liable in negligence to affected financial institutions for the cost of replacing credit and debit cards and other costs reasonably undertaken to protect consumers
- **Alabama (SB 382), (Part of new Notice of Breach Law)**, Intro. 2/19/08
 - **Does not mention PCIDSS**, but bars covered entities that accept credit or debit card payments from storing unencrypted payment card transaction data
 - includes a provision to make merchants liable to banks for their costs associated with the breach of credit or debit card information.



Spyware -- State Laws

- Arizona
 - HB 2414
 - Arkansas
 - SB 2904
 - California
 - SB 1436, SB 92
 - Georgia
 - SB 127
 - Hawaii
 - Iowa
 - HF 614
 - Louisiana
 - HB 690
 - New York
 - A. 891F
 - Rhode Island
 - HB 6811
 - Utah
 - HB 104, amending HB 323
 - Virginia
 - HB 2471
 - Washington
 - HB 1012
- Proposed in 2007 and carried to 2008:**

Illinois (SB 1199, SB 1495); Maine; Massachusetts (SD 1800, HD 460); Michigan (SB 145); Mississippi (SB 2261); New York (S 3655, S 1459, A 340, A 4948) (Criminalization); Pennsylvania (HB 755, S.B. 711)



New 2008 State Spyware Efforts

- **Alabama (SB 145)**
 - Covers pop-ups and provides civil remedies of costs and fees, plus either actual damages or up to \$500 per pop-up occurrence
- **Hawaii HB 2033 (Criminalization), Intro. 1/11/08**
 - prohibits the knowing transmission of spyware or adware when used to collect PII or to modify settings on another's computer, including removing antivirus programs
- **West Virginia (HB 4053), Intro. 1/16/08; Passed by House 1/31/2008**
 - Would make the transmission of spyware and malicious adware unlawful; would prohibit (i) the collection of PII by "deceptive" means, and (ii) software transmissions that cause damage or cause multiple pop-up windows.
 - Prohibited activities that cause a loss of up to \$1000 would be punishable as a misdemeanor; more than \$1000 would be punishable as a felony
- **Florida (SB 1658) Intro. 2/7/08**
 - Would make it a third degree felony to add spyware or other "contaminants" onto a computer
- **Washington (HB 2879), Intro. 1/17/08**
 - adds a host of computer-related spyware provisions to Washington current spyware law, and changes the burden of proof for existing provisions



State Social Security Laws

- Over the last three years the number of states with some sort of SSN restriction law has grown from 8 to 39
- The Social Security Laws vary widely from state-to-state. Some prohibitions on SSN uses that are common are as follows:
 - public posting of SSN information;
 - use of SSNs on registration and service cards;
 - requiring SSNs for access to Web sites;
 - transmitting SSN data over the Internet;
 - sending mail with visible SSNs;
 - putting SSNs on faxes;
 - using SSNs as an employee ID number;
 - using SSNs as customer account numbers;
 - printing SSNs on pay stubs; and
 - selling SSNs.



State Bills Providing Electronic Health Record Incentives

- **State Pilot Programs**
 - West Virginia (S.B. 544), New Mexico (S.B. 341)
- **Tax Credit for EHR Technology Investment**
 - West Virginia (H.B. 2177)
- **Further Study of EHR issues**
 - Oklahoma (S.B. 1719), Washington (S.B. 6889), and West Virginia (H.B. 3225). New Jersey (A.B. 1391) H.B. 2177
 - Oklahoma (Exec. Order 2008-4) to establish the "Health Information Security and Privacy Council" to address electronic health records issues
- **Interoperability**
 - New Jersey (A.B. 1390), prohibits purchasing software or systems that are not interoperable
- **Implementation deadline**
 - Indiana (H.B. 1342) no later than Jan. 1, 2010



Other Health Data Bills

- Measures to clarify when particular individuals, i.e., patient's family, legal counsel, or an emergency health care provider, may access and share patient health information
 - **West Virginia (H.B. 2978)**, Genetic Information Privacy Act" Intro Jan. 9 would make the results of genetic testing confidential and would, in most circumstances, limit genetic test result disclosures to the individual being tested. Health insurers would be prohibited under the proposed law from requiring individuals to submit to genetic testing as a condition of insurance coverage.
 - **Pennsylvania (S.B. 1261)** Intro. Jan. 29 would amend the state's rules concerning patient notification and consent to HIV testing. The bill's introduction states that was introduced to better conform with federal Centers for Disease Control and Prevention (CDC) standards.
 - **Mississippi (H.B. 364)**, Intro. Jan. 29, would prohibit discrimination in coverage by health benefit plans on the basis of genetic information. The bill does not include a ban on employer discrimination based on genetic information
 - **Hawaii (H.B. 3384)** would allow a patient's attorney with proper authorization to copy, scan, and print a patient's medical records at the health care provider's premises.



Mining Prescription Data for Marketing

- In 2006, New Hampshire passed the first law in the nation restricting the use of prescription data for marketing
 - It provides that records of "prescription information containing patient identifiable and prescriber-identifiable data" may not be sold by pharmacy benefits managers, insurers, or mail order or Internet pharmacies for commercial purposes.
 - "Commercial purpose" is defined under the law as "advertising, marketing, promotion, or any activity that could be used to influence sales or market share of a pharmaceutical product, influence or evaluate the prescribing behavior of an individual health care professional, or evaluate the effectiveness of a professional pharmaceutical detailing sales force."
- April 2007, a federal court struck down the law IMS Health Inc. v. Ayotte, No. 01-cv-00280-PB (D.N.H. 4/30/07)
 - Limits on truthful commercial speech that do not promote unlawful activity are permissible only in if three conditions are met: The law must (i) support a "substantial government interest," (ii) directly advance that interest, and (iii) must not be more extensive than necessary to serve the government interest. According to the court, none of the three conditions were met.
- New Hampshire attorney general appealed the decision to the U.S. Court of Appeals for the First Circuit
 - The First Circuit heard oral argument in the case Jan. 9, but has not issued an opinion



Other Prescription Data Mining Bills

- **Maine (L.D. 4)** would allow prescription providers to keep their information private from drug companies and marketing firms
 - The law said that a prescriber could request confidentiality by registering with the state
 - A federal judge Dec. 21, 2007, struck down Maine's law on First Amendment grounds (7 PVLR 14, 1/7/08).
- **Vermont (S. 115)**
 - The data mining provision protects personally identifiable prescription information unless health care providers explicitly agree to waive the protection (opt-in)
 - Drug marketing companies challenged the Vermont law and the litigation is in the middle of active discovery before the U.S. District Court for the District of Vermont.
- **Arizona (S.B. 1251), Intro. 1/29/08**
 - would prohibit pharmacies, insurance companies and related entities from the transfer, use, or sale of prescription information that identifies the patient or prescriber
 - create an outright ban on the use of prescription information, making it similar to the New Hampshire law, which was found unconstitutional
- **Washington (S.B. 6241), Intro. 1/14/08**
 - would not completely ban the use of prescription data but would prohibit "the sale or use of prescriber-identifiable prescription data for commercial or marketing purposes absent prescriber consent"
- **Maryland (HB 50)**
 - would establish a registry for health care providers who want to consent to the use of data on their prescription-writing habits
 - allow the state to prohibit health insurers and drug marketers from using prescriber data if they have contracts with the state employee retirement system.

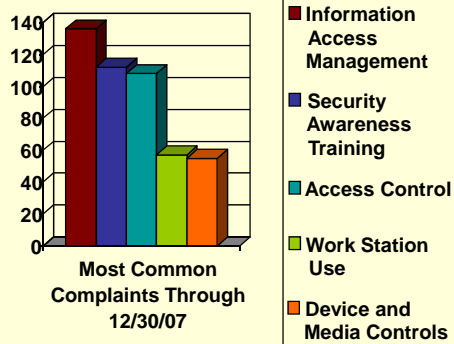


Agency Enforcement Actions and Private Litigation



HIPAA Security Enforcement

- According to CMS, as of September 2007 there are:
 - 379 Cases
 - 99 Open
 - 280 Closed
- To date, there have been no civil actions or fines imposed for HIPAA security violations.



Privacy Enforcement

- As of August 2007, 29,000 complaints were received by OCR in the past four years
 - Most common complaints are unauthorized use and disclosure of information, lack of safeguards, and failure to provide access to one's own medical records
- Approximately 9,600 of them have resulted in formal investigations
 - 7,000 cases have been resolved,
 - Two-thirds (approx. 4,600) resulting in agreements on corrective action and one third resulting in a finding of no violation
 - 410 cases have been referred to the Justice Department
 - 6,000 cases are pending

Comments of Linda Sanches, senior advisor in the HHS Office for Civil Rights at the Privacy Symposium 2007, August 23, 2007



FTC Security Enforcement

Deceptive Trade Practices

Based on notice of privacy practices and official statements regarding how an organization safeguards sensitive information. (e.g., In re Guidance Software Inc.)

Unfair Trade Practices

Practices that "threaten data security" are unfair practices. (e.g., In re BJ's Wholesale Club)

GLBA Safeguards

Violations of Safeguards Rule, (e.g., In re Superior Mortgage Corp.)



Enforcement/Consent Orders - FTCA

- In re Reed Elsevier Inc., FTC, File No. 052 3094, 3/27/08
- In re TJX Cos. Inc., FTC, File No. 072 3055 (3/27/08)
- United States v. ValueClick Inc., C.D. Cal., No. CV08-01711, (3/17/08)
- Life is good Inc., FTC, File No. 072-3046, (1/17/08)
- In re Guidance Software Inc., FTC, File No. 062 3057 (11/16/06)
- United States v. ChoicePoint, 106-cv-0198 (N.D. GA, 2-15-06)
- In re CardSystems Solutions Inc., FTC, File No. 052 3148 (9/5/06)

Total of 18 Cases



FTC Enforcement - GLBA Safeguards

- In re Goal Fin. LLC, *FTC*, No. 072-3013, (2/19/08)
- United States v. American United Mortgage Co., No. 07C 7064, (N.D. Ill., 12/17/07) (Disposal Rule)
- In re Nations Title Agency Inc., *FTC*, No. 052 3117, (5/10/06)
- In re Superior Mortgage Corp., *FTC*, File No. 052 3136, (9/28/05)
- In the Matter of Nationwide Mortgage Group, Inc., and John D. Eubank, *FTC* File No. 042-3104 4/15/05
- In re Sunbelt Lending Services, *FTC*, File No. 042-3153, 11/16/04)



Consent Orders and Security

Implement administrative, technical, and physical safeguards appropriate to the size, the nature of the company's activities, and the sensitivity of the personal information collected by each organization.

Security Program Elements:

1. designate an employee or employees to coordinate the information security program;
2. identify internal and external risks to the security and confidentiality of personal information and assess the safeguards already in place;
3. design and implement safeguards to control the risks identified in the risk assessment and monitor their effectiveness;
4. develop reasonable steps to select and oversee service providers that handle the personal information they receive from the companies; and
5. evaluate and adjust their information security programs to reflect the results of monitoring, any material changes to their operations, or other circumstances that may impact the effectiveness of their security programs

Biennial outside assessment of security programs basis for 20 years.

Auditors certification that the companies' security programs meet or exceed the requirements of the consent orders and are operating with *sufficient effectiveness* to provide reasonable assurance that the security of consumers' PI is being protected.

“US SAFE WEB Act”

- Undertaking Spam, Spyware, and Fraud Enforcement Beyond Borders Act" (S. 1608) authorizes the FTC to share information with foreign agencies that treat consumer fraud and deception as a criminal law enforcement issue. Signed into law December 22, 2006.
- U.S. SAFE WEB Act Cases
 - FTC v. Spear Sys. Inc., No. 07C-5597 (N.D. Ill. 10/3/07) used to share information with foreign enforcement partners in an investigation of international spam; obtained court order to halt email solicitations.
 - FTC v. B.C. Ltd. 0763496, (W.D. Wash.11/13/07) *preliminary injunction granted*). Federal Trade Commission's obtained an injunction against a fraud ring in Canada that placed telemarketing calls to U.S. residents listed on the FTC's do-not-call registry



U.S. InfoSec Litigation

“no court has considered the risk [of ID theft] itself to be damage”

- Guin v. Brazos Higher Educ. Serv. Corp. Inc., No. 05-668 (D. Minn. Feb. 2, 2006)
- Key v. DSW Inc., 454 F. Supp. 2d 684 (D. Ohio 2006);
- Bell v. Acxiom Corp., No. 4:06CV00458-WRW (E.D. Ark. Oct. 3, 2006)
- Stollenwerk v. Tri-West Healthcare Alliance., No. Civ. 03-0185 (D. Ariz. September 6, 2005)
- Forbes v. Wells Fargo Bank, No. 05-2409 (DSD/RLE) (D. Minn., March 16 2006)

This changes with actual damages

- TJX Class Actions (Discussed Next)



TJX Companies Breach

- **On Jan. 17, 2007**, TJX Companies Inc, including TJ Maxx, Marshalls and Home Goods announced that that the portion of its computer network that handles customer transactions was broken into by unauthorized individuals and at least 46.2 million credit and debit cards may have been compromised
 - This resulted in litigation and investigations consideration of new laws to protect banks in California, Connecticut, Illinois, Massachusetts, Minnesota New Jersey and Texas. Only the Minnesota law was actually enacted
 - have reduced what once was as many as 18 separate putative bank and consumer class action lawsuits against the company
- **September 2007** - Settlement include \$7 million to reimburse customers for credit monitoring and other identity theft mitigation measures they undertook and to hold a company wide one-day sale
- **November 2007** - Settlement with Visa (and issuing banks) \$40.9 million
- **December 2007** - TJX settled for \$40 million with banking associations and all but one individual bank that filed class actions seeking reimbursement of their costs associated with the breach, such as reissuing compromised credit cards and covering fraudulent purchases
- **April 2008** - Settlement with MasterCard (and issuing banks) \$34 million



New Security Breach Cases

- Hannaford Bros. Co. supermarket chain and its parent corporation Delhaize America Inc.
 - Over 12 separate class actions in Florida, Maine, New Hampshire and New York
- *Schaffer v. Davidson*, D. Mont., No. 2:08-cv-00019-SEH, *complaint filed 3/27/08*



FACTA Class Action Litigation

- Section 1681c(g) of the FACT Act provides that after Dec. 4, 2006 "no person that accepts credit or debit cards for the transaction of business shall print more than the last 5 digits of the card number or the expiration date upon any receipt provided to the cardholder at the point of the sale or transaction."

Acct: *****76775 Exp: ****

- Plaintiffs can recover a minimum of \$100 and up to \$1,000 in statutory damages per willful violation of the law (willful non-compliance. Plaintiffs can seek to recover actual damages for negligent violations of the law
- In early December, the first class action suits were filed in California for not complying with the FACT Act requirements
 - Toys-R-Us Delaware Inc., Rite Aid Corp. and Costco Wholesale Inc.; The Walt Disney Parks and Resorts; California Pizza Kitchen Inc., El Pololo, and Levy Restaurants; United Artists Theatre Circuit Inc.; FedEx Kinkos Office and Print Services Inc.; Valero Energy Corp.; and Avis Rent-A-Car Systems Inc.



FACT Act Litigation

- Willfulness, includes "reckless disregard of a legal obligation." Safeco Insurance Company of America v. Burr
- Superiority Clause
 - Is it the superior way to bring the case
 - California cases often held that financial impact on defendant for technical violation of FACTA would be disproportionate to any harm to the class



FACT Act Class Certification

- Harris v. Best Buy Co., No. 1:07-cv-02559 (N.D. Ill., *class certified* 3/20/08)
- Meehan v. Buffalo Wild Wings Inc., No. 07 C 4562 (N.D. Ill. *class certification granted* 2/26/08)
- Troy v. Red Lantern Inn Inc., No. 07 C2418 (N.D. Ill., *class certified*, 12/4/07)
- Halperin v. InterPark Inc., No. 07 C 2161 (N.D. Ill., *class certified* 11/29/07)



Transfers of Data from Europe for Litigation Preparation

- On 1/16/08, the French Data Protection Authority (CNIL) expressed concern in a statement over the increasing amount of data requests sent to French Companies under the FRCP --both personal and proprietary-- as part of preparation for litigation in the United States
- CNIL said it has identified three situations generating the majority of questionable data transfer requests:
 - documents or data transfers requested as part of "litigation hold" or "litigation freeze" procedures, in anticipation of judicial activity;
 - documents or data requested as part of pre-trial discovery; and
 - documents or data requested in response to injunctions issued by U.S. authorities, such as the Securities and Exchange Commission or the Justice Department, which are conducting various international investigations of corruption or compliance with the Sarbanes-Oxley Act.
- These issues will be put on the Agenda of the Article 29 Working Group



FRCP and DOC Safe Harbor

- Changes to the U.S. Federal Rules of Civil Procedure address treatment of electronically stored information (ESI) during discovery and litigation took effect Dec. 1, 2006
 - In part, the new rules require companies to retain all documents that may be relevant to pending and reasonably foreseeable litigation.
 - Some U.S. firms are asking foreign subsidiaries to conserve or transfer vast amounts of data, to avoid any potential violation of new rules on illegal or intentional destruction of documents.
 - For documents stored outside the United States, the retention and document production requirements may directly conflict with the EU Data Protection Directive (95/46/EC)
- The Safe Harbor program was implemented in 2000 as a means for U.S. companies to transfer PII to and from European Union countries and also comply with the EU Data Protection Directive.
 - Commerce certifies companies that supply adequate assurances of their commitment to privacy and security and includes them in a Safe Harbor registry.
 - As a result the U.S. Commerce Department's Safe Harbor program said that U.S. Companies have increasingly been seeking inclusion in the Safe Harbor.



Thank You!



M. Peter Adler
Attorney at Law

202.220.1278
Direct Fax: 800.684.2749
adlerp@pepperlaw.com

Hamilton Square
600 Fourteenth Street, N.W.
Washington DC 20005-2004
202.220.1200
Fax: 202.220.1665
www.pepperlaw.com

