

March 2, 2010



*Information
Security Law
Update 2010*

David G. Ries, Esq.

412-394-7787

dries@thorpreed.com

THORP REED
—  —
ARMSTRONG



1. Background

U.S. Information Security Law

“A Patchwork Quilt”



Data Governance

- **Information Security**
- **Records & Information Management**
- **Privacy**

Current Trends

- Generally increasing duties
- High level legal duties better defined
- Still substantial uncertainty
- Generally greater potential for liability



Information Security Laws

- 1. Laws protecting computers, networks and communications**
- 2. Laws requiring safeguards**
- 3. Other laws**



Computer Protection Laws

- 1. Computer Fraud and Abuse Act**
- 2. Electronic Communications Privacy Act**
- 3. State Laws**

Laws Requiring Safeguards

- Federal Information Security Management Act
- Financial Industries Modernization Act (GLB)
- Health Insurance Portability and Accountability Act (HIPAA)
- Children's Online Privacy Protection Act
- Fair Credit Reporting Act (FACTA)


Laws Requiring Safeguards

- Sarbanes-Oxley Act
- Family Educational Rights and Privacy Act
- Federal Trade Commission Act
- State Laws



2. The Emerging Legal Standard

- High level legal duties
- Better defined
- Consistent

- 
- **Develop, implement and maintain**
 - **A comprehensive information security program**
 - **Written**



■ Administrative, technical and physical safeguards

■ Appropriate to:

- Size and complexity**
- Nature and scope of activities**
- Sensitivity of information**

- 
- Based on a risk assessment
 - Designate responsibility



High Level Legal Standard

- Develop, implement and maintain a comprehensive, written information security program
- Appropriate administrative, technical and physical safeguards
- Based on a risk assessment
- Designate responsibility



“Reasonable” “Appropriate”

- **Legal requirements**

- **Standards and benchmarks**

Legal Requirements

Federal Agencies

- GISRA / FISMA
- National Institute for Standards and Technology (NIST)
(U.S. Dept. of Commerce)
- National Security Agency (NSA)

G-L-B, HIPAA, COPPA, state laws

Standards / Benchmarks

■ ISO Standards

– 17799:2000

– 27001:2005

■ FFIEC

■ Center for Internet Security

■ CERT

■ US-CERT

■ Legal Standards as guides: (NIST, NSA, OMB) (G-L-B, HIPAA, COPPA)

3. Data Breaches Continue

- ❑ High profile consumer data breaches
- ❑ Commercial data / intellectual property

Consumer Data Breaches

2009

 Breaches: 498

 Exposed: 222,477,043

2008

 Breaches: 656

 Exposed: 35,691,255

High Profile Breaches

BJs Wholesale Clubs



ChoicePoint



DSW Shoe Warehouse



CardSystems



Dept of Veterans Affairs



TJX



Hannaford Bros.



Heartland Payment Sys.





Consumer Data Breaches

Privacy Rights Clearinghouse

www.privacyrights.org/ar/ChronDataBreaches.htm

DataLossDB

<http://datalossdb.org/>

Interhack

Using Science to Combat Data Loss: Analyzing Breaches by Type and Industry

<http://web.interhack.com/publications/breach-taxonomy>

Privacy Rights Clearinghouse

Chronology of Data Breaches

Go to Breaches for [2005](#), [2006](#), [2007](#), [2008](#), [2009](#) or [2010](#).

DATE MADE PUBLIC	NAME(Location)	TYPE OF BREACH	NUMBER OF RECORDS
2005			
Jan. 10, 2005	George Mason University (Fairfax, VA)	Names, photos, and Social Security numbers of 32,000 students and staff were compromised because of a hacker attack on the university's main ID server.	32,000
Jan. 18, 2005	Univ. of CA, San Diego (San Diego, CA)	A hacker breached the security of two University computers that stored the Social Security numbers and names of students and alumni of UCSD Extension.	3,500
Jan. 22, 2005	University of Northern Colorado (Greeley, CO)	A hard drive was apparently stolen. It contained information on current and former University employees and their beneficiaries -- name, date of birth, SSN, address, bank account and routing number..	30,000
Feb. 12, 2005	Science Applications International Corp. (SAIC) (San Diego, CA)	On Jan. 25 thieves broke into a SAIC facility and stole computers containing names, SSNs, and other personal information of past and current employees. Stolen information included names, NNS, addresses, phone numbers and records of financial transactions.	45,000 employees
Feb. 15, 2005	ChoicePoint (Alpharetta, GA)	Bogus accounts established by ID thieves. The initial number of	163,000

		Letters and cards that contained one or more pieces of personal information were sent to incorrect addresses.	
Feb. 19, 2010	Valdosta State University (Valdosta, GA) http://www.valdosta.edu/notify/	A Valdosta State server that was reported as being breached could have exposed the information of up to 170,000 students and faculty. Valdosta State officials reported the discovery of a breach on Dec. 11 and estimated it began on Nov. 11. , the university said the grades and social security numbers of up to 170,000 students and faculty were exposed in the breach.	170,000
Feb. 24, 2010	Citigroup (New York City, NY)	About 600,000 Citigroup customers got a shock earlier this month when they received their annual tax documents with their Social Security numbers printed on the outside of the envelope. The digits were not identified as a Social Security number, and they were printed at the lower edge of the mailing envelope with and letters that resembled a number.	600,000

346,500,142



TOTAL number of records containing sensitive personal information involved in security breaches in the U.S. since January 2005. **346,500,142**
 What does the total number indicate?

Printing tip: Use the "landscape" setting for best results when printing the breach list.

4. Federal Enforcement Escalates

- Federal Trade Commission
- Dept. of Health and Human Services
- Securities and Exchange Commission
- Financial Industry Regulatory Authority (independent regulator)

FTC Enforcement

- Violation of laws & regulations
- Misrepresentations or false promises
-“Deceptive trade practices”
- “Unfair trade practices”

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

COMMISSIONERS: William E. Kovacic, Chairman
Pamela Jones Harbour
Jon Leibowitz
J. Thomas Rosch

In the Matter of

THE TJX COMPANIES, INC.
a corporation.

DOCKET NO. C-4227

In the Matter of

THE TJX COMPANIES, INC.
a corporation.

DOCKET NO. C-4227

order.

- Created an unnecessary risk to personal information by storing it on, and transmitting it between and within, its various computer networks in clear text;
- Did not use readily available security measures to limit wireless access to its networks, thereby allowing an intruder to connect wirelessly to its networks without authorization;
- Did not require network administrators and others to use strong passwords or to use different passwords to access different programs, computers, and networks;
- Failed to use readily available security measures, such as firewalls, to limit access among its computers and the Internet; and
- Failed to employ sufficient measures to detect and prevent unauthorized access to computer networks or to conduct security investigations, such as patching or updating anti-virus software.

FTC Press Release March 27, 2008



Department of Justice

FOR IMMEDIATE RELEASE
Tuesday, August 6, 2008
WWW.USDOJ.GOV

AG
(202) 614-2007
TDD (202) 614-1888

Retail Hacking Ring Charged for Stealing and Distributing Credit and Debit Card Numbers from Major U.S. Retailers

More Than 40 Million Credit and Debit Card Numbers Stolen

BOSTON – Eleven perpetrators allegedly involved in the hacking of nine major U.S. retailers and the theft and sale of more than 40 million credit and debit card numbers have been charged with numerous crimes, including conspiracy, computer intrusion, fraud and identity theft, Attorney General Michael B. Mukasey, U.S. Attorney for the District of Massachusetts Michael J. Sullivan, U.S. Attorney for the Southern District of California Karen P. Hewitt, U.S. Attorney for the Eastern District of New York Benton J. Campbell and U.S. Secret Service Director Mark Sullivan announced today. The scheme is believed to constitute the largest hacking and identity theft case ever prosecuted by the Department of Justice.

Three of the defendants are U.S. citizens, one is from Estonia, three are from Ukraine, two are from the People's Republic of China and one is from Belarus. One individual is only known by an alias online, and his place of origin is unknown.

Retail Hacking Ring Charged for Stealing and Distributing Credit and Debit Card Numbers from Major U.S. Retailers

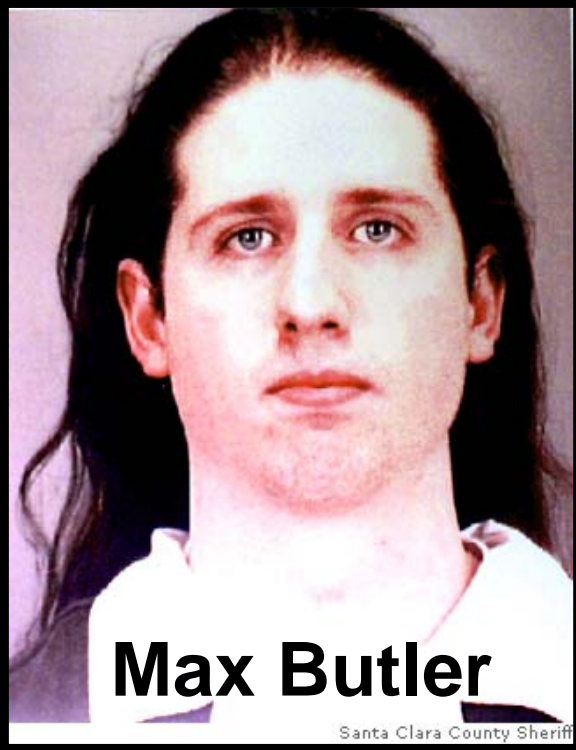
More Than 40 Million Credit and Debit Card Numbers Stolen

data in encrypted computer servers that they controlled in Eastern Europe and the United



- **TJX Companies**
- **BJ's Wholesale Club**
- **DSW Shoe Warehouse**
- **OfficeMax**
- **Boston Market**
- **Barnes & Noble**
- **Sports Authority**
- **Forever 21**
- **Hannaford Brothers**
- **7 Eleven**
- **Heartland Payment Systems**

Once inside the networks, they installed "sniffer" programs that would capture card numbers, as well as password and account information, as they moved through the retailers' credit and debit processing networks.



Max Butler

Santa Clara County Sheriff

Image Not Available NEWS RELEASE

MARY BETH BUCHANAN
UNITED STATES ATTORNEY
WESTERN DISTRICT OF PENNSYLVANIA

U.S. Post Office & Courthouse • 700 Grant Street • Suite 4000 • Pittsburgh, PA 15219 • (412) 644-3500

"ICEMAN," FOUNDER OF ONLINE CREDIT CARD THEFT RING, PLEADS GUILTY TO WIRE FRAUD CHARGES

United States Attorney Mary Beth Buchanan announced today, June 29, 2009, that Max Ray Butler, also known as Max Ray Vision, of San Francisco, California, has pleaded guilty in federal court in Pittsburgh to wire fraud charges.

"ICEMAN," FOUNDER OF ONLINE CREDIT CARD THEFT RING PLEADS GUILTY TO WIRE FRAUD CHARGES

- Stole 1.8 million credit card numbers
- Cost banks \$86.4 million

States Attorney Luke Dembosky advised the court that Butler, known widely on the Internet as "Iceman," among other aliases, conducted extensive criminal activity and caused significant financial damage to banks and other personal identification information. Many of these cards were provided to an accomplice, Christopher Aragon, based in the



For Release: March 27, 2008

Agency Announces Settlement of Separate Actions Against Retailer TJX, and Data Brokers Reed Elsevier and Seisint for Failing to Provide Adequate Security for Consumers' Data

In two unrelated Federal Trade Commission actions, discount retailer TJX and data brokers

Agency Announces Settlement of Separate Actions Against Retailer TJX, and Data Brokers Reed Elsevier and Seisint for Failing to Provide Adequate Security for Consumers' Data

According to the FTC complaint, TJX, with over 2,500 stores worldwide, failed to use reasonable and appropriate security measures to prevent unauthorized access to personal information on its computer networks. An intruder exploited these failures and obtained tens of millions of credit and debit payment cards that consumers used at TJX's stores, as well as the personal information of approximately 455,000 consumers who returned merchandise to the stores. Banks have claimed that tens of millions of dollars in fraudulent charges have been made on the cards and millions of cards have been cancelled and reissued.

Specifically, the agency charged that TJX:

- Created an unnecessary risk to personal information by storing it on, and transmitting it between and within, its various computer networks in clear text;
- Did not use readily available security measures to limit wireless access to its networks, thereby allowing an intruder to connect wirelessly to its networks without authorization;

HHS News

FOR IMMEDIATE RELEASE

Thursday, July 17, 2008

HHS, Providence Health & Services Agree on Corrective Action Plan to Protect Health Information

The U.S. Department of Health & Human Services (HHS) has entered into a Resolution Agreement with Seattle-based Providence Health & Services (Providence) to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules. In the agreement, Providence agrees to pay \$100,000 and implement a detailed Corrective Action Plan to ensure that it will appropriately safeguard identifiable electronic patient information against theft or loss.

HHS News

FOR IMMEDIATE RELEASE

Thursday, July 17, 2008

HHS, Providence Health & Services Agree on Corrective Action Plan to Protect Health Information

Director Wilkinson noted, "we commend Providence for their cooperation during the course of the investigation and for their voluntary implementation of comprehensive and system-wide improvements to protect individually identifiable health information."

The incidents giving rise to the agreement involved two entities within the Providence health system, Providence Home and Community Services and Providence Hospice and Home Care. On several occasions between September 2005 and March 2006, backup tapes, optical disks, and laptops, all containing unencrypted electronic protected health information, were removed from the Providence premises and were left unattended. The media and laptops were subsequently lost or stolen, compromising the protected health information of over 386,000 patients. HHS received over 30 complaints

**U.S. Department of Health & Human Services
News Release**

FOR IMMEDIATE RELEASE
Wednesday, February 18, 2009

Contact: HHS Press Office
(202) 690-6343

CVS Pays \$2.25 Million and Toughens Practices to Settle HIPAA Privacy Case

The U.S. Department of Health and Human Services (HHS) and the Federal Trade Commission (FTC) today announced that CVS, the nation's largest retail pharmacy chain, will pay the U.S. government a \$2.25 million settlement and take corrective action to ensure it does not violate the privacy of its millions of patients when disposing of patient information such as identifying information on pill bottle labels.

**U.S. Department of Health & Human Services
News Release**

FOR IMMEDIATE RELEASE
Wednesday, February 18, 2009

Contact: HHS Press Office
(202) 690-6343

CVS Pays \$2.25 Million and Toughens Practices to Settle HIPAA Privacy Case

The Privacy Rule requires health plans, health care clearinghouses and most health care providers (covered entities), including most pharmacies, to safeguard the privacy of patient information, including such information during its disposal.

Among other issues, the reviews by OCR and the FTC indicated that:

- CVS failed to implement adequate policies and procedures to appropriately safeguard patient information during the disposal process; and
- CVS failed to adequately train employees on how to dispose of such information properly.

Under the HHS resolution agreement, CVS agreed to pay a \$2.25 million resolution amount and implement a robust corrective action plan that requires Privacy Rule compliant policies and procedures for safeguarding patient information during disposal, employee training and employee sanctions for noncompliance.



SEC Charges LPL Financial for Failing to Protect Customer Privacy

FOR IMMEDIATE RELEASE
2008-193

Washington, D.C., Sept. 11, 2008 — The Securities and Exchange Commission today took an enforcement action against LPL Financial Corporation for failing to adopt policies and procedures to safeguard their customers' personal information, leaving at least 10,000 customers

SEC Charges LPL Financial for Failing to Protect Customer Privacy

San Diego. Under the Safeguards Rule of Regulation S-P of the federal securities laws, broker-dealers and SEC-registered investment advisers like LPL are required to adopt policies and procedures reasonably designed to safeguard customer information. The firm agreed to pay a \$275,000 penalty to settle the SEC's enforcement action without admitting or denying the findings.

"With the increase in the number of incidents involving information security breaches, regulated firms must be vigilant about satisfying their obligation to protect customer information from anticipated threats and unauthorized access," said Linda Chatman Thomsen, Director of the SEC's Division of Enforcement. "Today's action demonstrates the Commission's commitment to holding those firms responsible for their deficient controls, policies, and procedures, particularly when personal customer information is at issue."

Rosalind Tyson, Regional Director of the SEC's Los Angeles Regional Office, added, "Regulated entities should make it a priority to protect their customers' private information. LPL disregarded this crucial responsibility even in the face of known security deficiencies, and information of at least 10,000 customers may have been exposed as a result."



NEWS RELEASE

For Release: Tuesday, April 28, 2008
Contacts: Nancy Condon (202) 728-8378
Herb Perone (202) 728-8484

FINRA Fines Centaurus Financial \$175,000 for Failure to Protect Confidential Customer Information

Firm Will Provide Free Credit Monitoring to Customers

Washington, D.C. — The Financial Industry Regulatory Authority (FINRA) has announced today that it has fined Centaurus Financial, Inc. (CFI), of Orange County, CA, \$175,000 for its failure to protect certain confidential customer information. Centaurus was also ordered to provide notifications to affected customers and their brokers

FINRA Fines Centaurus Financial \$175,000 for Failure to Protect Confidential Customer Information

Firm Will Provide Free Credit Monitoring to Customers

unauthorized access to their system," said Susan L. Merrill, FINRA Executive Vice President and Chief of Enforcement. "When a firm becomes aware of an unauthorized access, it must conduct an effective review and provide customers with accurate information about that unauthorized access."

On July 15, 2007, CFI's fax server was used by an unauthorized third party to host a phishing scam. Phishing scams are designed to trick computer users into divulging personal information such as usernames, passwords and bank and credit card information. A file simulating a popular Internet auction site was uploaded to CFI's fax server and over a three-day period there were 894 unauthorized logins by 459 unique IP addresses, most of them from recipients of a mass email sent by the perpetrators of the scam.

Following the discovery of the phishing scam, CFI sent a misleading letter to approximately 1,400 customers and their brokers, inaccurately stating that the unauthorized access was limited to one person and that information on the server was not openly available. The letter failed to state that other unauthorized logins had occurred and did not inform the customers that the unauthorized access was made possible by the inadequate firewall and weak username ("Administrator") and password ("password") on its computer fax server.

CFI's conduct violated federal Regulation O-P and FINRA rules.




Under the terms of the settlement, Centaurus has agreed to provide corrected notifications of the unauthorized accesses to all previously notified customers and brokers and to offer these customers one year of free credit



5. States Lead in New Laws

- Data Breach Notice
- Credit Freeze
- Reasonable Security
- Encryption
- Secure Disposal
- Liability for Breaches

States Lead in New Laws

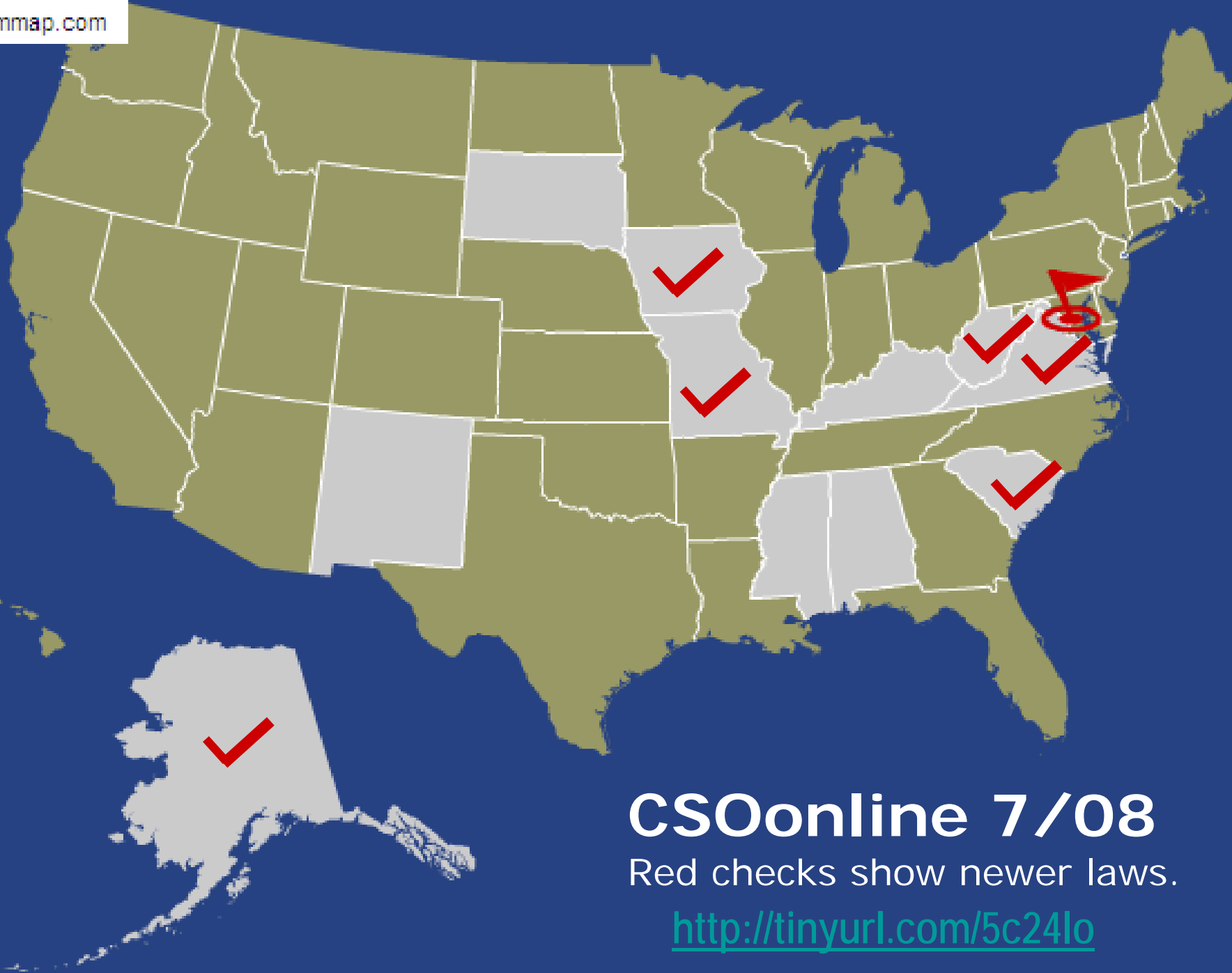
 Data Breach Notice	- 45
 Credit Freeze	- 25
 Reasonable Security	- 12
 Encryption	- 6
 Secure Disposal	- 21
 Liability for Breaches	- 2

State Laws

Breach notification

- Cal Database Security Breach Notification Act
- 45 states
- PA law 73 P.S. §2301-2329
- List of laws:
<http://tinyurl.com/pmyrmb>

“Doing Business”



CSOonline 7/08

Red checks show newer laws.

<http://tinyurl.com/5c24lo>





Notice of Breaches

- Information covered
- Entities covered
- Definition of “breach”
- Who must be notified
- Risk of harm
- Time of notice
- Form or method of notice
- Exceptions
 - Safe Harbor
 - Encryption



New Mass. Law - M.G.L. c. 93H

 “persons who own, license, store or maintain personal information about a resident of the Commonwealth of Massachusetts”

 “shall develop, implement, maintain and monitor a comprehensive, written information security program”



New Mass. Law - M.G.L. c. 93H

Office of Consumer Affairs and Business Regulation

- 201 CMR 17.00:
Standards for The Protection of
Personal Information of
Residents of the Commonwealth
- Effective March 1, 2010
- www.mass.gov/Eoca/docs/idtheft/201CMR1700reg.pdf

Federal Laws

■ Several bills pending in Congress

■ No comprehensive law passed to date

■ H.R. 2221
Passed House 12/09

“Data Accountability and Trust Act”

www.govtrack.us/congress/billtext.xpd?bill=h111-2221

111TH CONGRESS
1ST SESSION **H. R. 2221**

To protect consumers by requiring reasonable security policies and procedures to protect computerized data containing personal information, and to provide for nationwide notice in the event of a security breach.

IN THE HOUSE OF REPRESENTATIVES

APRIL 20, 2009

Mr. RUSH (for himself, Mr. STEARNS, Mr. BARTON of TEXAS, Mr. SCHAKOWSKY, and Mr. RADANOVICH) introduced the following bill, which was referred to the Committee on Energy and Commerce

A BILL

To protect consumers by requiring reasonable security policies and procedures to protect computerized data containing personal information, and to provide for nationwide notice in the event of a security breach.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*
3 SECTION 1. SHORT TITLE.

4 This Act may be cited as the “Data Accountability
5 and Trust Act”.

6 SEC. 2. REQUIREMENTS FOR INFORMATION SECURITY.

7 (a) GENERAL SECURITY POLICIES AND PROC-

8 DURES.—



6. Economic Stimulus

The American Recovery and Reinvestment Act of 2009

Health Information

Technology for Economic and Clinical Health (HITECH) Act

- promote the use of electronic health records by all hospitals and physicians by 2015
- enhanced privacy & security

HITECH

- **HIPAA privacy & security rules extended to business associates**
 - Definition of “business associates” expanded
- **Breach notice requirement**
- **Increased enforcement and penalties**

American Recovery and Reinvestment Act of 2009 (Public Print)

Subtitle D—Privacy

SEC. 13400. DEFINITIONS.

In this subtitle, except as specified otherwise:

(1) BREACH- The term 'breach' means the unauthorized acquisition,

American Recovery and Reinvestment Act of 2009

respectively, was made in good faith and within the course and scope of the employment or other contractual relationship of such employee or agent, respectively, with the covered entity or business associate and if such information is not further acquired, accessed, used, or disclosed by such employee or agent.

(2) BUSINESS ASSOCIATE- The term 'business associate' has the meaning given such term in section 160.103 of title 45, Code of Federal Regulations.

(3) COVERED ENTITY- The term 'covered entity' has the meaning given such term in section 160.103 of title 45, Code of Federal Regulations.

(4) DISCLOSE- The terms 'disclose' and 'disclosure' have the meaning given the term 'disclosure' in section 160.103 of title 45, Code of Federal Regulations.

(5) ELECTRONIC HEALTH RECORD- The term 'electronic health record' means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.

(6) HEALTH CARE OPERATIONS- The term 'health care operation' has the meaning given such term in section 164.501 of title 45, Code of Federal Regulations.

(7) HEALTH CARE PROVIDER- The term 'health care provider' has the meaning given such term in section 160.103 of title 45, Code of Federal Regulations.

7. Victims Face An Uphill Battle

Consumers

- Increased Risk
- Victims of ID Fraud or ID Theft

Financial Institutions

Common Law

■ Contract

■ Negligence

■ Products Liability

■ Directors' & Officers'
Liability





Heartland Payment Sys.

- I. Negligence
- II. Breach of Contracts
(Third Party Beneficiaries)
- III. N.J. Consumer Fraud Act
- IV. Negligence *Per Se*
- V. Negligent
Misrepresentation

Louisiana Restaurants Case

15th JUDICIAL DISTRICT COURT

LAFAYETTE PARISH

STATE OF LOUISIANA

NO.

SECTION:

CRAWFISH TOWN, USA, INC., DON'S SEAFOOD & STEAK HOUSE, INC.,
MANSY ENTERPRISES, LLC, MEL'S DINER PART II, INC., AND
SAMMY'S, LLC, and SAMMY'S OF ZACHARY, LLC

VERSUS

COMPUTER WORLD, INC. AND RADIANT SYSTEMS, INC.

JURY DEMAND

PETITION FOR DAMAGES

NOW INTO COURT, through undersigned counsel, comes petitioners, Crawfish Town USA, Inc., et al., who file this Petition for Damages and represent the following:

PLAINTIFFS

1.

Made plaintiffs herein are:

Crawfish Town USA, Inc., a Louisiana corporation.

Don's Seafood & Steak House, Inc., a Louisiana corporation.

Mansy Enterprises, LLC, d/b/a Picante's Mexican Restaurant, a Louisiana corporation.

Mel's Diner Part II, Inc., a Louisiana corporation.

Sammy's, LLC, d/b/a Sammy's Grill, a Louisiana limited liability company.

Sammy's of Zachary, LLC, d/b/a Sammy's Grill, a Louisiana limited liability company.

DEFENDANTS

2.

8. Red Flags Update

- FACTA “Red Flag” Rule
- November 1, 2008 deadline
- Enforcement extended to May 1, 2010
only for entities regulated by FTC



9. Contracting for Security

- Reasonable and appropriate safeguards
- Current industry standards
- Comply with all applicable laws and regulations
- Questionnaire
- Inspection / audit
- Notice of material changes



Contracts Requiring Safeguards

- HIPAA, G-L-B, etc.
- Payment Card Industry Data Security Standard (PCI)
- Outsourcing
- Business partners

10. E-Discovery

- Federal Rules Amendments (effective Dec. 1, 2006)
- “electronically stored information”
- Legal Hold or Litigation Hold
- Expense + Risk of Sanctions



Legal Hold or Litigation Hold

■ When is it required?

- the trigger

■ What must be preserved?

-the scope

■ How should it be done?

-the process



The *Zubulake* Duty

1. Issue a “litigation hold” at outset and periodically reissue.
2. Communicate directly with the “key players.”
[key custodians / IT]
3. Instruct all employees to produce copies of relevant electronic files.
4. Make sure that all backup media which the party is required to retain is identified and stored in a safe place. [all files and media]

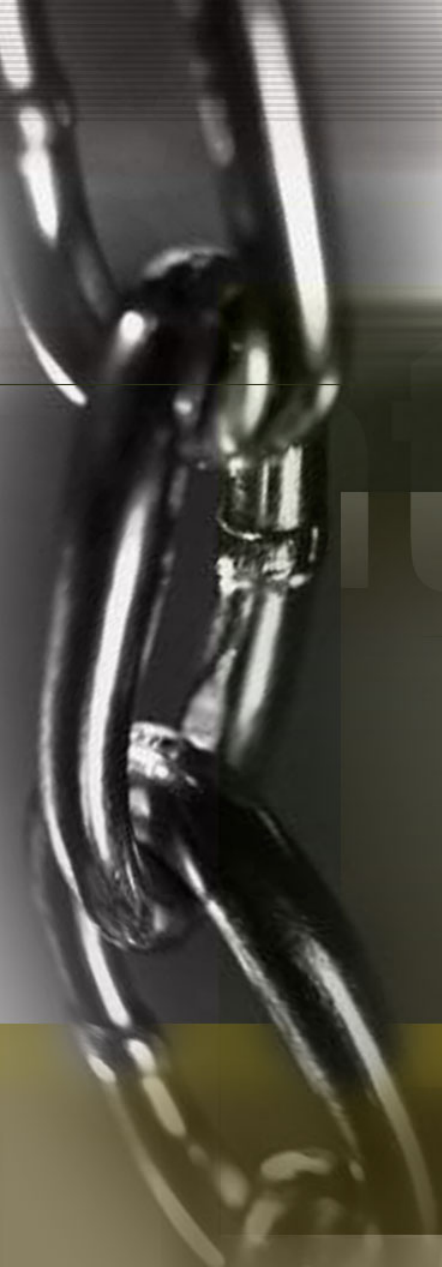


Pension Committee

(S.D.N.Y. Jan. 15, 2010)

“ Possibly after October, 2003, when *Zubulake IV* was issued, and definitely after July, 2004, when the final relevant *Zubulake* opinion was issued, the failure to issue a *written* litigation hold constitutes gross negligence because that failure is likely to result in the destruction of relevant information.”

- Opinion available at <http://tinyurl.com/yjhb76x>



Questions

THORP REED
— & —
ARMSTRONG