



# Secure Date CE Seminar January 13<sup>th</sup> , 2011



**“We Work for You”**

**A New Breed of Wholesaler**

## *Agenda:*

- The world today versus 10 years ago
- Secure Data versus Identity Theft
- Understanding what created all this new exposure?
- How Technology companies helped create dilemma
- Impact on Financials Institutions
- Impact on Educational Institutions
- Impact on Healthcare Industry and HITECH law
- Claims, Coverage and forms

## *Secure Data*

*“Understanding the exposures and the infrastructure of the new economy”*

*“Information technology pervades all aspects of our daily lives, our national lives... Disrupt it, destroy it or shut down the information network, and you shut down America as we know it.”*

- *Tom Ridge, Secretary, Department of Homeland Security*

## *Privacy Issues*

### ***Collection and dissemination of user information***

“You already have zero privacy. Get over it.”

**Scott McNealy, CEO, Sun Microsystems**

## *TECHNOLOGY INDUSTRY-DYNAMIC PACE OF CHANGE*

- ***Radio took 30 years to reach 50 million Americans***
- ***Television took 13 years to reach 50 million***
- ***Internet- Lightning speed and accelerating- reached 100 million Americans in only 6 years.***
  - Today's computer chips are over 20,000 times more powerful than those introduced by Intel in the 1970s.

*There is no such thing as a **totally** secure computer or network, except one that is turned off!*

## *Secure Data versus Identity Theft*

- **Identity theft** occurs to individuals who might have credit cards, social security numbers, and other private information stolen or lost which will allow access to their private financial resources or funds.
- **Secure data** is the information that corporations and business entities control and have a legal and fiduciary responsibility to protect and provide a secure environment for that proprietary data by using a standard of care spelled out by certain generic and specific industry laws and benchmarks. IE. Gramm Leach, HIPAA, Secure data CA1386/1798, HITECH etc

## *US Market Trends the last 5 years.*

- Shifts in value. *Intangible assets account for more than 87% of the value of US businesses, up from 38% in 1982. - Brookings Institute Unseen Wealth, '07 2<sup>nd</sup> edition*
- Information productivity of higher importance. *77% of Fortune 500 companies now measure information productivity and 73% have created Chief Security Officer positions for data protection. – Forbes '06*
- Unsustainable lack of tech provider accountability. *Software quality problems cost the US \$60B per year, and users bear 2/3's of cost – NIST '06*
- Emergence of technology compliance. *New data standards are HIPAA for Health Care and Gramm-Leach Bliley (GLB) for FS, NSIT/FISMA for Government – Information and Technology '04*
- Cyber crime on the rise. *38% ID Theft increase in '04. CIO Magazine '05*
- Technology is pervasive and growing. *Already represents 13% of the US GDP, up from 3% in 1992. - IDC '07*
- IT Professional Certifications on the Rise. *US demand for IT Security certifications up 34% in '04. Computerworld, Feb '06*

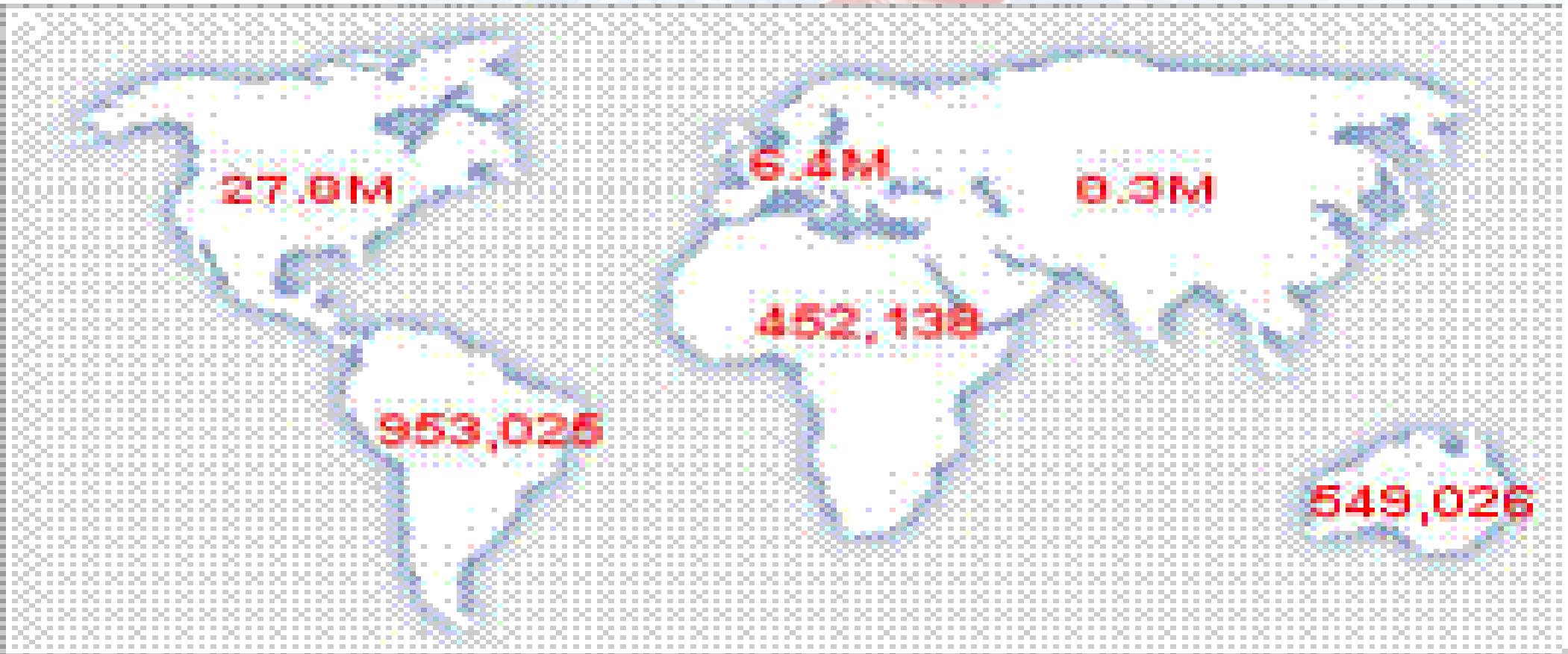
## *The New Technology Infrastructure Risk*

- Everyone has a computer or PDA
- Predicted to be one of the fastest growing areas of Professional Liability.
- Privacy Practice and Related compliance (Gramm-Leach-Bliley 501B/ HIPAA Compliance, Red Flag Rules, PCI, HITECH)
- Sarbanes-Oxley (proper records/information management)
- California Information Security Law 2004 (sb 1386/1798) etc.
- Universal Access (e.g. visually impaired Web discrimination)
- Tech E&O (malpractice) no governance nor legal standard of care
- Trademark and copyright
- Unauthorized and prolific access to personal information
- Denial of access
- Proliferation of websites
- Creation of “Chief Security Officers” in many public firms

**sample of live network attacks/ events from last 24 hours**

**50% have 1,000 employees or less and 26% were on companies with 11 to 100 employees**

*Are the Risks Real?....*





# Encryption

*If data are encrypted even though the state may utilize an acquisition based trigger, there generally is no reporting obligation.*

- Encryption is usually defined as the use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without the use of a confidential process or key.
- However, some states like Massachusetts require the use of at least 128-bit encryption to protect any personal data in transit including information sent via e-mail, laptops, external hard drives, USB memory sticks, CDs, etc. (201 CMR 17.00)(effective January 1, 2010).

## *How Much Does a Data Breach Cost?*

- **The average cost of a data breach in 2009 was \$204 per lost customer record up from \$125 in 2006**
- **The average total cost per breach is \$6.75M up from \$4.7m in 2006**
- **High end claim cost for 2009 \$31m and low cost \$750,000**
- \$4.4M or \$140 per record is lost business.
- The other \$2.2M or \$64 per record is comprised by the following
  - Internal Investigation
  - Attorney's Fees
  - PR Spin
  - Customer Notification
  - Call Center Support
  - Crisis Management/media cost
  - Credit Monitoring
  - Regulatory Investigation defense costs
  - **Replacement and reissue of credit cards (Minn.)**

\*(Ponemon Institute study 2009)

# *Typical Costs:*

## **Notification Costs:**

- \$1 to \$2 per individual

## **Credit Monitoring:**

- \$10 to \$20 per person per year
- 15% to 20% acceptance rate

## **Credit Card Replacement**

- Cost and fees for cancelling and reissuing credit cards (Minnesota)

## **Claim Defense:**

- Cost to defend class action suits may be significant!
  - Hannaford
  - Bank of New York Mellon Corp.
  - Triwest Healthcare
  - **Heartland** (may become largest breach thus far)
  - CVS



High-Tech & High-Touch Solutions  
for your Professional Liability Insurance needs.

# What created this new exposure?

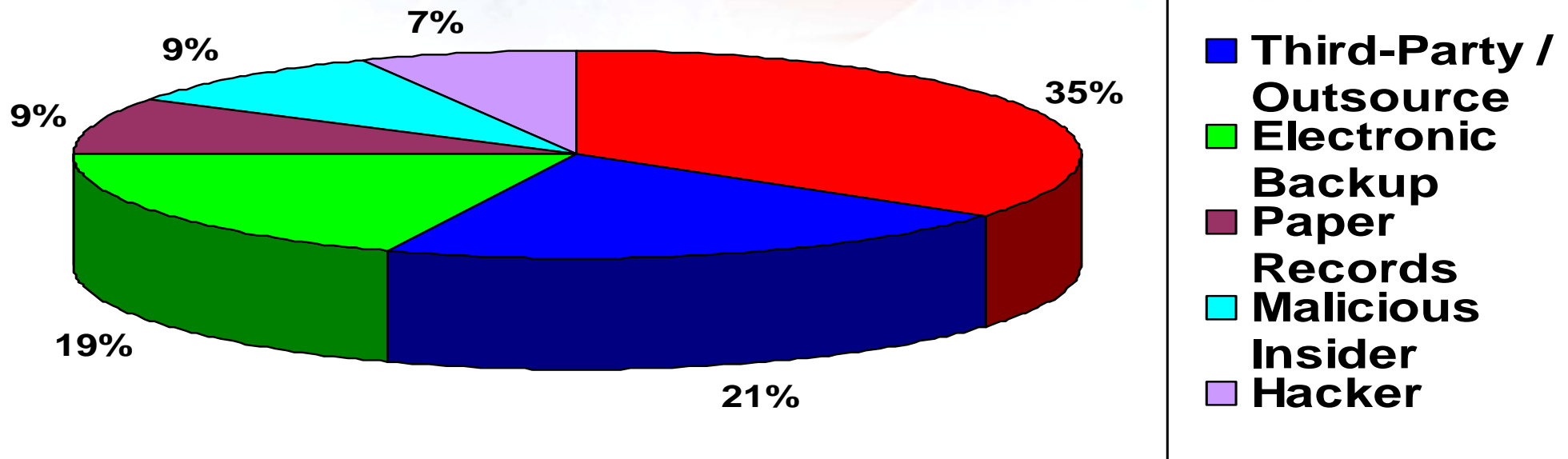
## *Data Breach Notification Laws – California Leads the Way*

- California Security Breach Information Act (Senate Bill 1386 and revised 1798) enacted on July 1, 2003. Since then, 44 states have passed similar laws.
  - At the heart of these laws is the requirement that companies storing personal information must promptly notify persons whose information may have been accessed by an unauthorized person.
  - California Assembly Bill 1798 went into effect on January 1, 2008. It expands the definition of “personal information,” as that term is used in California’s data breach notification laws, to include medical and health information and applies to all entities, whether or not they are health care providers.
  - In addition to costs of notification, these laws create potential civil liability if proper and timely notification of a data security breach is not given.

## *Other Recent Notable legislation*

- Processing Card Industry Standards (PCI)
- Digital Discovery Laws (6/30/05)
- FACTA /Fair and Accurate Credit Transactions Act
- **FTC “Red Flag Rule” regulations (11/01/08)** *delayed until May of 09 , delayed to August 09, further Delayed Nov 1, 2009, finally Take effect January 2011*
- American Restoration and Recovery Act (ARRA) HITECH Feb 2009 effective 2/17/2010

# Privacy Risks - Where is the Danger



## *Example Breach Statistics*

- 85% of businesses have experienced a data security breach
- 46% of businesses failed to implement encryption solutions even after suffering a data breach.... and 82% did not seek legal counsel prior to responding to the incident despite having no prior response plan in place.
- 95% of businesses suffering a data breach were required to notify data subjects whose information was lost or stolen.
- 1 in 3 breaches were attributed to lost or stolen equipment. The cost associated with these incidents is higher at \$225

### Damages:

- 74% report loss of customers.
- 59% faced potential litigation.
- 33% faced potential fines.
- 32% experienced a decline in share value.
- Almost half of the breach incidents were attributed to lost or stolen equipment such as laptops, PDAs, and memory sticks. The second largest threat came from negligent employees, temporary employees, and/or contractors.
- direct and indirect costs of replacing a credit or debit card runs at \$186 per card.

Source: Ponemon Institute (700 cos)

# Breach Timeline

A Breach is discovered

After Identifying the applicable Notification requirements the company must begin to notify all affected parties at a cost of \$1-\$2 per record

The company must begin to enroll those affected parties in a credit monitoring program for a period of no less than 12 months. Each person accepting the credit monitoring costs \$10-\$20 per year.

The insured must go before any state or federally required regulatory/penalty hearings. Fines and penalties will be state specific.

Experts and Forensic specialists are hired to identify the cause of the breach and how to prevent further exposure.

All of these costs could have been prevented!!!

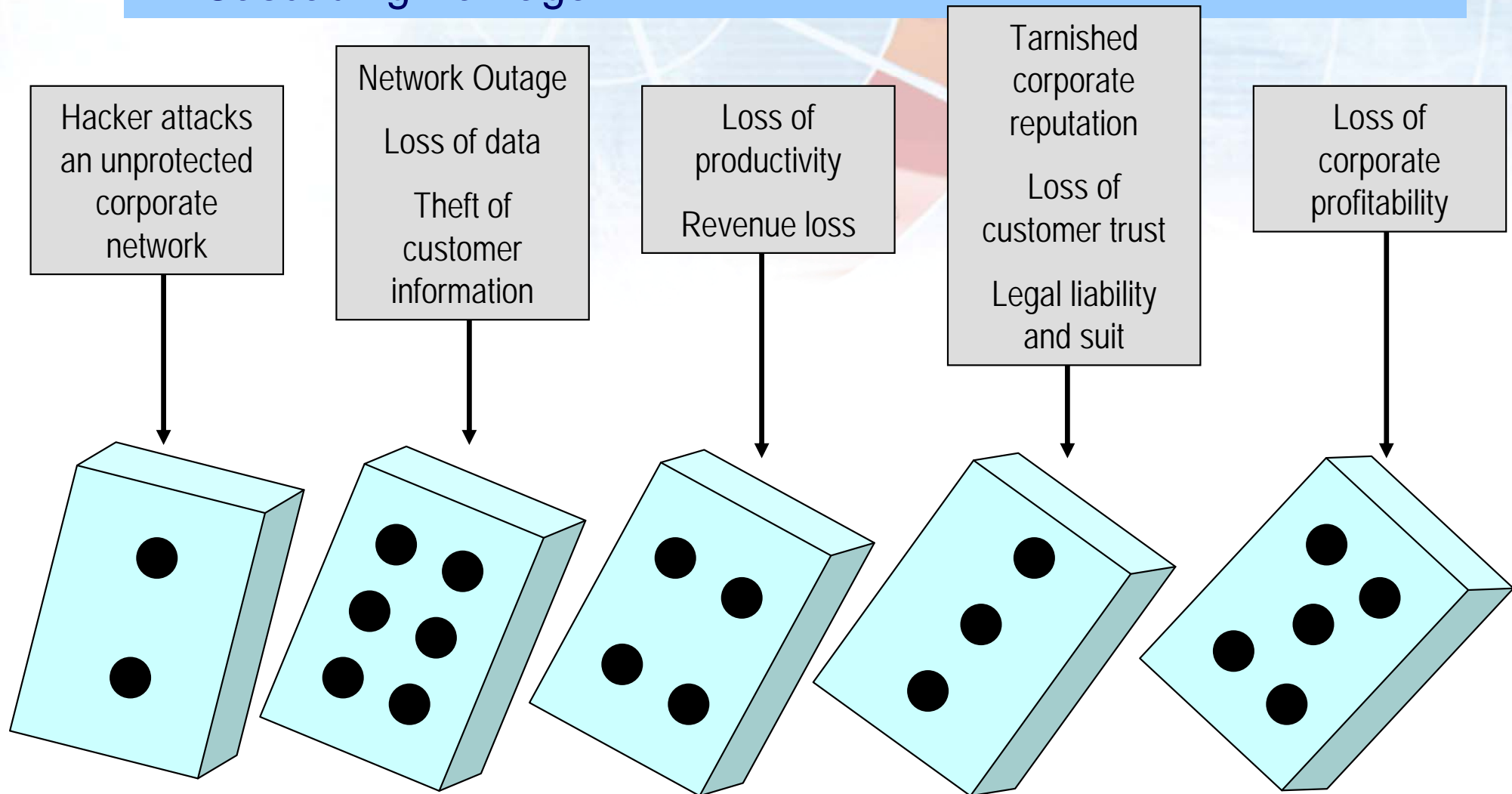
These exposures can be covered through insurance

The total cost of an average breach is \$204 per record affected. These requirements can be triggered by even a potential breach

The insured would ideally hire a PR firm to help control bad press, provide damage control and act as a spokesperson for the organization

## What can happen?

### .... Cascading Damage



## *The situation today.....*

- Minimizing costs no longer an option because of legal reporting requirements and notification laws
- Case law is evolving and limited, as are guidelines and regulations
- Overwhelmed/uninformed patent office
- Globalization of economic enterprise, Global Coverage?
- Outdated insurance contract wording “Cyberspace Activity” “Cyber Toxicity”?, Negligent acts, Description of insured’s professional service, CGL 101 excludes all electronic data?
- Insurer’s quite often make their own language and policy structure
- “No” Standard of Care or certification for Technology professionals, 70% of all projects end in failure!
- **One to many Exposure versus typical one to one**
- Leads to many class action suits
- Can we ever insure the internet?
- All and any associated Healthcare Information exposure

# *TECH Companies!*

*Are we taking off in plane we can't land?*

*Who is building our infrastructure?*

# Actual Tech Application, go figure!

Please describe any percentages listed above: \_\_\_\_\_

11. Do you provide eCommerce services that promote the sale of goods and/or the ability to transfer funds (i.e. online monetary exchange for goods and services, shopping cart, credit card processing)?  Yes  No

12. (a) Describe the 3 largest jobs or projects within the last three years:

Name of Client	Services Provided	Gross Billings
Nucor Steel Marion Inc.	CAD Draftsman & Product Support	~\$400,000
Vibe Social Jukebox	System Admin & Website	~\$10,000
EZCash Check Cashing	Application Development	~\$10,000

- (b) If in business less than 1 year or a start up company, please describe the industries you are targeting for your products

and/or services? Any and all ... if you pay me, I work. Bio-Pharma - Banking - Industrial Fab - Highway Safety - Internet & Ecommerce

## Whose Watching the Technology Professionals?

- All Professionals are all intertwined and reliant on technology professionals for our infrastructure
- Lack of professional standard of care or regulatory oversight
- Multinational Outsourcing and use of independent contractors
- Global ramifications and worldwide exposures
- Constant Patches and updates to secure and to correct applications
- Background Checks and Qualification?

# *Are Technology Professionals Licensed?*



## Simple things

Can be built by one person  
Learning by doing is OK  
Requires  
    Minimal modeling  
    Simple process  
    Simple tools

## Complex things

Requires a holistic view of the goals  
Requires planning and coordination  
Requires knowledge of all the individual parts  
Experience is a key to success  
Requires Modeling – ability to abstract details to  
    simpler diagrams and graphics  
Methods (defined processes)

## *Are the Risks Real?*

....a growing threat matrix

<b>virus damage</b>	<b>hackers</b>	<b>cyber extortion</b>	<b>Internet liability</b>
<b>human mistakes</b>	<b>Web vandals</b>	<b>denial of service</b>	<b>Web site disability access discrimination</b>
<b>computer /server malfunctions</b>	<b>rogue administrators</b>	<b>ASP service outage</b>	<b>malicious code transmission</b>
<b>Intellectual property infringement</b>	<b>privacy breach</b>	<b>ISP outage</b>	<b>Unix &amp; Windows O.S. Flaws</b>

## *What are the network emanating risks*

### First Party – Network Asset Exposures

- Data and software (modified, stolen, deleted)
- E-money (stolen, extorted)
- Information and trade secrets (modified, stolen, deleted)
- Business interruption (lost revenue and profits)

### Third Party – Legal Liability

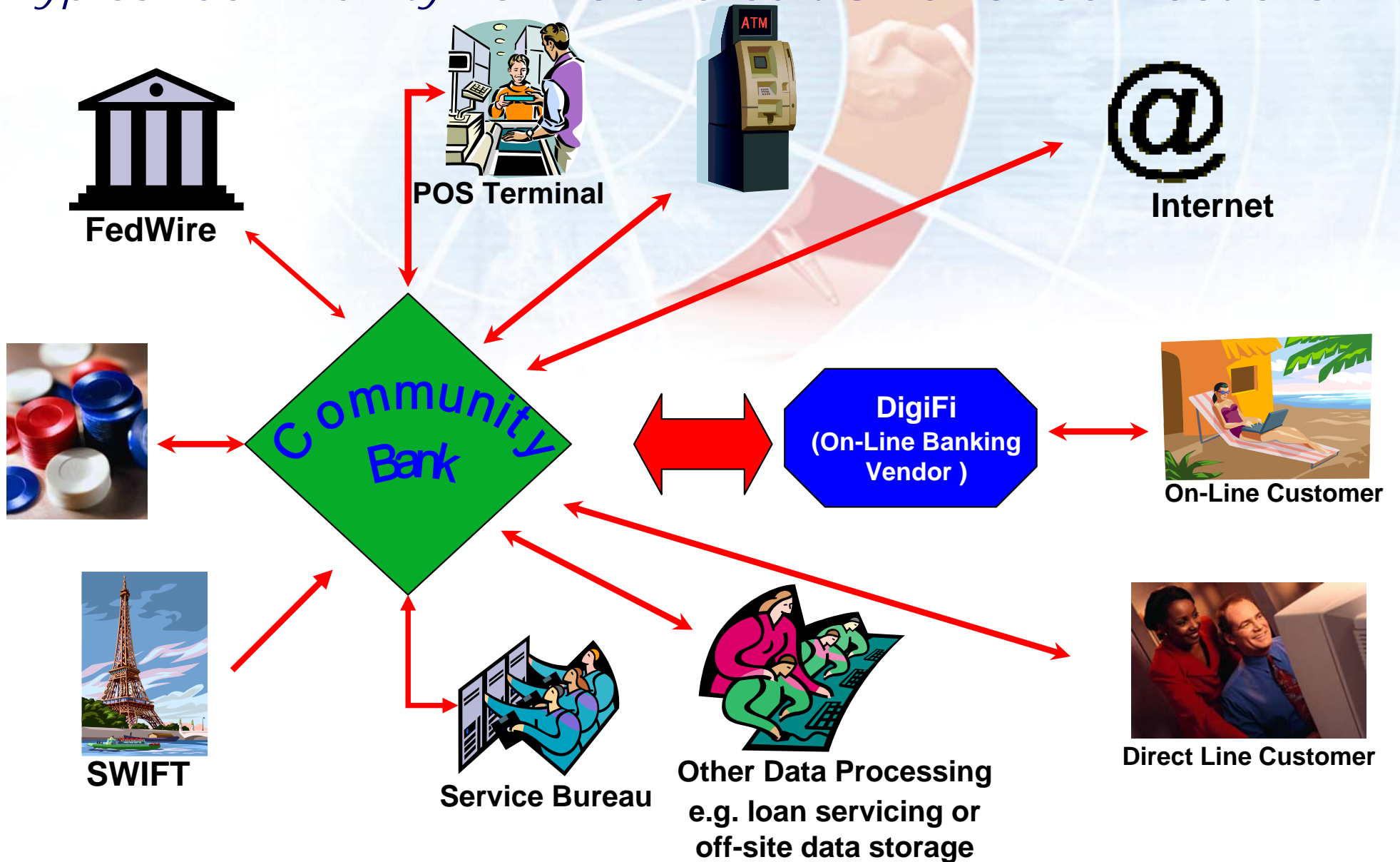
- Computer virus transmission (to customers, etc.)
- Privacy policy breach (leak of customer NPI, data or paper records)
- Software glitch (E&O)
- ASP – Service Outage (damages due to no access)
- Attacks against 3<sup>rd</sup> party sites (Zombie launch pad)
- Website activities: intellectual property infringement (trademark or copyright)



High-Tech & High-Touch Solutions  
for your Professional Liability Insurance needs.

# *Financial Institutions*

# A Typical Community Bank's or Credit Union's "Connections"



## *Gramm-Leach-Bliley Act*

*"The Financial Modernization Act of 1999"*

Three Principal Parts to the Federal Legislation:

**1. The Financial Privacy Rule**

Governs the collection and disclosure of customers personal financial information.

**2. Safeguards Rule**

Requires financial institutions to design, implement, and maintain safeguards to protect customer information.

**3. Pretexting Provisions**

Protect consumers from individuals and companies that obtain their personal financial information under false pretenses

### **Recent Red Flag Rules**

## *Red Flag Rules, Take effect January 2011*

**An alphabet soup of government agencies, including the OCC, the FTC and the FDIC, had a hand in the implementation of various regulations, together referred to as the Red Flag rules.. Rather, the Red Flag rules are found in Sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003 ("FACTA"), and require various entities to implement procedures for detecting and preventing identity theft. Not surprisingly, these rules are challenging in their scope and complexity.**

**One of the most challenging aspects of the rules concerns who or what is covered by them. Technically, the Red Flag rules apply to “financial institutions” and “creditors” with “covered accounts.”**

**Covered accounts include (1) an account...primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, and (2) any other account...for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft. 12 C.F.R. § 222.90(3).**

**Old Language: In other words, any company that permits a customer to defer payment is covered by the rules.**

**Updated language on 12/03/2010:**

**Due to concerns over how this broad definition might affect unsuspecting businesses, the new legislation relies on the definition of "creditor" under Section 702 of the Equal Credit Opportunity Act and sets forth the following requirements in order to meet the definition of "creditor":**

- **Obtains or uses consumer reports in connection with a credit transaction**
- **Furnishes information to consumer reporting agencies in connection with a credit transaction; or**
- **Advances funds to or on behalf of a person, based on an obligation of the person to repay the funds.**

**According to a published colloquy in the Senate in support of the bill, the purpose of the Act is to exclude businesses that pose little risk for consumers. Senator Dodd stated that the bill makes clear that lawyers, doctors, dentists, orthodontists, pharmacists, veterinarians, accountants, nurses and other health care and service providers will no longer be classified as "creditors" for purposes of the Red Flags Rules, just because they do not receive payment in full from their clients at the time that services are provided. The colloquy further indicates that the FTC has delayed enforcement of the Red Flags Rule specifically to wait for Congressional clarification on this issue.**

**\*Multiple challenges and law suits from Medical groups, CPA, Lawyers etc delaying implementation of this law**

## *Heartland Financial, possibly largest claim thus far*

- Announced on Obama Inaugural Day 1/20/09, some say to minimize impact?
- TJX was 45m cards and Heartland is over 100m cards
- Already affected 665 financial institutions
- Multiple Class action lawsuits already filed (31 to date)
- Claims that announcements and monitoring offerings were misrepresented to effected card holders
- Arrests have occurred and appears to be large organized syndicate
- Long way from being over already \$12m in costs for first 6 months
- Incident trigger will be critical
- 50% loss of stock value
- One bank reissued 400,000 credit and debit cards
- What would impact be with New Minnesota law?

## *National Claims Examples*

- **Banks:** Kellogg Community Federal Credit Union says that a computer containing personal information on an undisclosed number of members was stolen. A file containing names, addresses, SSN, birth date was on the computer's hard drive.
- **Credit Card Company:** TJX Cos. reported 46.5 million customers credit and debit cards stolen in January 2008. *update current costs at \$256m 2009 with over \$200k for class action alone*
- **Mortgage Broker/Banker:** LendingTree had a privacy breach in April 2008 that exposed personal data such as income and job information on an undisclosed number of users.
- **Insurance Agent:** CS Stars, an independent insurance brokerage; says the names, addresses, and SSN's for 540,000 injured workers may have been lost.
- **Insurance Company:** Wellpoint [health benefits company] said two computer servers on which the records were stored were maintained by a third party vendor and were not properly secured between 2007 and 2008. 130,000 customers' protected health information, personal records, and SSN's have been exposed over the internet for an unspecified period of time.
- **Processing Company:** Between 2004 to present, CardSystems is facing a class action lawsuit over security breach which may have exposed 40 million credit card numbers to fraud.



High-Tech & High-Touch Solutions  
for your Professional Liability Insurance needs.

# *Educational Market*

## *Educational Institutions*

- Difficult class to insure
- Educational institutions represent 13% of total US Institutions but account for 30% of all data breach incidents
- Typically, colleges and universities track students by Social Security number and have for many years. Some recently have moved away from this practice.
- Breaches in last 12 months: Georgetown, University of Maryland, Harvard, Notre Dame University, NYU, Penn State, Baylor, University of Texas, Modesto City Schools, CA State University, Cornell, Virginia Commonwealth University, Johns Hopkins, Irving Texas Schools, etc

## *Harm to Third Parties as the Result of an Electronic Data Security Breach*

- Two basic claims of damages by third parties when their private electronic information is compromised.
  - **Identity Theft** – The illegal use of an individual’s personally identifiable information to assume that person’s identity, usually for the purpose of obtaining money or other valuable goods or services.
  - **Invasion of Privacy** – The public disclosure of private information.



High-Tech & High-Touch Solutions  
for your Professional Liability Insurance needs.

# *Healthcare Industry*

## Some of the Other Well Known Laws that Apply to Private Electronic Information

- **HIPAA - Health Insurance Portability and Accountability Act**
  - Establishes regulations for the use and disclosure of Protected Health Information (PHI). PHI is any information about health status, provision of health care, or payment for health care that can be linked to an individual. Since updated by the American Recovery and Reinvestment Act (ARRA)
  - Covered entities are any health care related business that stores or transmits health care data in any way. They now all fall under HIPAA regulations.
  - The Security Rule of HIPAA deals specifically with Electronic Protected Health Information (EPHI). The Rule identifies various security standards required to protect this information.
  - Per California Security Breach Information Act, potential **Civil Liability Exposures** have been created
  - American Restoration and Recovery Act (ARRA) HITECH language and HIPAA fines increased to max of \$1.5m

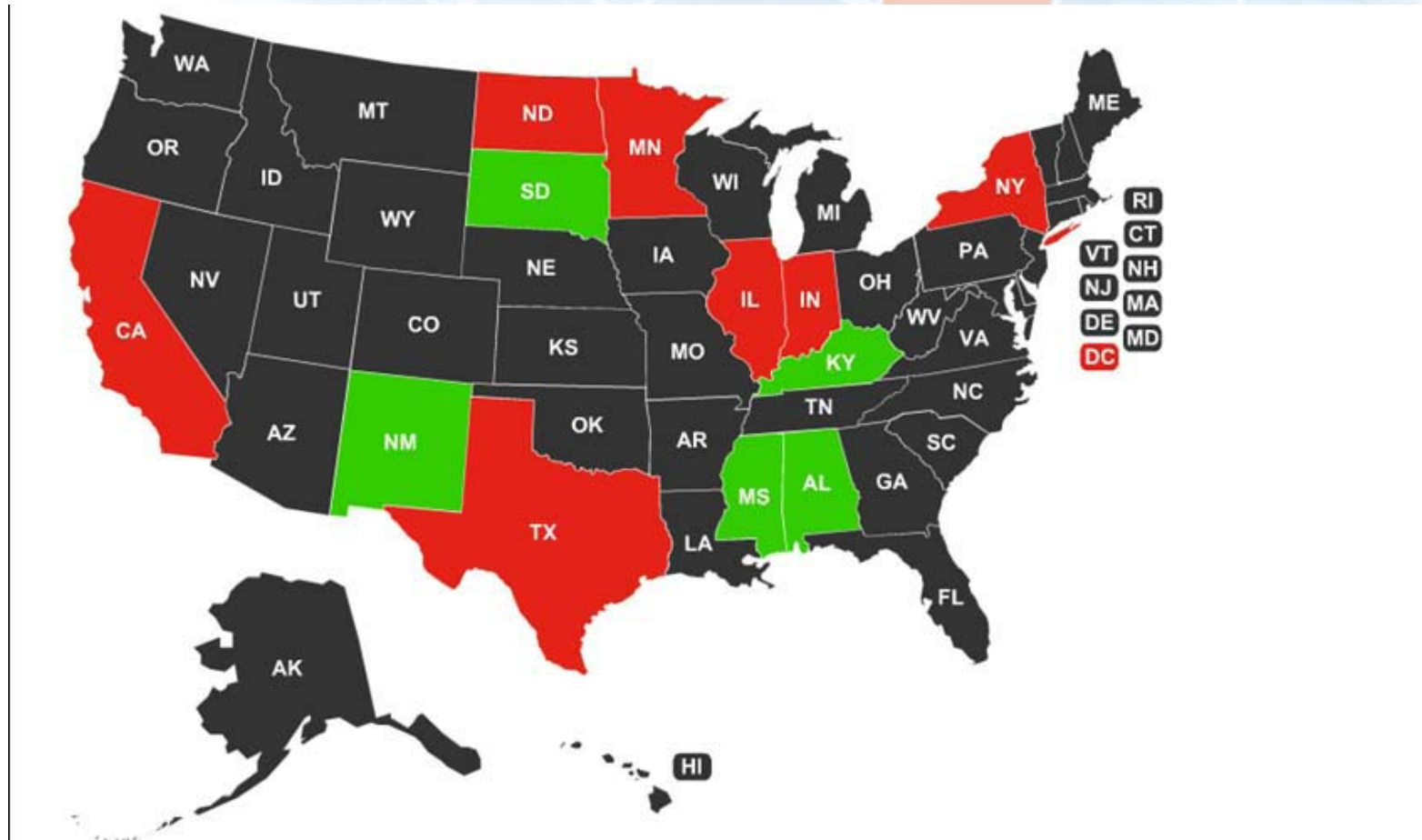
*Health and Information Technology for Economic and  
Clinical Health Act (HITECH)  
American Recovery and Reinvestment ACT*

- Clarifies that any associated entity with Protected Healthcare information (PHI) both paper and electronic is responsible under HIPAA and HITECH
- Increased HIPAA fines from \$150k to \$1.5million and can be levied by State Attorney Generals
- Fines can range from \$100 to \$50,000 per individual violation
- Notification Changes effective Feb 17<sup>th</sup> 2010
- Annual ongoing log for small breaches under 500 records
- Defers to secure data vs HITECH depending on most stringent

## *HITECH continued*

- Compliancy audit will become annual standard from the Office of Civil Rights which oversees Health Information but not quite sure yet how this will be scheduled
- In depth method to police both Business Associate and Covered entity (Provider of service)

# *At Risk States / Versus Acquisition*



Red –Acquisition Based  
Black –Risk Based  
Green –None Available

## Healthcare Industry Wide Exposure

- Potential for Data Loss & Damage Increases Exponentially when Stored Digitally (Servers, PC's, Laptops, CD's....)
- Electronic Transportability (via e-mail, Excel, PDF's...)
- Unauthorized Acquisition of or Access to Sensitive Data
- Hacker / Physical Theft / Improper Display / Insider Access / Lost Backup
- 30% of all stored data is healthcare related
- All associated entities and healthcare information now falls under HIPAA

## *Recent HITECH Compliance incident*

- The Attorney General of CT has already filed a complaint against several health plans alleging HIPAA violations under the HITECH Authority act. The complaint includes late notice, ineffective policies in place and failure to train employees. The state is seeking injunctive relief under HIPAA and states law resulting in fines of 5k per incident.
- Notification requirements of affected parties are based on their state of residence not the company's location. This means the company would have to conform to the statutes and regulations in each state. Currently, each state has unique and different laws in place that make it difficult to adhere to this rule without the help of a third party.
- HITECH reporting requirements are unique in that they apply to ERISA plans for data breaches occurring for business associates and administrative entities as well. The breach extends beyond the affected company onto other parties that are responsible for the handling of the data. \*
  - This is new because it opens up the associates and insured's to notification requirements

# *Affinity Health Plan*

## **Insurer alerts 400,000 after data found on leased copy machines**

April 21, 2010 - Howard Anderson, Managing Editor, [HealthcareInfoSecurity.com](http://HealthcareInfoSecurity.com)

A New York managed care plan has learned an important lesson about leased copy machines: Many contain hard drives that should be scrubbed of information before the copiers are returned.

Affinity Health Plan has notified more than 409,000 customers, clinicians, employees, job applicants and others about a breach related to personal information stored on the hard drives of copiers it returned to a leasing company. The health plan also notified three state agencies plus federal authorities.

Under the HITECH Act's breach notification **rule**, breaches affecting more than 500 individuals must be reported to federal authorities and the media within 60 days.

"Like many organizations across the country, we were not aware copy machines contained hard drives that need to be wiped," says Abenaa Abboa-Offei, senior vice president of customer and community connections at Affinity. The insurer chose to "cast as wide a net as possible out of an abundance of caution" in deciding how many people to notify about the breach as the investigation of what data was on the copiers

## *Medical Claims Examples*

### **Providence Class Action Lawsuit and HIPAA Fines**

**Providence Home Services of Portland Oregon in 2006 had 365,000 records stolen on laptops and backup tapes that were not encrypted and contained patient information including financial information on some patient records.**

**Consequence:**

**Oregon attorney general in 2008 forced secure data settlement to include monitoring and reimbursement of personal losses and severe measures to update and encrypt all future information and submit to random inspection measures to be monitored by Health and Human Services Dept including a \$100,000\* fine for lack of HIPAA standards of care. The class action suit is still open and ongoing. Costs already over \$1.2m**

***\*ARRA/ HITECH increased HIPAA fines to \$1.5m***

# *Virginia Department of Health Professions*

Extortion demand posted on WIKI leaks seeks \$10m to return 8 million patient records and 35 million prescriptions allegedly stolen from Virginia Dept of Health.

Cyber extortion coverage, BI/PD questions

## CVS Pharmacy

- January 16, 2009, CVS accepted \$2,250,000 penalty and Corrective Action Plan (CAP) to settle complaint stemming from its practice of disposing of old prescriptions and prescription bottles
  - The CAP requires: Revising and distributing its policies and procedures regarding disposal of protected health information;
  - Sanctioning workers that do not follow the policies and procedures;
  - Training workforce members on these new requirements;
  - Conducting internal monitoring;
  - Engaging a qualified, independent third-party assessor to conduct assessments of CVS compliance with the requirements of the CAP and render reports to HHS;
  - New internal reporting procedures requiring workers to report all violations of these new privacy policies and procedures; and
  - Submitting compliance reports to HHS for a period of three years.
- Subsequently, OCR issued PHI Disposal FAQs

## Who are Potential Markets for these New Coverages?

- Health Care Providers such as Hospitals, Doctor Offices, Surgery Centers, home healthcare
- Pharmacies, Med Spas, Dentists, Physical Therapists, MRI Centers, Radiologist etc
- Chiropractors – Acupuncture – Pain Centers
- Health Plan Providers, Laboratories, Optician
- Medical Transcriptionists / Medical Records Storage
- TPA's, All benefit related organizations etc etc
- **Anyone and everyone who has Electronic Healthcare Info**

## *How Much Does a Data Breach Cost?*

- **The average cost of a data breach in 2009 was \$204 per lost customer record up from \$125 in 2006**
- **The average total cost per breach is \$6.75M up from \$4.7m in 2006**
- **High end claim cost for 2009 \$31m and low cost \$750,000**
- \$4.4M or \$140 per record is lost business.
- The other \$2.2M or \$64 per record is comprised by the following
  - Internal Investigation
  - Attorney's Fees
  - PR Spin
  - Customer Notification
  - Call Center Support
  - Crisis Management/media cost
  - Credit Monitoring
  - Regulatory Investigation defense costs
  - **Replacement and reissue of credit cards (Minn.)**

\*(Ponemon Institute study 2009)



## Example Breach Notice

High-Tech & High-Touch Solutions  
for your Professional Liability Insurance needs.

### URGENT ALERT

Dear \_\_\_\_\_:

At COMPANY, we take your privacy very seriously. That is why we are very sorry to have to report to you that \_\_\_\_\_ . The theft occurred on \_\_\_\_\_. We have no reason to believe that the thieves gained access to the password-protected information on the laptop, let alone of any fraudulent or other misuse of your information by the thieves or anyone else, but want you to be aware immediately of this event. Meanwhile we are engaged in a thorough review of this incident to determine how we can better protect your information.

There are some actions you can take to help protect yourself against misuse of your personal information, in the event that it is ever compromised. You can go to [www.annualcreditreport.com](http://www.annualcreditreport.com) and get a copy of your credit report. This service has now been made available across the United States at no charge to you.

You may also wish to call the toll-free number of any of the three major credit bureaus and place a fraud alert on your credit report. As soon as any one credit bureau receives your fraud alert it will notify the other two. The credit bureaus are:

Equifax Credit Information Services, Inc.  
(888) 766-0008  
P.O. Box 740241  
Atlanta, GA 30374  
[www.equifax.com](http://www.equifax.com)

Experian  
(888) 397-3742  
[www.experian.com](http://www.experian.com)

TransUnion  
(800) 680-7289  
Fraud Victim Assistance Division  
P.O. Box 2000  
Chester, PA 19022  
[www.transunion.com](http://www.transunion.com)

The websites for all three credit reporting agencies have additional helpful information on how to protect your information. If you have any questions, please call \_\_\_\_\_ at \_\_\_\_\_.

Very truly yours,



High-Tech & High-Touch Solutions  
for your Professional Liability Insurance needs.

# *Claims and Coverage Examples*

## *A Scenario - The Unattended Laptop*



**Jack's laptop computer is stolen when he leaves it unattended in an airline club at the Newark Airport.**

**On the laptop are the names, account numbers, Social Security numbers and dates of birth of 25,000 persons his bank considers to be their Gold Level customers and 500 persons they plan to solicit as customers.**

**The brazen laptop thief sends his bank's CIO an e-mail with a link to a URL, at which the list of customers and prospective customers is now posted.**

**The thief will publish the link on a computer bulletin board unless he is paid \$250,000.**

## Technology E&O? Financial Institution Incident

Programmer was an Independent contractor born in India and employed by a technology company building a CRM system for the bank. Contract called for the bank to not provide any proprietary information to programmers in populating the data base. The programmer was however in lieu of contract given private information. After completing the project the programmer wanted to show his mother back in India what he had done.

He posted on his personal website a link to the software he built so his mother could see. An executive from the bank saw the link and followed to their bank website where the contents showed social security numbers of bank personnel, account #'s and other specific secure data.

Bank sued the technology company for assorted breach of contract and secure data law malfeasance. Technology company had only GL and no E&O or secure data law coverage.

Costs ran in the multimillion dollar range for notification and compliance of states secure data laws. Can coverage be argued or not

# Recent Class action

10 IN THE SUPERIOR COURT OF THE STATE OF CALIFORNIA  
 11 IN AND FOR THE COUNTY OF SAN FRANCISCO  
 12 Unlimited Jurisdiction  
 13 ERIC PARKE and ROYAL SLEEP ) Case No.  
 14 CLEARANCE CENTER, INC., a California )  
 15 corporation, On Behalf Of Themselves, All ) CLASS ACTION  
 16 Others Similarly Situated, and in the Interest of )  
 17 the General Public of the State of California, ) COMPLAINT FOR DECLARA  
 18 Plaintiffs, ) INJUNCTIVE RELIEF; VIOLA  
 19 vs. ) CALIFORNIA BUSINESS AN  
 20 CARDSYSTEMS SOLUTIONS, INC., a ) PROFESSIONS CODE §§ 1720  
 21 CORPORATION, a corporation; MERRICK BANK ) UNFAIR, UNLAWFUL AND I  
 22 CORPORATION, a corporation; VISA ) BUSINESS PRACTICES  
 23 INTERNATIONAL SERVICE )  
 24 ASSOCIATION, a corporation; VISA U.S.A. )  
 25 INC., a corporation; MASTERCARD )  
 INTERNATIONAL INCORPORATED, a )  
 corporation; and DOES 1-200, inclusive, )  
 Defendants.

UNITED STATES DISTRICT COURT  
 CENTRAL DISTRICT OF CALIFORNIA **BY FAX**

JENNIFER HARRINGTON and  
 JESSICA SEYMOUR,  
 Plaintiffs,  
 v.  
 CHOICEPOINT, INC., a corporation;  
 and CHOICEPOINT SERVICES,  
 INC., a corporation,  
 Defendants.

Case No. CV05 1294 SJO JWJx  
**FIRST AMENDED CLASS  
 ACTION COMPLAINT**  
 Complaint Filed: February 22, 2005  
 Trial Date: None

THIS IS A CLASS ACTION COMPLAINT

UNITED STATES DISTRICT COURT  
 DISTRICT OF MASSACHUSETTS

PAULA G. MACE, on behalf of herself  
 and all others similarly situated,  
 Plaintiff,  
 v.  
 TJX COMPANIES, INC.,  
 Defendant.

Civil Action No: \_\_\_\_\_  
 COMPLAINT - CLASS ACTION  
JURY TRIAL DEMANDED

**PLAINTIFF'S CLASS ACTION COMPLAINT**  
 Plaintiff Paula G. Mace ("Plaintiff") hereby brings this class action suit against TJX

## *TJ Maxx settlement (TJX Cos.)*

- Agreed to pay total of \$9.75 million with 41 states attorneys
- \$2.5 for states security fund, \$5.5 settlement, \$1.75m to cover states investigations
- Bank Re-issue of cards not included
- Doesn't include other costs to date, defense costs, PR costs, Crisis management, etc
- Incident trigger still in dispute with carrier
- 11 people accused and 4 pleading guilty

“Safeguarding personal information isn't just good business, it's crucial for our economy,” Washington state Attorney General Rob McKenna said.

# *Regulatory Exposures*

## *Case Example*

- **January 2006 - The FTC announced ChoicePoint Inc. (a data broker) will pay \$15 million** to settle charges that its security and record-handling procedures violated consumers' privacy rights and federal laws.
- The agency charged that ChoicePoint violated the FTC Act by making **false and misleading statements about its privacy policies** [Choicepoint had publicized privacy principles that address the confidentiality and security of personal information it collects and maintains] .
- At Least 800 Cases of Identity Theft Arose From Company's Data Breach [financial records of more than 163,000 consumers in its database had been compromised]
- The settlement requires ChoicePoint to implement new procedures - must establish and maintain a comprehensive information security program **and to obtain audits by an independent third-party** security professional every other year until 2026.
- Costs can be significant to monitor for 20 years

## *"Grocer Hannaford hit with class action Suit over data breach"*

March 21, 2008

Hannaford Bros. Co. has been hit with two class action lawsuits filed on behalf of consumers whose credit and debit card numbers were compromised as a result of a major security breach.

A Philadelphia law firm, Berger & Montague, said it filed suit Wednesday in U.S. District Court in Portland, alleging that the supermarket chain was negligent for failing to provide adequate security for computer data. Hannaford Chief Executive Ron Hodge offered an apology for the intrusion. There are 165 Hannaford stores in the U.S. Northeast and 106 Sweetbay supermarkets in Florida.

"We sincerely regret any concern or inconvenience this has caused," Hodge said in a statement. "We have taken aggressive steps to augment our network security capabilities."

## *How Much Does a Data Breach Cost?*

- **The average cost of a data breach in 2009 was \$204 per lost customer record up from \$125 in 2006**
- **The average total cost per breach is \$6.75M up from \$4.7m in 2006**
- **High end claim cost for 2009 \$31m and low cost \$750,000**
  
- \$4.4M or \$139 per record is lost business.
- The other \$2.2M or \$63 per record is comprised by the following
  - Internal Investigation
  - Attorney's Fees
  - PR Spin
  - Customer Notification
  - Call Center Support
  - Crisis Management/media cost
  - Credit Monitoring
  - Regulatory Investigation defense costs
  - **Replacement and reissue of credit cards (Minn.)**

\*(Ponemon Institute study 2009)

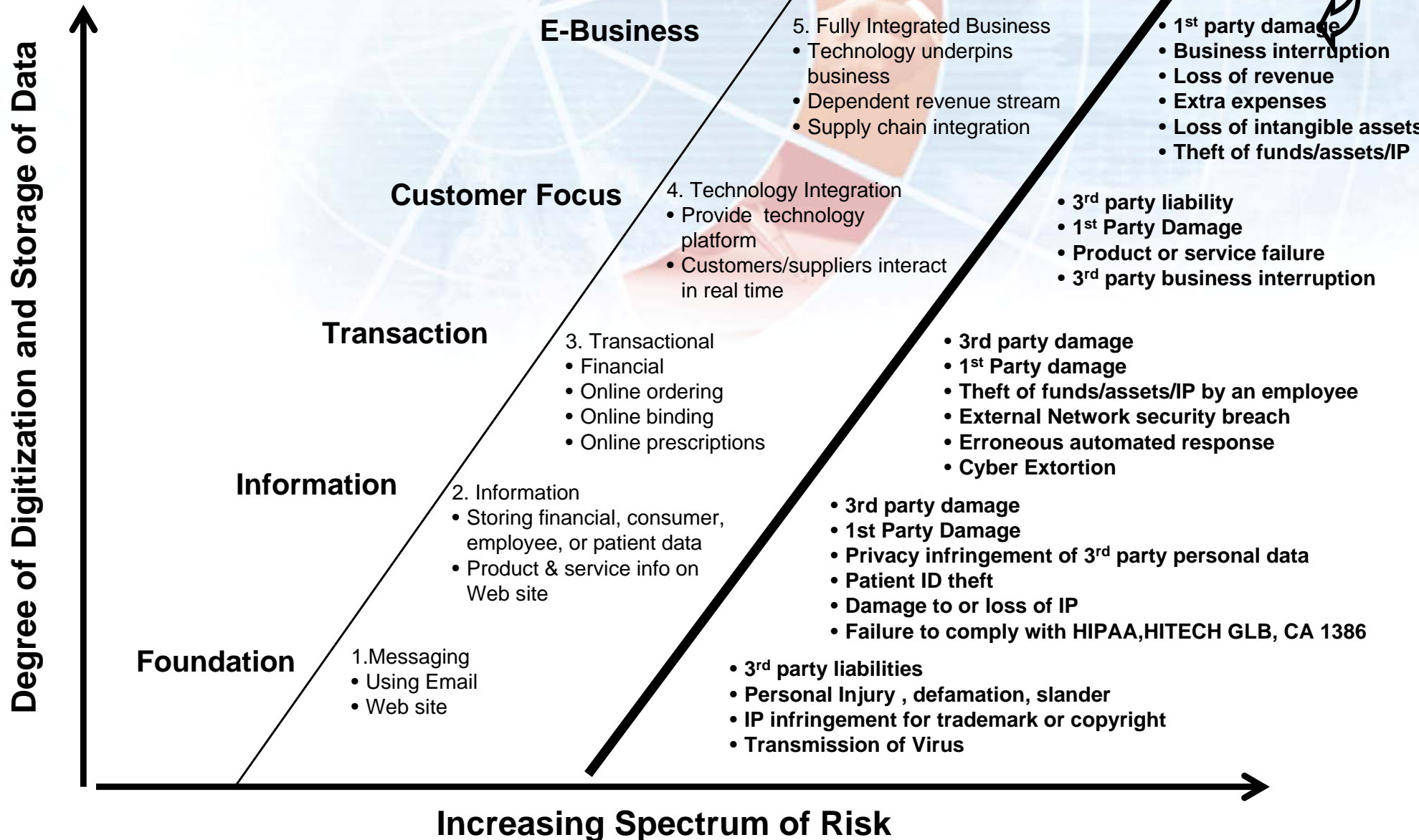


High-Tech & High-Touch Solutions  
for your Professional Liability Insurance needs.

# *New Insurance Solutions*

Companies are increasing their information risks at an alarming rate

High-Tech & High-Touch Solutions  
for your Professional Liability Insurance needs.



(privacy, 1<sup>st</sup> party, 3<sup>rd</sup> party viruses, loss of service, loss of data, defamation, IP, cyber extortion)

OPTION 2

<b>SUBSIDIARY COVERAGE:</b>				
None		Only those listed by Endorsement		X Blanket
<b>POLICY PERIOD:</b>	From: 08/06/2007	To: 08/06/2008	12:01 A.M. at the address in Item 1(a)	
<b>LIMITS OF LIABILITY</b>				
<b>POLICY AGGREGATE:</b> Aggregate for all coverages combined (including claim expenses):				\$10,000,000
COVERAGE MODULE (OR SECTIONS)	SUBLIMIT OF LIABILITY	RETENTION	RETROACTIVE DATE	FIRST INCEPTION DATE
TECH	\$10,000,000	\$100,000	08/06/1995	08/06/1995
TELECOM	Nil		Not Applicable	Not Applicable
INTERNET PRO	Nil		Not Applicable	Not Applicable
MPL	Nil		Not Applicable	Not Applicable
MEDIA	Nil		Not Applicable	Not Applicable
SEC LIAB	\$10,000,000	\$100,000	08/06/2007	08/06/2007
CCP	Nil	(a) Non-indemnifiable loss: (b) All other Loss:	Not Applicable	Not Applicable
INFO ASSET	Nil		Not Applicable	Not Applicable
BUS INT	Nil	The greater of: \$ _; or the business interruption loss during the _ hour waiting hours period	Not Applicable	Not Applicable
CYBER EXT	Nil		Not Applicable	Not Applicable
CM	Nil	Not Applicable	Not Applicable	Not Applicable
<b>PREMIUM (1 YEAR):</b>				\$113,465+ applicable NJ Surcharge

## *Coverages Available in the Marketplace*

- **Errors and Omissions:** loss caused by an act, error, or omission, committed by the insured technology professional while performing services for another
- **Breach of Representation:** Loss caused by the failure of the insured technology professional's product or service to perform as intended or represented
- **Security Failure:** Loss caused by failure, on the part of the insured technology professional, to prevent unauthorized access to or use of an electronic system.
- **Intellectual Property Infringement:** Loss caused by the infringement of a third party's copyright, trademark, or similar intellectual property and arising out of an insured technology professional's product or service.
- **Personal Injury:** Loss resulting from defamation, invasion of privacy or related peril and out of the insured technology professional's product or service.

## *Coverage Available*

- **Cyber:** Loss resulting from first and third party risks associated with e-business, the internet, networks including virus transmission.
- **Secure Data:** Loss resulting from the failure of corporations and business entities that have a legal and fiduciary responsibility to protect and provide secure a environment for that proprietary data by using a standard of care spelled out by certain generic and specific industry laws and benchmarks.
- **Identify Theft:** Loss occurring to individuals who might have credit cards, soc security numbers or other private information data or codes etc stolen or lost which will allow access to their private financial resources or funds.
- **Crisis Management:** Expert team of support specialists to advise and help with PR spin and other critical issues during initial phase.
- **Call Center Support:** Question and answer team needed to diffuse customer lack of confidence and general confusion towards the process.
- **Business Interruption:** loss of business revenues during crisis and shutdown of normal operations created by security breach.
- **\*Record coverage verses Sublimit:** coverage guaranteed for a certain amount of record notifications

**\* Newest entry in market**

## *Other ISO Exclusions*

- **Internet Service Providers and Internet Access Providers Errors & Omissions**  
CG 22 98 12 04
- **Professional Liability Exclusion – Computer Data Processing**  
CG 22 77 07 98
- **Professional Liability Exclusion – Computer Software**  
CG 22 75 07 98

## *ISO Financial Services Exclusion*

The following exclusion is added to Paragraph 2., **Exclusions of Section I – Coverage A – Bodily Injury And Property Damage Liability** and **Section I – Coverage B – Personal And Advertising Injury Liability**:

This insurance does not apply to "bodily injury", "property damage" or "personal and advertising injury" resulting from the rendering of or the failure to render financial services by any insured to others. For the purpose of this exclusion, financial services include but are not limited to:

1. Planning, administering or advising on:
  - a. Any:
    - (1) Investment;
    - (2) Pension;
    - (3) Annuity;
    - (4) Savings;
    - (5) Checking; or
    - (6) Individual retirement plan, fund or account;
  - b. The issuance or withdrawal of any bond, debenture, stock or other securities;
- c. The trading of securities, commodities or currencies; or
- d. Any acquisitions or mergers;
2. Acting as a dividend disbursing agent, exchange agent, redemption or subscription agent, warrant or scrip agent, fiscal or paying agent, tax withholding agent, escrow agent, clearing agent, or electronic funds transfer agent;
3. Lending, or arranging for the lending of, money, including credit card, debit card, leasing or mortgage operations or activities or interbank transfers;
4. Repossessing of real or personal property from a borrower or acting as an assignee for the benefit of creditors;
5. Checking or reporting of credit;
6. Maintaining of financial accounts or records:
7. Tax planning, tax advising or the preparation of tax returns; or
8. Selling or issuing credit, certified checks, money orders.

CG 21 52 07 98

## Key coverage Language

18. **Privacy regulations** mean the following statutes and regulations associated with the control and use of personally identifiable financial or medical information:

**Health Insurance Portability and Accountability Act of 1996** (public Law 104-191), known as HIPAA, including Title II that requires protection of confidentiality and security of electronic protected health information and the rules and regulations promulgated there under as they currently exist and as amended, and other similar privacy statutes, the Computer Fraud, Misuse and Abuse Act, the Digital Millennium Copyright Act, the Federal Wiretap Statute and other federal, state or local laws establishing legal liability for operation and use of the Internet and computer systems, including intranets and extranets, and anti-cyber squatting and domain name disputes;

## Key Coverage Language

**Gramm-Leach-Bliley Act of 1999 (G-L-B)**, known as Financial Services Modernization Act of 1999, including sections concerning security protection and standards for customer records maintained by financial services companies, and the rules and regulations promulgated there under as they currently exist and as amended:

State Attorneys General and Federal Trade Commission enforcement actions regarding the security and privacy of consumer information; and

**State privacy protection laws, such as the California Database Protection Act of 2003 (previously called SB 1386 currently revised 1798)**, as they now exist or in the future that require commercial Internet sites or on-line services that collect personally identifiable information to post privacy policies and adopt specific privacy controls.

Federal and state consumer credit reporting laws, such as the Federal Fair Credit Reporting Act (FCRA) and the California consumer Credit Reporting Agencies Act (CCCRAA).

## *Additional important language*

**We** will reimburse those reasonable and necessary expenses **you** incur with **our** prior written consent if **you** have suffered a security breach resulting in the unauthorized acquisition of computer data that compromises the security, confidentiality, or integrity of personal information maintained by **you**,

- (a) where such breach triggers **your** notification obligations under California Civil Code section 1798.82 or any other equivalent state or federal statute, including **your** costs of contacting issuing or acquiring banks for details such as the name and address of those whose personal information has been compromised, to comply with the notice requirements only under such statute, and
- (b) **your** notification obligations under VISA CISP, Operating Regulations or any other equivalent notification obligations under card issuer operation regulations, to comply with the notice requirements only under such rules, and
- for identity theft education and assistance, credit file monitoring services, or any other similar service.
- **Claims trigger language critical to coverage**

## *Key Coverage issues*

- Fines, penalties and costs: HIPAA, state data privacy, HITECH etc
- Sublimit for various components
- Limits= Number of records held times \$125 per record for minimum coverage limit
- Prior acts and retro
- Incident trigger
- First party
- Cyber extortion
- Crisis management
- Notification costs
- Lost of income from PR release
- Mental Distress and Anguish
- Normal coverage issues: 1<sup>st</sup> dollar, defense outside, Consent to settle etc
- Reissue costs for credit cards?

## *A note on 'Privacy'*

### **Privacy Practices are often based on Fair Information Principles**

*The Fair Information Principles, the basic components of a privacy program, are:*

- Provide consumers with **notice** regarding data collection
- Give consumers **choice** regarding use of their data
- Provide consumer **access** to review/comment on **quality**
- Ensure data accurate/ up-to-date; review and **correct** all data
- Set **collection** and **use limits** (purpose)
- Provide adequate **security** against improper use
- Be **accountable** for legal conformance

## *Closing thought...*

“Many company networks are compromised... without them even knowing it.”

