

TABLE OF CONTENTS

Tab 1 Attorney Tim Murphy's Presentation Outline

- I. Records Security / Identity Theft
- II. First Steps towards a Solution
- III. Property Managers/ Owners are now on the Front Line
- IV. What can you do / Defenses

Tab 2

Privacy Clearing House: How many Identity theft victims are there? What is the Impact on Victims

Tab 3

U. S. Department of Veterans affairs Article

Tab 4

IRS tapes missing in Kansas City
Georgia loses 2.9 million records
Ohio / stolen laptop 200,000 +/- records

Tab 5

UCLA break-in puts 800,000 records at risk

Tab 6

Boeing loses 380,000 records
Fidelity Information: Employee illegally sells 2.3 million records

Tab 7

TJ Maxx loses 45 million records
TJ Maxx sued by Banks

Tab 8

Health Insurance Portability and Accountability Act
U.S. Code collection

Tab 9

FACTA Disposal Rule Goes into Effect June 1

Tab 10

Statutes and Session Law M.R.S. 10 § 1346 Short Title
Statutes and Session Law M.R.S. 10 § 1347 Definitions

Tab 11

Group Pushes Congress for Data Protection; Cites More than 100 Million Compromised
Personal Records

Tab 12

Identity Theft Complaints by Victim Age - Chart

Tab 1

I. RECORDS SECURITY /IDENTY THEFT

A. SCOPE AND COST OF THE PROBLEM: Some experts have said Identity Theft is the fastest growing crime in the U.S. One report suggested there were 9 million victims just in 2005. A Presidential task force has been set up to address the problem.

1. Costs: 50 +/- Billion dollars in 2006
30+/- Million people affected since 1990
600 hours to correct per victim
\$740.00 +/- average cost per victim
2. See Tab 2: Summary of Findings by Privacy Clearing House

B. HOW ARE RECORDS LOST: The number of lost data incidents and total lost records involved is staggering. A tracking report of the Privacy Rights Clearing House runs 82 pages. It lists approximately 1,000 +/- major breaches with an estimated 100,000,000 records released.

1. Records are lost by Government, Private Businesses and by individuals. Some of it is stolen; some of it is lost through incompetence, accident, poor policies, mis-handling, and employee theft.
 - Tab 3: Federal Government / VA laptops (incompetence / poor policies) / no encryption
 - Tab 4: State and local Government / City of Kansas City loses Key IRS data (mis-handling); Georgia loses 2.9 million citizen records; Ohio (stolen laptop)
 - Tab 5: Schools and Universities. UCLA exposes 800,000 records (Crime / Hacking)
 - Tab 6: Private Industry including sophisticated entities such as Fidelity National Info. (2.3 million records); Boeing (380,000 records, stolen laptop / employee theft)

C. WHY SHOULD YOU CARE Recent incident involving TJ Maxx and its affiliate stores is a cautionary tale. Company had retained info on all credit card transactions. Data – 45 million records pilfered by hackers. Fraudulent credit card transactions based on that information are taking place. TJ Maxx delayed alerting customers and banks, and initially grossly underestimated number of cards stolen. Tremendous business harm.

- Tab 7: Customers upset. Will shop elsewhere
Their Banks upset. Can TJ Maxx secure credit
Blow to reputation. Now being sued by Banks.

Cost to correct / mitigate huge
Actions may have violated Federal & State Law. Fines /
Prosecution

II. FIRST STEPS TOWARDS A SOLUTION

The Federal Government has enacted a series of laws which address, in part, records security. State and local governments as well have begun their first steps to mitigate against records loss. And, even private industry is paying attention / seeking solutions.

A. FEDERAL EFFORTS: Federal Government has passed laws regulating health insurance, financial records of public companies, banking regulation and fair credit rules all of which dictate records security requirements.

- Tab 8: Health Insurance Portability and Accountability Act – HIPAA.
- Sarbanes – Oxley Act, also known as SOX, regulates records of all publicly traded corporation
- Tab 9: Gramm-Leach-Bliley. Affects all financial institutions, including banks and credit unions.
- Tab 10: Fair and Accurate Credit Transaction Act – “FACTA”. Covers all parties such as EquiFax, Trans Union, Experian, as well as all business who use credit report information banks, car dealerships, Tenant-Net, and may include property owners and managers. Includes a “Disposal Rule” as records retention and destruction.

B. STATE RESPONSES: State Governments, including Maine, enact similar laws as well. Maine now requires protection of the following confidential information: Social Security number, Drivers license number, Account numbers

- Tab 11: Notice of Risk to Personal Data Act 10 MRSA § 1346

Recently, the Act was expanded to reach beyond “information brokers” such as lenders, companies like Tenant-Net. It now reaches “any person” who holds / retains such confidential information. This may include property owners and managers.

C. PRIVATE INDUSTRY: Even private industry is pushing itself, and its own vendors / customers to “tighten up” on security. Example Trans Union reacts to changes like FACTA discussed above, and forces companies like Tenant-Net to undertake protective steps.

1. Trans Union requires we audit-inspect business users of Tenant-Net

2. Trans Union now requires we meet ISO 17799 Security Standards

- Security policy
- Physical security
- Access control
- Incident protocol

D. NEW EFFORTS: Even with all the various parties taking actions, new laws and standards enacted, records are still lost and/or at risk. There are renewed efforts to have Congress pass stricter, more comprehensive laws

- See Tab 12: Cyber Security Industry Alliance calls for National Standards

III. PROPERTY MANAGERS / OWNERS ARE NOW ON THE FRONT LINE

A. LAW CHANGES: Due to “FACTA” and Maine’s new law (10 MRSA 1346, et. seq.) owners and managers are now bound by records security obligations.

1. Maine specifically expanded its law to reach beyond “information brokers” to any “person” who holds and maintains confidential information such as SSN, Drivers license numbers, bank or other financial account information.

2. FACTA’s disposal rules reaches any party that uses consumer credit information

B. OWNERS AND MANAGERS HOLD CONFIDENTIAL INFORMATION: You retain tenant applications, credit reports and other records which contain confidential information. Both federal and state law place requirements for safe handling and/or destruction of those records.

1. You are at risk by law

2. At risk by action per our audits

C. DEMOGRAPHICS OF CRIME: According to the US Department of Justice, the vast majority of identity theft falls upon people ages 18-49 (74%). This is the demographic of the population of renters.

See Tab 13:

1. Your tenants are at risk.

IV. WHAT CAN YOU DO / DEFENSES

A. BE PROACTIVE: Property owners and managers can help themselves with some relatively simple steps, and some other more costly steps.

1. Shred: Shred documents with confidential information as soon as feasible.
2. Locking files: Purchase a lockable storage cabinet/ file for those records you need to maintain.
3. Limit data collection: Only collect data that you absolutely need.
4. Computer Security: If you retain confidential info on a computer, hire someone to encrypt that data, and definitely keep that computer from being linked to the Internet. Do not store confidential information on a laptop.
5. Consider Biometrics: Face scan and fingerprint scan systems are now very affordable, and will deter all but the most determined hacker. Those parties are generally not a threat to you.
6. Audits: Self audits are a first step, but consider hiring an outside firm. If you use Tenant-Net, we will audit you for free, as Trans Union requires it of us.
7. Iron Mountain: Consider using a records destruction firm such as Iron Mountain. Consider also keeping one on site for benefit of Tenants.

Tab 2

How Many Identity Theft Victims Are There? What IS the Impact on Victims?



Posted September 2003.
Updated February 2006.

Recent Surveys and Studies from the Better Business Bureau, Identity Theft Resource Center, Federal Trade Commission, Gartner, and Privacy & American Business

Search Our Site:
www.privacyrights.org/search.htm
Have a Question?
www.privacyrights.org/preinquiry.html
Web: www.privacyrights.org

[HOME](#)

How Many Identity Theft Victims Are There? What IS the Impact on Victims?

**Recent Surveys and Studies from the Better Business Bureau,
Identity Theft Resource Center, Federal Trade Commission,
Gartner, and Privacy & American Business**

Contents:

Javelin/Better Business Bureau Survey - January 2006
Javelin/Better Business Bureau Survey - January 2005
Federal Deposit Insurance Corporation - December 2004
Identity Theft Resource Center - September 2003
Federal Trade Commission Survey - September 2003
Gartner Survey - July 2003
Privacy & American Business Survey - July 2003

Javelin/Better Business Bureau Survey - January 2006 (no charge for Consumer Version)

In January 2006, Javelin Strategy and Research co-released its 2006 Identity Fraud Survey Report with the Better Business Bureau. The report is issued as a longitudinal update to the Javelin 2005 Identity Fraud Survey Report and the Federal Trade Commission's (FTC) 2003 Identity Theft Survey Report. The Consumer Version of the survey is available at no cost.

Survey findings Include:

- The number of US adult victims of identity fraud decreased from 10.1 million in 2003 and 9.3 million in 2005 to 8.9 million in 2006.
- Total one year fraud amount rose from \$53.2 billion in 2003 and \$54.4 billion in 2005 to \$56.6 billion in 2006.
- With the mean fraud amount per fraud victim rising from \$5,249 in 2003 and \$5,885 in 2005 to \$6,383 in 2006.
- The mean resolution time is at a high of 40 hours per victim in 2006 compared to 28 hours in 2005 and 33 hours in 2003.

Javelin/Better Business Bureau Survey - January 2005

On January 26, 2005, the Better Business Bureau in conjunction with Javelin Strategy and Research released its Identity Theft survey as an update to the Federal Trade Commission's 2003 Identity Theft Survey Report. The full

report is available online at <http://www.javelinstrategy.com/reports/2005IdentityFraudSurveyReport.html>.

Survey findings include:

- Within the last twelve months, 9.3 million Americans were victims of identity theft.
- The total U.S. annual identity fraud cost remains essentially unchanged since [the FTC's] 2003 [results], at \$52.6 Billion, an increase of 2.3% from the 2003 inflation-adjusted level of \$51.4 Billion.
- Most thieves still obtain personal information through traditional rather than electronic channels. In the cases where the method was known, 68.2% of information was obtained off-line versus only 11.6% obtained online.
- Conventional methods such as through lost or stolen wallets, misappropriation by family and friends, and theft of paper mail are among the most common ways thieves gain access to information.

Recommendations for consumers include:

- Cancel your paper bills and statements wherever possible and instead check your statements and pay bills online. Monitor your account balances and activity electronically (at least once per week).
- If you do not have access to online accounts, review paper bank and credit card statements monthly and monitor your billing cycles for missing bills or statements.
- Use emailbased account "alerts" to monitor transfers, payments, low balances and withdrawals and review your credit report (now available for free annual review).

Identity Theft Resource Center - September 2003

On September 23, 2003, the Identity Theft Resource Center (www.idtheftcenter.org) released its survey of the impact of identity theft on 173 known victims. To read the full survey, see: www.idtheftcenter.org/idaftermath.pdf

Survey findings include:

- Nearly 85% of all victims find out about their identity theft case in a negative manner. Only 15% of victims find out due to a proactive action taken by a business.
- The average time spent by victims is about 600 hours, an increase of more than 300% over previous studies.
- While victims are finding out about their cases earlier, it is taking far longer now than before to eliminate negative information from credit reports.
- A large majority of respondents indicates the opening of a credit card (73%) or takeover of a card account (27%) to be among crimes committed.
- The emotional impact of identity theft has been found to parallel that of victims of violent crime.
- The responsiveness toward victims by the various entities with which they must interact continues to be lacking in sensitivity in most cases and has not improved since studies released in 2000 (Nowhere to Turn).

Federal Deposit Insurance Corporation - December 2004

On December 14, 2004, the Federal Deposit Insurance Corporation (FDIC) released a study on phishing and account-takeover including information about fraudulent automated clearing house (ACH) payments. A complete copy of the FDIC's study is available online at: www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf.

Key findings include:

- While precise statistics on the prevalence of account hijacking are difficult to obtain, recent studies indicate that unauthorized access to checking accounts is the fastest growing form of identity theft.

- Another recent study has estimated that almost 2 million U.S. adult Internet users experienced this fraud during the 12 months ending April 2004. Of those, 70 percent do their banking or pay their bills online and over half believed they received a phishing e-mail.
- Consumers are attributing risk to their use of the Internet to conduct financial transactions, and many experts believe that electronic fraud, especially account hijacking, will have the effect of slowing the growth of online banking and commerce.
- Up to 5 percent of the recipients of spoofed e-mails respond to them.
- An estimated 19 percent of "those attacked" have clicked on the link in a phishing e-mail. Most, if not all, large financial institutions and electronic bill-paying services (such as PayPal) have been hit with phishing attacks.
- Because many phishing attacks originate overseas and because the average life span of a phishing Web site is 2.25 days, the sites are hard to shut down.

Federal Trade Commission Survey - September 2003

On September 3, 2003, the Federal Trade Commission (FTC) issued a survey on identity theft. The survey was conducted in March and April of 2003 with a random sample of over 4,000 households. To read the survey, go to <http://www.ftc.gov/os/2003/09/synovatereport.pdf>

Key findings include:

How Many Consumers Are Victims of Identity Theft?

- 27.3 million Americans have been victims of identity theft in the last five years, including 9.91 million people or 4.6% of the population in the last year alone.
- In the past 12 months, 3.23 million consumers or 1.5% of the population discovered that new accounts had been opened, and other frauds such as renting an apartment or home, obtaining medical care or employment, had been committed in their name. 6.6 million experienced their existing accounts compromised by an identity theft. A total of almost 10 million individuals were victims of identity theft.
- 52% of all ID theft victims, approximately 5 million people in the last year, discovered that they were victims of identity theft by monitoring their accounts.

Misuse of Personal Information

- On average, 49% of victims did not know how their information was obtained.
- Another 26% - approximately 2.5 million people - reported that they were alerted to suspicious account activity by companies such as credit card issuers or banks.
- 8% reported that they first learned when they applied for credit and were turned down.
- 15% of all victims - almost 1.5 million people in the last year - reported that their personal information was misused in nonfinancial ways, to obtain government documents, for example, or on tax forms.
- 67% of identity theft victims - more than 6.5 million victims in the last year - report that existing credit card accounts were misused.
- 19% reported that checking or savings accounts were misused.
- Nearly one-quarter of all victims - roughly 2.5 million people in the last year - said their information was lost or stolen, including lost or stolen credit cards, checkbooks or social security cards.
- Stolen mail was the source of information for identity thieves in 4 percent of all victims - 400,000 in the last year.

Costs to Businesses and Consumers

- Last year's identity theft losses to businesses and financial institutions totaled \$47.6 billion and consumer victims reported \$5 billion in out-of-pocket expenses.
- In those cases, the loss to businesses and financial institutions was \$10,200 per victim totaling \$32.9 billion.

Individual victims lost an average of \$1,180 for a total of \$3.8 billion.

- Where the thieves solely used a victim's established accounts, the loss to businesses was \$2,100 per victim totaling \$14.0 billion. For all forms of identity theft, the loss to business was \$4,800 and the loss to consumers was \$500, on average.

Gartner Survey - July 2003

On July 21, 2003, Gartner (www.gartner.com) released the results of a survey of 2,445 households regarding identity theft. To read the press release, go to:

http://www3.gartner.com/5_about/press_releases/pr21july2003a.jsp

The survey found the following:

- Identity theft is up nearly 80 percent from last year.
- 7 million U.S. adults or 3.4 percent of U.S. consumers were identity theft victims in the past 12 months.
- Because this crime is often misclassified, the thieves have just a one in 700 chance of being caught by the federal authorities.

Privacy & American Business Survey - July 2003

A July 30, 2003, *Privacy & American Business* survey found the following. To read the press release, go to http://www.pandab.org/id_theftpr.html.

How Many Consumers Are Victims of Identity Theft?

- 33.4 million Americans were victims of identity theft since 1990.
- Over 13 million Americans have become victims of identity theft since January 2001.
- Consumer out-of-pocket expenses have totaled \$1.5 billion annually since January 2001.
- 34% say someone obtained their credit card information, forged a credit card in their name, and used it to make purchases.
- 12% say someone stole or obtained improperly a paper or computer record with their personal information on it and used that to forge their identity.
- 11% say someone stole their wallet or purse and used their identity.
- 10% say someone opened charge accounts in stores in their name and made purchases as them.
- 7% say someone opened a bank account in their name or forged checks and obtained money from their account.
- 7% say someone got to their mail or mailbox and used information there to steal their identity.
- 5% say they lost their wallet or purse and someone used their identity.
- 4% say someone went to a public record and used information there to steal their identity.
- 3% say someone created false IDs and posed as them to get government benefits or payments.
- 16% say it was a friend, relative or co-worker who stole their identity.
- The seven million victims the survey identified in 2002 represent an 81% rise over victims in 2001.
- Identity theft incidents reported so far in 2003 suggest a major rise over 2002. The victims level and upward trend parallel findings of a Gartner survey released last week.

What Are Victims' Out of Pocket Expenses?

- While 62% of victims did not incur any out-of-pocket expenses, 38% did, representing 13-14 million Americans.
- Since January 2001, these 38% have paid approximately \$3.8 billion, or an average of \$1.5 billion per year. Based on actual amounts volunteered by respondents themselves, the average cost per victim for this time period is \$740.
- An earlier June 2002 survey on ID theft by *P&AB* and Harris found that a majority of Americans, 91%, do

Tab 3

Tab 4

News

VA Loses Data on 26 Million Veterans

Employee Claims Laptop With Sensitive Data Was Stolen

**By Martin H. Bosworth
ConsumerAffairs.Com**

May 22, 2006

In the latest laptop data theft, the Veterans Administration says that 26.5 million veterans' personal information is at risk because of a burglary at an employee's home.

According to the VA, the employee, a data analyst residing in suburban Maryland, saved the information on disk "in violation of policy," and took the data home with him to use on his laptop. The employee's home was burglarized, and the laptop was stolen.

The unidentified analyst was placed on leave "pending review," according to Veterans' Affairs Secretary Jim Nicholson, who said the employee's home had been burglarized on previous occasions..

The VA has launched an investigation in conjunction with the FBI and local law enforcement agencies, Nicholson said.

According to the **notice**(<http://www1.va.gov/opa/FAQ.pdf>) the VA prepared for those affected by the data breach, "no electronic medical records were compromised" in the theft. However, the data did include names, addresses, Social Security Numbers, and some information relating to individuals' disabilities.


The VA was notifying individual beneficiaries and Congressmen of the theft, according to the press statement, and was in the process of setting up a toll-free hotline and **Web site** (<http://www.firstgov.gov/veteransinfo.shtml>) to address questions about the theft.

Coincidence or Not?

It's worth noting that virtually all of the public cases of laptop theft seem to follow the same pattern -- an employee takes home unsecured data and ends up losing the laptop.

In the last seven months, there has been an explosion of reported cases of laptop thefts and losses, all of which contained valuable personal data that put millions of people at risk. **Notable cases** (http://www.consumeraffairs.com/news04/2006/03/laptop_thefts.html) included Hewlett-Packard, the Ford Motor Company, Ameriprise,



[Back to article](#)  [Print this](#)

Update: Veterans Affairs laptop recovered

FBI says the personal data on the hardware was not accessed by thieves

By Grant Gross, IDG News Service

June 29, 2006

Authorities have recovered a laptop and hard drive containing personal information on 26.5 million U.S. military veterans and their spouses, and determined that the data was not accessed, the U.S. Department of Veterans Affairs (VA) announced Thursday.

The U.S. Federal Bureau of Investigation told the VA Thursday morning that the personal data on the hardware was not accessed by thieves, VA Secretary R. James Nicholson told the House of Representatives Veterans Affairs Committee. The FBI conducted forensic testing on the two devices, he said.

The laptop and hard drive were stolen from a VA analyst's home in early May.

"This is a reason to be optimistic," Nicholson said earlier. "It's a very positive note in this entire tragic event."

The stolen hardware contained unencrypted data with names, Social Security numbers, dates of birth and some limited health information on military veterans.

As Nicholson announced the recovery, Representative Bob Filner interrupted him. "Mr. Secretary, does this leave you off the hook?" he said.

The VA continues to have major data security problems, Filner, a California Democrat, said during the hearing. While Nicholson has called the analyst who took the data home "grossly negligent," VA officials who failed to notify Nicholson of the breach for nearly two weeks haven't been held responsible, Filner said.

The committee has learned that the analyst had permission to take the hardware and data home, contradicting earlier statements from Nicholson, Filner added.

The recovery "doesn't change the fact that your intentions seem to be to blame all of this on one guy," Filner said. "He informed the cops in 52 minutes. Your guys didn't inform you for several days. Who was grossly negligent?"

Committee Chairman Steve Buyer, an Indiana Republican, reiterated concerns that the VA has been repeatedly warned of lax security practices going back to 1997. The VA's decentralized structure, with three divisions largely controlling their own IT systems, makes it "practically impossible" to secure the VA's systems, Buyer said.

Security experts have told the committee fast action and timely communication to victims are needed to recover from data breaches, Buyer said. "The word 'quick' does not seem to characterize anything about the VA's response to this threat over the years," he added.

Nicholson told the committee the data theft was a wake-up call for the agency. "This has brought to the light of day some real deficiencies in our department," he said.

Since the data theft, the agency has drafted a policy requiring encryption of sensitive data, and the agency is looking at contracts with data breach analysis firms that can track whether data has been compromised, Nicholson said. The agency is also looking into its policy on security clearances, and it began a reorganization of its IT structure late last year, he said.

Tab 5



UCLA break-in puts data on 800,000 at risk

By Dawn Kawamoto

http://news.com.com/UCLA+break-in+puts+data+on+800%2C000+at+risk/2100-1029_3-6143003.html

Story last modified Tue Dec 12 10:32:57 PST 2006

In one of the largest known security breaches at a university, the database at the University of California, Los Angeles has been broken into, exposing the private information of about 800,000 people.

Administrators discovered November 21 that the database had been compromised, according to a letter dated Tuesday that was posted to the university's Web site (PDF here). The hacker had exploited a previously undetected software flaw and gained access to the database from October 2005 until the discovery. Norman Abrams, acting UCLA chancellor, said in the letter.

"While we are uncertain whether your personal information was actually obtained, we know that the hacker sought and retrieved some social security numbers," Abrams said.

The breach affects UCLA students, staff, applicants and some students' parents. It also included information on current and some former faculty and staff at the University of California, Merced, and at the University of California Office of the President.

Sensitive information stored in the database included social security numbers, home addresses, dates of birth and contact information. Financial information, such as credit card numbers or bank accounts, were not housed in the database.

When the illicit activity was discovered, university staff immediately blocked access to social security numbers housed in the database and began an investigation, UCLA said. The database normally operates under restricted access and requires a password from authorized users, it said. In addition, the institution said it began notifying all those affected as well as the FBI, which has launched its own investigation.

UCLA's security breach is among the largest to hit a university. Last month, for example, Western Illinois University suffered a hacker attack that compromised the personal information of 180,000 people, and Ohio University earlier this year found three of its servers, one of which contained 137,000 social security numbers, had been compromised.

Last year, the University of Southern California suffered a security breach of a database containing personal information on 275,000 applicants over a eight-year period.

For a number of universities and colleges, balancing security with the free flow of information particular to



IRS tapes missing in Kansas City

01 / 22 / 07 |

Twenty-six computer tapes containing Internal Revenue Service taxpayer data have gone missing from City Hall in Kansas City, Mo.

The tapes were originally shipped to the City Hall building in August as part of an information-sharing agreement between the IRS and the municipality of Kansas City, according to *The Kansas City Star*.

Officials lost track of the tapes in December. On Friday, the local newspaper revealed that the city was working with the Department of the Treasury, of which the IRS is a division, in an attempt to locate the missing tapes' whereabouts. No updates have been provided.

Officials from City Hall could not be reached for further comment.

"There really isn't any excuse at this point other than poor management," said Avivah Litan, an analyst at research firm Gartner, who suggested that internal threats should not be ruled out in the investigation. "If you want to look at some of the biggest culprits, you don't have to look very far past the federal government," she commented, adding that it's nevertheless unlikely that this will turn into a major case of data theft. "In reality, the chances of anything bad happening are probably less than 1 percent."

IRS spokesman Michael Devine declined to comment on the matter, which he said was an "ongoing investigation."

But according to Litan, situations like the missing IRS tapes may have to be tackled differently in the future, because they've become increasingly common and high profile. "It's become practically impossible to control all the sensitive information out there on us, so a more effective solution would be making the information useless to thieves if it's stolen."

According to *The Kansas City Star* report, there was indeed some form of protection on the tapes that required special equipment to unlock them, but the data could still potentially be stolen and misused.

"After the (Department of Veterans' Affairs) lost laptops, even though the chances of identity theft taking place with these stolen devices is very small, you would think

Tab 6

ChoicePoint data theft widens to 145,000 people

By Matt Hines

http://news.com.com/ChoicePoint+data+theft+widens+to+145%2C000+people/2100-1029_3-5582144.html

Story last modified Fri Feb 18 12:53:12 PST 2005

ChoicePoint has confirmed that scammers culled the personal information of tens of thousands of Americans in a recent attack on its consumer database, resulting in 750 individual cases of identity theft.

The Atlanta-based company said that it plans to inform approximately 110,000 consumers outside the state of California whose information may have been accessed in the criminal scheme, originally reported on Tuesday. The company has already told some 35,000 Californians that their personal data, including their names, addresses, Social Security numbers and credit reports, was stolen by scammers. California is the only U.S. state with legislation in place that requires companies to notify its residents when their personal data has been compromised.

ChoicePoint also said that law enforcement officials informed the company of 750 cases of identity theft tied directly to the incident. One California man has already pleaded no contest to felony charges related to the ChoicePoint attack, while federal and state law enforcement agencies continue to look for others involved in the operation.

The perpetrators were able to dupe the company, which provides consumer data services to insurance companies, other businesses and government agencies, by passing themselves off as legitimate customers. Chuck Jones, a company spokesman, said the criminals set up 50 fraudulent accounts with ChoicePoint by posing as businesses including collection agencies that were looking to run background checks on potential customers.

Jones said that ChoicePoint was misled via a detailed effort, as the criminals used previously stolen identities to set up what appeared to be legitimate business licenses, phone numbers and addresses for the organizations they claimed to be when applying for accounts with the company. He said the firm has changed its policies for qualifying new accounts, and will now go as far as having people who are looking to access the company's databases visit the physical location of firms in order to verify those persons' legitimacy.

"We're working hard to deploy new technologies and tighten up the policies and procedures that ChoicePoint already had in place," Jones said. "It's always been critical for us to verify that people are who they say they are, but we think that our verification process has already been improved significantly (since the attack)."

The spokesman said that ChoicePoint has been targeted by criminals seeking to steal consumer data in the past, but never on such a wide scale. He said the company does not expect to report any additional consumers affected by the scheme.

The company said that it first learned of the security problem last fall, but ChoicePoint claims that law enforcement officials would not allow it to disclose the incident until now, so as not to compromise their investigations. Jones said the company is working on the case with the Los Angeles County Sheriff's office, U.S. Postal inspectors and the FBI.

Some privacy experts have predicted that the debacle will shine new light on the risks posed to consumers by information brokers such as ChoicePoint, and said the incident may convince other states to adopt legislation similar to the guidelines required by California. Last month, Sen. Dianne Feinstein, a Democrat from California, proposed legislation for a federal law that would require companies to inform consumers in any U.S. state of personal data losses.

Jones said ChoicePoint might support such legislation and will continue to work to help improve consumer protection across the data services industry.

"ChoicePoint has always been a proponent of responsible use of consumer data," he said, "and we remain hopeful that there will be a national discussion for improving policies that involves legislators, privacy experts and industry, to help establish better ground rules for this issue moving forward."

However, at least one privacy expert called ChoicePoint's claim of dedicated protection "comical." Ray Everett-Church, an attorney who runs his own consulting company, PrivacyClue, said data brokers such as ChoicePoint are far more concerned with making a profit than actively guarding against fraud.

"They're taking (consumer data) in the front door with the promise of protection and shoving it out the back door as fast as they can to the highest bidders--it's just a matter of time before we see more of these scenarios," Everett-Church said. "I've always marveled at these companies' ability to say they care about consumer privacy with a straight face."

He said ChoicePoint and other data aggregation companies have been doing very little in the way of completing background checks on customers, and said the firm probably could have identified the criminal enterprise as fraudulent by researching information in its own databases more closely.

"Don't tell me that your first priority is protecting consumers, when clearly the first priority is maximizing value for your shareholders," said Everett-Church. "I'm not buying it."

Copyright ©1995-2007 CNET Networks, Inc. All rights reserved.

Tab 7

SEATTLE POST-INTELLIGENCER

http://seattlepi.nwsourc.com/opinion/295794_ided.html

Data Security: Laptop secrets

Thursday, December 14, 2006

SEATTLE POST-INTELLIGENCER EDITORIAL BOARD

The Boeing Co. has joined the rapidly growing club of major businesses and institutions that have experienced thefts of computer data on employees, customers, students and others. Corporate practices and rules need to be improved quickly.

Voluntary action is critical. Otherwise, Congress likely will prescribe the fixes, which will be written with an eye to headlines.

Boeing said a laptop computer stolen from an employee's car earlier this month contained files for more than 380,000 past and present employees. The files reportedly contained Social Security numbers and, in most cases, home addresses, phone numbers and dates of birth.

The questions about how well institutions maintain identity security are rising. Locally, Starbucks reported in November that laptops with employee information were missing. Compass Health issued a security advisory after the theft of a laptop in June.

As with Boeing, Starbucks and Compass Health noted that no one seemed to be misusing the information when they made their announcements. But the loss of laptops with personnel information creates all sorts of potential problems. Institutions would protect themselves and others if they keep personnel information off laptops and in secure computers. Whatever difficulties may entail, the problems will be much worse if Congress issues one-size-fits-all orders.

On the Net: Tips from Attorney General Rob McKenna at atg.wa.gov.

© 1998-2007 *Seattle Post-Intelligencer*

Tab 8



Home > Business Today > Business > RSS Feed

E-mail Graphic Popular del.icio.us

Crooks' TJX plan: Charge! Banks see fraud with stolen info

By Jay Fitzgerald and Donna Goodison

Thursday, January 25, 2007 - Updated: 04:17 AM EST

TJX Co.'s customer data disaster turned into a nightmare yesterday as banks reported fraudulent purchases made with compromised data from credit and debit cards.

The Massachusetts Bankers Association put out an emergency alert that local customer data stolen from TJX stores is now being fraudulently used in Hong Kong, Sweden, Florida, Georgia and Louisiana.

The banking group, which has been harshly critical of TJX's handling of the cyber-breach of its computer system, said banks have linked recent fraud usage of card information with card-carriers who have previously shopped at TJX stores.

"This has the potential to be huge," said bankers association spokesman Bruce Spitzer, of the financial damage from the TJX cyber caper.

Meanwhile, the massive theft of possibly millions of consumers' credit- and debit-card numbers is prompting banks from Framingham to West Point, Va., and beyond to reissue cards in an attempt to protect customers' accounts.

Middlesex Savings Bank has begun reissuing about 10,000 cards as a "precaution," though there are no known cases of fraud committed against customers' accounts stemming from the TJX incident, said a spokesman.

Larry Dillon, president of Citizens and Farmers Bank in Virginia, said his bank is also being "proactive" by issuing new cards to customers. "We had to make a quick decision," said Dillon of his bank's reaction to news late last week that TJX's computers had been hacked into by data thieves.

One Virginia customer who's bank account was frozen as a precaution told the Herald yesterday that she's so furious with TJX for not alerting customers earlier that she plans to picket stores in her Richmond, Va., area.

"I'm not going to be quiet about this," said Loretta Donaldson, a licensed contractor in Newkent, Va., and a Citizens and Farmers Bank customer. "They (TJX officials) left us in jeopardy."

A spokesman for TJX - which has said it waited a month to alert the public about its computer breach because of law enforcement reasons - could not be reached for comment.

TJX's handling of the entire affair has mystified bankers, customers and public-relations experts.

"It's really a case study in what not to do, in thinking about the steps you need to do to protect your customers as well as all the other constituencies that are impacted by it," said Ann Murphy, vice president of Boston's O'Neill and Associates, a public relations firm.

With multiple newspaper stories about the TJX security breach running day after day, Murphy is sure the publicity will affect customers' behavior, at least in the short term.

"It's a very serious situation with no end in sight, and that's the tough part for TJX," she said.

The Massachusetts bankers group urged customers to closely monitor their accounts, via bank statements or ATM receipts, for suspicious activities. Banks will also alert customers if they have information that their accounts may be vulnerable to thieves.

Today's Top Articles

Viewed Emailed Rated

Updated 12:52 PM

N.E. Patriots

Taking stock of the Pats

More Inside Track

Bridget's A-list dreams may come

More Inside Track

Want a recipe for disaster? Slam Oprah

Boston Red Sox

Sox make Cash call for backup

N.E. Patriots

Rodney bent on a return: Agent says Harrison determined

[View the Herald Top Ten](#)

E-mail Graphic Popular del.icio.us

Tab 9

Health Insurance Portability and Accountability Act

From Wikipedia, the free encyclopedia
(Redirected from HIPAA)

The **Health Insurance Portability and Accountability Act (HIPAA)** was enacted by the U.S. Congress in 1996.

According to the Centers for Medicare and Medicaid Services' (CMS) website, Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs.

Title II of HIPAA, the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers.

The AS provisions also address the security and privacy of health data. The standards are meant to improve the efficiency and effectiveness of the nation's health care system by encouraging the widespread use of electronic data interchange in the US health care system.

Contents

- 1 Title I: Health Care Access, Portability, and Renewability
- 2 Title II: Preventing Health Care Fraud and Abuse; Administrative Simplification; Medical Liability Reform
 - 2.1 The Privacy Rule
 - 2.2 The Transactions and Code Sets Rule
 - 2.3 The Security Rule
 - 2.4 The Enforcement Rule
 - 2.5 The National Provider Identifier
- 3 Effect on research and clinical care
 - 3.1 Effects on research
 - 3.2 Effects on clinical care
 - 3.3 Costs of implementation
- 4 Legislative information
- 5 See also
- 6 References
- 7 External links

Title I: Health Care Access, Portability, and Renewability

Title I of HIPAA regulates the availability and breadth of group and individual health insurance plans. It amends both the Employee Retirement Income Security Act and the Public Health Service Act.

Title I prohibits any group health plan from creating eligibility rules or assessing premiums for individuals in the plan based on health status, medical history, genetic information, or disability.^[1] This does not apply to private individual insurance.

Title I also limits restrictions that a group health plan can place on benefits for preexisting conditions. Group health plans may refuse to provide benefits relating to preexisting conditions for a period of 12 months after enrollment in the plan or 18 months in the case of late enrollment.^[2] However, individuals may reduce this exclusion period if they had health insurance prior to enrolling in the plan. Title I allows individuals to reduce the exclusion period by the amount of

The Privacy Rule gives individuals the right to request that a covered entity correct any inaccurate PHI.^[18] It also requires covered entities to take reasonable steps to ensure the confidentiality of communications with individuals.^[19] For instance, an individual can ask to be called at his or her work number, instead of home or cell phone number.

The Privacy Rule requires covered entities to notify individuals of uses of their PHI. Covered entities must also keep track of disclosures of PHI and document privacy policies and procedures.^[20] They must appoint a Privacy Official and a contact person^[21] responsible for receiving complaints and train all members of their workforce in procedures regarding PHI.^[22]

An individual who believes that the Privacy Rule is not being upheld can file a complaint with the Department of Health and Human Services Office for Civil Rights (OCR).^{[23][24]}

The Transactions and Code Sets Rule

The HIPAA/EDI provision was scheduled to take effect October 16, 2003 with a one-year extension for certain "small plans"; however, due to widespread confusion and difficulty in implementing the rule, CMS granted a one-year extension to all parties. As of October 16, 2004, full implementation was not achieved and CMS began an open-ended "contingency period." Penalties for non-compliance were not levied; however, all parties are expected to make a "good-faith effort" to come into compliance.

CMS announced that the Medicare contingency period ended July 1, 2005. After July 1, most medical providers that file electronically will have to file their electronic claims using the HIPAA standards in order to be paid. There are exceptions for doctors that meet certain criteria.

Key EDI transactions are:

- **837**: Medical claims with subtypes for Professional, Institutional, and Dental varieties.
- **820**: Payroll Deducted and Other Group Premium Payment for Insurance Products
- **834**: Benefits enrollment and maintenance
- **835**: Electronic remittances
- **270/271**: Eligibility inquiry and response
- **276/277**: Claim status inquiry and response
- **278**: Health Services Review request and reply

These standards are X12 compliant, and are grouped under the label X12N.

Implementation Guides are available from the Washington Publishing Company (<http://www.wpc-edi.com/>) for a fee, now that CMS is not subsidizing the publications.

The National Council for Prescription Drug Programs' Telecommunication Standard version 5.1 is also used for the transmission of third-party pharmacy claims. The NCPDP Telecommunication Standard version 5.1 is available to NCPDP members at NCPDP's website (<http://www.ncdp.org/>).

The Security Rule

The Final Rule on Security Standards was issued on February 20, 2003. It took effect on April 21, 2003 with a compliance date of April 21, 2005 for most covered entities and April 21, 2006 for "small plans". The Security Rule complements the Privacy Rule. It lays out three types of security safeguards required for compliance: administrative,

physical, and technical. For each of these types, the Rule identifies various security standards, and for each standard, it names both required and addressable implementation specifications. Required specifications must be adopted and administered as dictated by the Rule. Addressable specifications are more flexible. Individual covered entities can evaluate their own situation and determine the best way to implement addressable specifications. The standards and specifications are as follows:

- **Administrative Safeguards** - policies and procedures designed to clearly show how the entity will comply with the act
 - Covered entities (entities that must comply with HIPAA requirements) must adopt a written set of privacy procedures and designate a privacy officer to be responsible for developing and implementing all required policies and procedures.
 - The policies and procedures must reference management oversight and organizational buy-in to compliance with the documented security controls.
 - Procedures should clearly identify employees or classes of employees who will have access to protected health information (PHI). Access to PHI in all forms must be restricted to only those employees who have a need for it to complete their job function.
 - The procedures must address access authorization, establishment, modification, and termination.
 - Entities must show that an appropriate ongoing training program regarding the handling PHI is provided to employees performing health plan administrative functions.
 - Covered entities that out-source some of their business processes to a third party must ensure that their vendors also have a framework in place to comply with HIPAA requirements. Companies typically gain this assurance through clauses in the contracts stating that the vendor will meet the same data protection requirements that apply to the covered entity. Care must be taken to determine if the vendor further out-sources any data handling functions to other vendors and monitor whether appropriate contracts and controls are in place.
 - A contingency plan should be in place for responding to emergencies. Covered entities are responsible for backing up their data and having disaster recovery procedures in place. The plan should document data priority and failure analysis, testing activities, and change control procedures.
 - Internal audits play a key role in HIPAA compliance by reviewing operations with the goal of identifying potential security violations. Policies and procedures should specifically document the scope, frequency, and procedures of audits. Audits should be both routine and event-based.
 - Procedures should document instructions for addressing and responding to security breaches that are identified either during the audit or the normal course of operations.
- **Physical Safeguards** - controlling physical access to protect against inappropriate access to protected data
 - Controls must govern the introduction and removal of hardware and software from the network. (When equipment is retired it must be disposed of properly to ensure that PHI is not compromised.)
 - Access to equipment containing health information should be carefully controlled and monitored.
 - Access to hardware and software must be limited to properly authorized individuals.
 - Required access controls consist of facility security plans, maintenance records, and visitor sign-in and escorts.
 - Policies are required to address proper workstation use. Workstations should be removed from high traffic areas and monitor screens should not be in direct view of the public.
 - If the covered entities utilize contractors or agents, they too must be fully trained on their physical access responsibilities.
- **Technical Safeguards** - controlling access to computer systems and enabling covered entities to protect communications containing PHI transmitted electronically over open networks from being intercepted by anyone other than the intended recipient
 - Information systems housing PHI must be protected from intrusion. When information flows over open



LII / Legal Information Institute

U.S. Code collection

TITLE 15 > CHAPTER 94 > SUBCHAPTER I > § 6801[Prev](#) | [Next](#)**§ 6801. Protection of nonpublic personal information***How Current is This?***(a) Privacy obligation policy**

It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information.

(b) Financial institutions safeguards

In furtherance of the policy in subsection (a) of this section, each agency or authority described in section 6805 (a) of this title shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards—

- (1) to insure the security and confidentiality of customer records and information;
- (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and
- (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

[Search
this title:](#)[Notes](#)
[Updates](#)
[Parallel
authorities
\(CFR\)](#)
[Your
comments](#)[Prev](#) | [Next](#)

LII has no control over and does not endorse any external Internet site that contains links to or references LII.

Tab 10



Search:



HOME | CONSUMERS | BUSINESSES | NEWSROOM | FORMAL | ANTITRUST | CONGRESSIONAL | ECONOMIC | LEGAL
 Privacy Policy | About FTC | Commissioners | File a Complaint | HSR | FOIA | IG Office | En Español

For Release: June 1, 2005

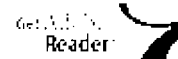
Related Documents:

FACTA Disposal Rule Goes into Effect June 1

Business Information:

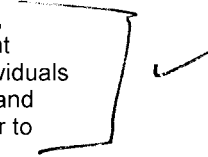
Beginning today, a new federal rule will require businesses and individuals to take appropriate measures to dispose of sensitive information derived from consumer reports. Any business or individual who uses a consumer report for a business purpose is subject to the requirements of the Disposal Rule, a part of the Fair and Accurate Credit Transactions Act of 2003 (FACTA), which calls for the proper disposal of information in consumer reports and records to protect against "unauthorized access to or use of the information."

- Disposing of Consumer Report Information? New Rule Tells How



The standard for the proper disposal of information derived from a consumer report is flexible, and allows the organizations and individuals covered by the Rule to determine what measures are reasonable based on the sensitivity of the information, the costs and benefits of different disposal methods, and changes in technology. Although the Disposal Rule applies to consumer reports and the information derived from consumer reports, the FTC encourages those who dispose of any records containing a consumer's personal or financial information to take similar protective measures.

The Rule applies to people and both large and small organizations that use consumer reports, including: consumer reporting companies; lenders; insurers; employers; landlords; government agencies; mortgage brokers, car dealers; attorneys; private investigators; debt collectors; individuals who pull consumer reports on prospective home employees, such as nannies or contractors; and entities that maintain information in consumer reports as part of their role as a service provider to other organizations covered by the Rule.



The Disposal Rule applies to consumer reports or information derived from consumer reports. The Fair Credit Reporting Act defines the term consumer report to include information obtained from a consumer reporting company that is used – or expected to be used – in establishing a consumer's eligibility for credit, employment, or insurance, among other purposes. Examples of consumer reports include credit reports, credit scores, reports businesses or individuals receive with information relating to employment background, check writing history, insurance claims, residential or tenant history, or medical history.

The Rule requires disposal practices that are reasonable and appropriate to prevent the unauthorized access to – or use of – information in a consumer report. For example, reasonable measures for disposing of consumer report information could include establishing and complying with policies to: burn, pulverize, or shred papers containing consumer report information so that the information cannot be read or reconstructed; destroy or erase electronic files or media containing consumer report information so that the information cannot be read or reconstructed; or conduct due diligence and hire a document destruction contractor to dispose of material specifically identified as consumer report information consistent with the Rule. Due diligence could include: reviewing an independent audit of a disposal company's operations and/or its compliance with the Rule; obtaining information about the disposal company from several references; requiring that the disposal company be certified by a recognized trade association; or reviewing and evaluating the disposal company's information security policies or procedures.

Financial institutions that are subject to both the Disposal Rule and the Gramm-Leach-Bliley (GLB) Safeguards Rule, which requires institutions to take steps to protect sensitive customer information, should incorporate practices dealing with the proper disposal of consumer information into the information security program that the Safeguards Rule requires. Information is available at www.ftc.gov/privacy/privacyinitiatives/safeguards.html.

FACTA directed the FTC, the Federal Reserve Board, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision, the National Credit Union Administration, and the Securities and Exchange Commission to adopt comparable and consistent rules regarding the disposal of sensitive consumer report information. The FTC's

Disposal Rule became effective June 1, 2005. It was published in the Federal Register on November 24, 2004 [69 Fed Reg 68690], and is available at www.ftc.gov/os/2004/11/041118disposalfrn.pdf.

The FTC has issued a new publication, "**New Rule Seeks to Protect Privacy by Requiring Proper Disposal of Sensitive Consumer Information**," available at www.ftc.gov/bcp/conline/pubs/alerts/disposalalrt.htm, to educate businesses about the new requirements.

The FTC works for the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them. To file a complaint in English or Spanish (bilingual counselors are available to take complaints), or to get free information on any of 150 consumer topics, call toll-free, 1-877-FTC-HELP (1-877-382-4357), or use the complaint form at <http://www.ftc.gov>. The FTC enters Internet, telemarketing, identity theft, and other fraud-related complaints into Consumer Sentinel, a secure, online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

MEDIA CONTACT:

Jen Schwartzman
Office of Public Affairs
202-326-2674

STAFF CONTACT:

Katherine Armstrong
Bureau of Consumer Protection
202-326-3250

(<http://www.ftc.gov/opa/2005/06/disposal.htm>)

HOME | CONSUMERS | BUSINESSES | NEWSROOM | FORMAL | ANTITRUST | CONGRESSIONAL | ECONOMIC | LEGAL
Privacy Policy | About FTC | Commissioners | File a Complaint | HSR | FOIA | IG Office | En Español

Tab 11

Prev: Chapter 210-B §1346

Next: Chapter 210-B §1348

Title 10: COMMERCE AND TRADE**Part 3: REGULATION OF TRADE****Chapter 210-B: NOTICE OF RISK TO PERSONAL DATA (HEADING: PL 2005, c. 379, §1 (new))**Download Chapter 210-B
PDF, Word (RTF)Download Section 1347
PDF, Word (RTF)**§1347. Definitions (CONTAINS TEXT WITH VARYING EFFECTIVE DATES)**

Statute Search As used in this chapter, unless the context otherwise indicates, the following terms have
List of Titles the following meanings. [2005, c. 379, §1 (new); §4 (aff).]
Maine Law

1. (TEXT EFFECTIVE UNTIL 1/31/07) Breach of the security of the system.

Disclaimer "Breach of the security of the system" or "security breach" means unauthorized acquisition
Revisor's Office of an individual's computerized data that compromises the security, confidentiality or
integrity of personal information of the individual maintained by an information broker.

Maine Legislature Good faith acquisition of personal information by an employee or agent of an information
broker for the purposes of the information broker is not a breach of the security of the
system if the personal information is not used for or subject to further unauthorized
disclosure. [2005, c. 379, §1 (new); §4 (aff).]

1. (TEXT EFFECTIVE 1/31/07) Breach of the security of the system. "Breach of the security of the system" or "security breach" means unauthorized acquisition of an individual's computerized data that compromises the security, confidentiality or integrity of personal information of the individual maintained by a person. Good faith acquisition of personal information by an employee or agent of a person on behalf of the person is not a breach of the security of the system if the personal information is not used for or subject to further unauthorized disclosure. [2005, c. 583, §1 (amd); §14 (aff).]

2. Encryption. "Encryption" means the disguising of data using generally accepted practices. [2005, c. 379, §1 (new); §4 (aff).]

3. Information broker. "Information broker" means a person who, for monetary fees or dues, engages in whole or in part in the business of collecting, assembling, evaluating, compiling, reporting, transmitting, transferring or communicating information concerning individuals for the primary purpose of furnishing personal information to nonaffiliated 3rd parties. "Information broker" does not include a governmental agency whose records are maintained primarily for traffic safety, law enforcement or licensing purposes. [2005, c. 379, §1 (new); §4 (aff).]

4. Notice. "Notice" means:

A. Written notice; [2005, c. 379, §1 (new); §4 (aff).]

B. Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 United States Code, Section 7001; or [2005, c. 379, §1 (new); §4 (aff).]

C. (TEXT EFFECTIVE UNTIL 1/31/07) Substitute notice, if the information broker demonstrates that the cost of providing notice would exceed \$5,000, that the affected class of individuals to be notified exceeds 1,000 or that the information broker does not

have sufficient contact information to provide written or electronic notice to those individuals. Substitute notice must consist of all of the following:

- (1) E-mail notice, if the information broker has e-mail addresses for the individuals to be notified;
- (2) Conspicuous posting of the notice on the information broker's publicly accessible website, if the information broker maintains one; and
- (3) Notification to major statewide media.
[2005, c. 379, §1 (new); §4 (aff).]

C. (TEXT EFFECTIVE 1/31/07) Substitute notice, if the person maintaining personal information demonstrates that the cost of providing notice would exceed \$5,000, that the affected class of individuals to be notified exceeds 1,000 or that the person maintaining personal information does not have sufficient contact information to provide written or electronic notice to those individuals. Substitute notice must consist of all of the following:

- (1) E-mail notice, if the person has e-mail addresses for the individuals to be notified;
- (2) Conspicuous posting of the notice on the person's publicly accessible website, if the person maintains one; and
- (3) Notification to major statewide media.
[2005, c. 583, §2 (amd); §14 (aff).]
[2005, c. 379, §1 (new); §4 (aff); c. 583, §2 (amd); §14 (aff).]

5. (TEXT EFFECTIVE UNTIL 1/31/07) Person. "Person" means an individual, partnership, corporation, limited liability company, trust, estate, cooperative, association or other entity. "Person" as used in this chapter may not be construed to require duplicative notice by more than one individual, corporation, trust, estate, cooperative, association or other entity involved in the same transaction. [2005, c. 379, §1 (new); §4 (aff).]

5. (TEXT EFFECTIVE 1/31/07) Person. "Person" means an individual, partnership, corporation, limited liability company, trust, estate, cooperative, association or other entity, including agencies of State Government, the University of Maine System, the Maine Community College System, Maine Maritime Academy and private colleges and universities. "Person" as used in this chapter may not be construed to require duplicative notice by more than one individual, corporation, trust, estate, cooperative, association or other entity involved in the same transaction. [2005, c. 583, §3 (amd); §14 (aff).]

6. (TEXT EFFECTIVE UNTIL 1/31/07) Personal information. "Personal information" means an individual's first name, or first initial, and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:

- A. Social security number; [2005, c. 379, §1 (new); §4 (aff).]
- B. Driver's license number or state identification card number; [2005, c. 379, §1 (new); §4 (aff).]
- C. Account number, credit card number or debit card number, if circumstances exist wherein such a number could be used without additional identifying information, access codes or passwords; [2005, c. 379, §1 (new); §4 (aff).]
- D. Account passwords or personal identification numbers or other access codes; or [2005, c. 379, §1 (new); §4 (aff).]
- E. Any of the data elements contained in paragraphs A to D when not in connection with the individual's first name, or first initial, and last name, if the information if compromised would be sufficient to permit a person to fraudulently assume or attempt to assume the identity of the person whose information was compromised. [2005, c. 379, §1 (new); §4 (aff).]

"Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media.
[2005, c. 379, §1 (new); §4 (aff).]

6. (TEXT EFFECTIVE 1/31/07) Personal information. "Personal information" means an individual's first name, or first initial, and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:

- A. Social security number; [2005, c. 379, §1 (new); §4 (aff).]
- B. Driver's license number or state identification card number; [2005, c. 379, §1 (new); §4 (aff).]
- C. Account number, credit card number or debit card number, if circumstances exist wherein such a number could be used without additional identifying information, access codes or passwords; [2005, c. 379, §1 (new); §4 (aff).]
- D. Account passwords or personal identification numbers or other access codes; or [2005, c. 379, §1 (new); §4 (aff).]
- E. Any of the data elements contained in paragraphs A to D when not in connection with the individual's first name, or first initial, and last name, if the information if compromised would be sufficient to permit a person to fraudulently assume or attempt to assume the identity of the person whose information was compromised. [2005, c. 379, §1 (new); §4 (aff).]

"Personal information" does not include information from 3rd-party claims databases maintained by property and casualty insurers or publicly available information that is lawfully made available to the general public from federal, state or local government

records or widely distributed media.

[2005, c. 583, §4 (amd); §14 (aff).]

7. System. "System" means a computerized data storage system containing personal information.[2005, c. 379, §1 (new); §4 (aff).]

8. (TEXT EFFECTIVE UNTIL 1/31/07) Unauthorized person. "Unauthorized person" means a person who does not have authority or permission of an information broker to access personal information maintained by the information broker or who obtains access to such information by fraud, misrepresentation, subterfuge or similar deceptive practices.[2005, c. 379, §1 (new); §4 (aff).]

8. (TEXT EFFECTIVE 1/31/07) Unauthorized person. "Unauthorized person" means a person who does not have authority or permission of a person maintaining personal information to access personal information maintained by the person or who obtains access to such information by fraud, misrepresentation, subterfuge or similar deceptive practices.[2005, c. 583, §5 (amd); §14 (aff).]

Section History:

PL 2005, Ch. 379, §1 (NEW).

PL 2005, Ch. 379, §4 (AFF).

PL 2005, Ch. 583, §1-5 (AMD).

PL 2005, Ch. 583, §14 (AFF).

The Revisor's Office cannot provide legal advice or interpretation of Maine law to the public. If you need legal advice, please consult a qualified attorney.

Office of the Revisor of Statutes
7 State House Station
State House Room 108
Augusta, Maine 04333-0007

This page created on: 2006-11-01

Tab 12



Group Pushes Congress For Data Protection; Cites More Than 100 Million Compromised Personal Records

CSIA warns that political and economic fallout will continue until lawmakers agree on a uniform federal data protection standard.

By K.C. Jones, InformationWeek

Dec. 15, 2006

URL: <http://www.informationweek.com/story/showArticle.jhtml?articleID=196700229>

The Cyber Security Industry Alliance is calling on Congress to enact federal laws requiring public and private entities to secure sensitive personal information.

"The continued mishandling of personal information is a problem affecting every corner of the country and a wide range of organizations, including private sector corporations, government agencies, financial firms, educational institutions, healthcare and insurance companies," CSIA wrote in a statement outlining its reasons behind the push for new legislation. "The types of personal information that have been lost range from medical records to Social Security numbers to bank account details. Furthermore, the burden is on the victims to determine what degree of risk they face and how best to protect themselves from future incidents, creating a frustrating and daunting situation for so many Americans."

More than 100 million personal records, or roughly one record for every three Americans, have been compromised since February 2005, according to the Privacy Rights Clearinghouse. CSIA estimates that the average victim of identity theft spends \$834 and 77 hours to clear their name.

As the number of data breaches grows, states, local governments, and private groups are creating a patchwork of regulations and guidelines to try to deal with the problem. CSIA, which has done a number of surveys on attitudes about information security and identity theft, warns that political and economic fallout will continue until lawmakers agree on a uniform federal standard.

"Congress should be very concerned about this milestone not only because of the sheer number of individuals affected, but also because the decline in consumer confidence in the security of personal information is a serious drag on our economy," CSIA Executive Director Paul Kurtz said through a statement released Thursday.

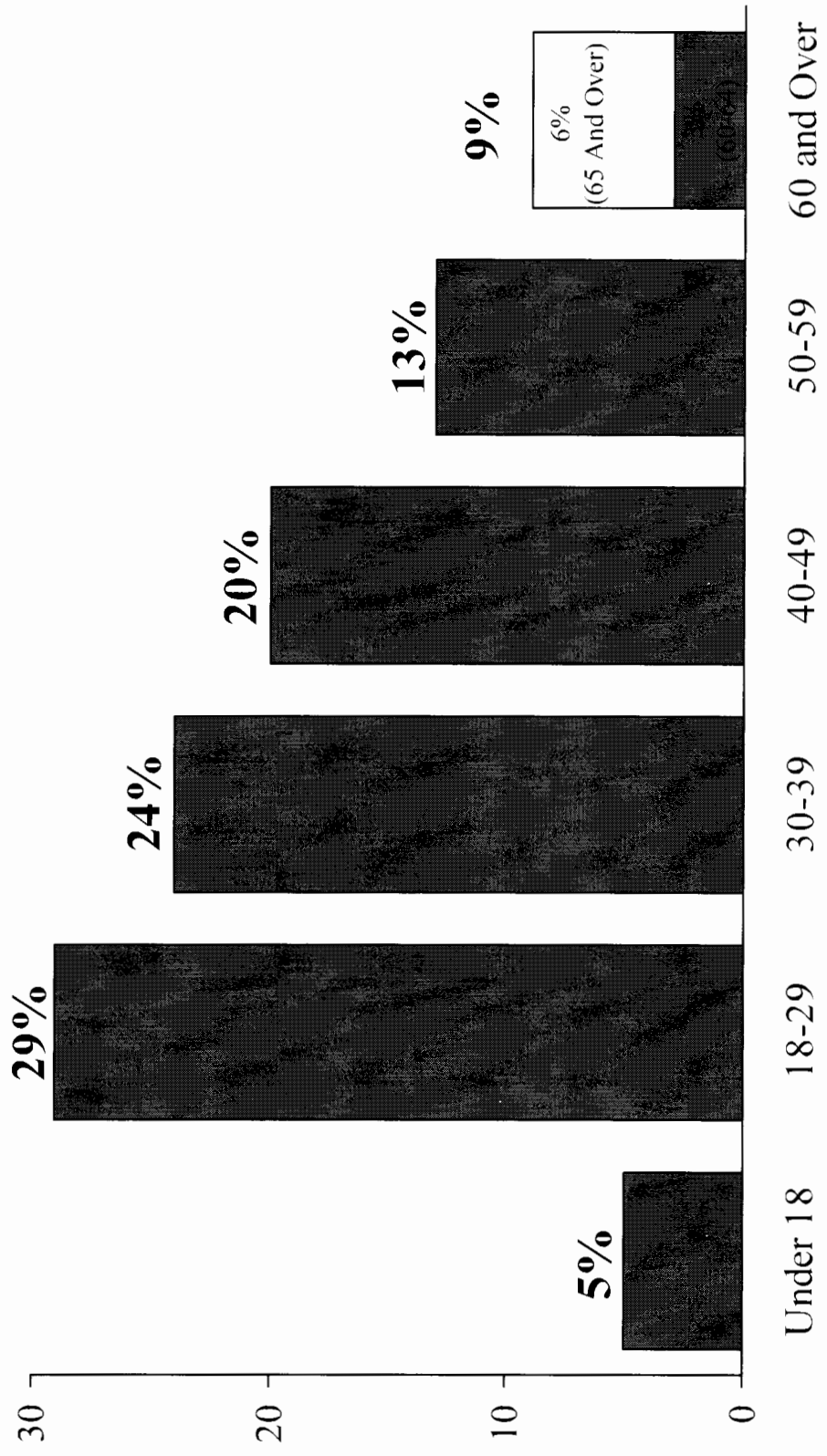
Ninety-five percent of voters responding to a survey conducted in the spring of 2006 said that identity theft is a serious problem and less than one in five said they believe that existing laws protect their privacy. Seventy-two percent said the private sector should do more to protect their personal information.

About 44% of American Internet users, or 70 million people who are confident that their Internet transactions are safe, spend an average of \$116 online every month, according to CSIA. Online retailers could be losing up to \$3.8 billion a month from the remaining 38 million people who avoid making online purchases because of a lack of confidence in information security, according to CSIA.

Tab 13

Figure 6 Identity Theft Complaints by Victim Age¹

January 1 – December 31, 2005



¹Percentages are based on the total number of identity theft complaints where victims reported their age (239,277). 95% of the victims who contacted the Federal Trade Commission directly reported their age.