HB

226

HOUSE COMMITTEE REPORT

(7)
Date Referred to Committee: April 22, 2005 **FURTHER REFERRALS: Finance**

Date of Committee Action: 02/10/06

The JUDICIARY Committee considered: **HB 226**

HOUSE BILL NO. 226 **PERSONAL INFORMATION BREACH**

"An Act relating to breaches of security involving personal information; and relating to credit report security freezes."

Recommends it be replaced with [ ] HCS *or* [X] CS for HB 226 (JUD)
For Senate Bills with new title: [ ] Technical Title [ ] New Title: HCR_____ [ ] Same Title [ ] New Title

[ ] attach amendments
[ ] add new referral to _____Committee
[ ] Letter of Intent_____Committee

List of Abbrev for Depts.:
ADM
CED
COR
CRT
EED
DEC
DFG
GOV
HSS
LEG
LAW
LWF
MVA
DNR
DPS
REV
DOT
UA

NEW FISCAL NOTES *Assigned by Chief Clerk's Office

List by Dept(s):	*FN#	Fiscal	Indet.	Zero
LAW				X

PREVIOUS FISCAL NOTES

List by Dept(s):	FN#	Fiscal	Indet.	Zero

Signing with recommendations	Printed Last Name	DP	DNP	NR	AM
	Gara	✓			
	Coghill			✓	
	WILSON	✓			
	Gruenberg	✓			
	ANDERSON				X
	KOTT			✓	
Chair:	McGuire	✓			
Chair:					

FISCAL NOTE

STATE OF ALASKA
2006 LEGISLATIVE SESSION

Fiscal Note Number:
Bill Version: HB226-LAW-C&FB-2-9-0
() Publish Date:

Revision Date/Time ("Note if correction):
Dept. Affected: LAW
Title "An Act relating to breaches of security involving personal information; and relating to credit report..."
RDU CIVIL
Component Commercial & Fair Business
Sponsor Representative Gara
Requester House Judiciary
Component No.

Expenditures/Revenues (Thousands of Dollars)

Note: Amounts do not include inflation unless otherwise noted below.

OPERATING EXPENDITURES	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
Personal Services						
Travel						
Contractual						
Supplies						
Equipment						
Land & Structures						
Grants & Claims						
Miscellaneous						
TOTAL OPERATING	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**
CAPITAL EXPENDITURES						
CHANGE IN REVENUES ( )						

FUND SOURCE (Thousands of Dollars)

1002 Federal Receipts						
1003 GF Match						
1004 GF						
1005 GF/Program Receipts						
1037 GF/Mental Health						
Other (Specify Type--Do not abbreviate)						
TOTAL	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**

Estimate of any current year (FY2005) cost: 0.0
Mark this box (X) if funding for this bill is included in the Governor's FY 2006 budget proposal:

POSITIONS

Full-time						
Part-time						
Temporary						

ANALYSIS: *(Attach a separate page if necessary)*

This bill ads a chapter to AS 45 that imposes disclosure requirements on businesses that collect and store personal information if there is a security breach of the businesses' information system. In the event of a security breach, notice of the breach must be made to consumers by either written or electronic means, with some exceptions if the notice will cost more than $250,000, or the number of affected consumers exceeds 500,000. Consumers can bring a court action for violations of this law to recover damages and injunctive relief.

The bill also ads a section that allows consumers to place a security freeze on his or her credit report. When a security freeze is in place, a credit reporting agency may not release information from the consumer's credit report to third parties unless requested by the consumer. There are several exemptions for access required to correct technical information, and for some agencies like the child

Prepared by: Kathryn Daughhetee, Director
Phone 465-3673
Division Administrative Services Division
Date/Time 2/9/06 4:33 PM
Approved by: Kathryn Daughhetee for David Márquez, Attorney General
Date 2/9/2006
Agency Department of Law

STATE OF ALASKA **BILL NO.** _____
2005 LEGISLATIVE SESSION

ANALYSIS CONTINUATION

support enforcement agency, Department of Health and Social Services, and Department of Revenue. Court action can be brought by consumers to enforce this law. Remedies include injunctive relief, damages (including lost wages and pain and suffering), and punitive damages up to $5000.

Violations of the provisions of this bill are not automatically violations of Alaska's Consumer Protection Act. Consumers will likely be left to their own enforcement efforts for violations of this Act except in the most agregious cases where the State may bring an action. I do not believe there will be any significant fiscal impact to the Department of Law from this bill.

ALASKA STATE LEGISLATURE

REPRESENTATIVE LES GARA REPRESENTATIVE JOHN COGHILL

CSHB 226 (L&C): Personal Information Breach / Security Freeze

Sponsor Statement

In February ChoicePoint, Inc., a Georgia-based financial database company admitted personal information affecting almost 150,000 consumers had been stolen from its company. Recently the company admitted it knew of this breach since the fall and had delayed letting consumers, including 251 Alaskans, know about the breach until last month. HB 226 is based on two provisions in California law.

This bill requires that any business or governmental entity that collects this personal customer information as part of their business must notify consumers if the security of that information is compromised. California is currently the only state to mandate consumer notification and this bill is modeled after the California law.

Once an individual learns or believes their personal information has been compromised, that person should be able to block access to credit reports and credit scores. Blocking access to a credit report prevents an identity thief from fraudulently opening new lines of credit in his or her name.

The second section of the bill contains this "security freeze" provision. There are three companies in the country (Experian, Equifax and TransUnion) which act as consumer financial information clearinghouses, and that provide consumer data to banks, credit card, insurance, and other companies. The security freeze provision allows consumers to prevent the clearinghouses from sharing their information. The provision will allow a consumer to regulate who will receive a copy of their credit report. Under the security freeze provision the consumer is required to give the credit reporting agency an access code to release their report to a company wishing to extend a line of credit.

Many businesses like ChoicePoint make money by selling consumer information. Alaskans value their privacy. Companies that profit from trading financial and personal information need to protect that information.

Representative Les Gara
State Capitol, Room 418
Juneau, AK 99801
(907) 465-2647

Representative John Coghill
State Capitol, Room 204
Juneau, AK 99801
(907) 465-3719

ALASKA STATE LEGISLATURE

REPRESENTATIVE LES GARA

SECTIONAL ANALYSIS

CSHB 226 (L&C) – Personal Information Breach / Security Freeze

---

Section 1 Establishes *Chapter 48 – Information Security* under AS 45.

Article 1. Breach of Security Involving Personal Information.

- **Sec. 45.48.010.** A business or governmental agency must notify Alaskans of any breach of security that compromises their personal information.

- **Sec. 45.48.020 – 45.48.060.** The business or governmental agency may notify people of a breach by email or written documentation. These disclosures may be delayed if it would compromise a Dept. of Law investigation. An exception is made for employees or agents of a business who view personal information if they do not use that information for purposes unrelated to the business. An exception is also made if the business or governmental agency already has a policy in place that complies.

- **Sec. 45.48.070.** A person has the right to civil legal action if any part of AS 45.48.010 - 45.48.090 is violated.

- **Sec. 48.45.090.** Definitions.

Article 2. Security Freeze.

- **Sec. 45.48.100.** A consumer may freeze part or all of their credit report information.

- **Sec. 45.48.110 – 45.48.120.** To place a security freeze a person must notify credit reporting agencies by certified mail. The reporting agency is then required to place the freeze within 5 days after receiving the request and send a written confirmation of the security freeze within 10 days. A personal identification number or password must accompany this written confirmation for the consumer to use when authorizing the release of their credit report.

- **Sec. 45.48.130.** Once a security freeze is in place a consumer may contact a credit reporting agency to release their credit information to a specific third party. The consumer must provide proper identification, the password or number provided under the previous section, and information to identify the party to allow access to. The reporting agency must comply with a consumer's request within 3

days. Once a security freeze is in place, a credit reporting agency may not release a credit report without prior authorization.

- **Sec. 45.48.140 – 45.48.150.** If a consumer requests a security freeze, the credit reporting agency must disclose the process to the consumer. A credit reporting agency must remove a security freeze within 3 days if the consumer requests it.

- **Sec. 45.48.160.** Credit reporting agencies may not charge more than $10 to place or remove a security freeze or more than $12 to allow access for a specific person. They may not charge a fee if the person has had personal information stolen.

- **Sec. 45.48.170 – 45.48.180.** A credit reporting agency may require additional information from the consumer only when needed to reasonably identify the consumer. During a security freeze a credit reporting agency may not change information in a consumer's file without sending confirmation to the consumer.

- **Sec. 45.48.190.** A person who suffers damages as a result of AS 45.48.100 – 45.48.290 may bring about a court action and recover damages. A person who knowingly violates these sections is also liable in a class action suit.

- **Sec. 45.48.270.** Certain reports are not covered by AS 45.48.100 – 45.48.290. These reports include:
  - Reports that contain only information about transactions between the consumer and the person making the report.
  - Reports that are internal communications within the organization that is making the report as long as the consumer is informed that this information may be communicated.
  - Reports of an authorization or approval of a specific extension of credit.
  - Reports that contain only information about a person's decision whether to extend credit if the person is informed where
  - Reports that contain only general information such as character, reputation, personal characteristics gained from personal interviews.
  - Reports that contain credit information to be used only for a commercial purpose.

- **Sec. 45.48.280.** Certain uses of credit reports are exempted from the provisions of AS.45.48.100 – 45.48.290. These include use by the Dept of Health and Social Services when investigating fraud, use by the Dept. of Revenue when investigating or collecting delinquent taxes, and use by a state or municipal agency that establishes and enforces child support obligations.

- **Sec. 45.48.290.** Definitions.

Article 3. General Provisions.

- **Sec. 45.48.300.** If any provision of AS 45.48 conflicts with federal law, the provision does not apply to the extent of the conflict.

- **Sec. 45.48.390.** Definitions.

adn.com
Anchorage Daily News

Identity thieves may have hit Alaska

CHOICEPOINT: Information clearinghouse breach could have compromised privacy of 251.

By RICHARD RICHTMYER
Anchorage Daily News

(Published: February 24, 2005)

Identity thieves who scammed information clearinghouse ChoicePoint Inc. may have obtained the personal information -- including names, addresses and Social Security numbers -- of 251 Alaskans.

The security breach, which ChoicePoint has known about since last fall but made public only this month, involves more than 145,000 consumers nationwide, the company said.

The scope of the fraud and the lapse in ChoicePoint's security underscore how vulnerable consumers are and highlight weaknesses in Alaska laws to protect against identity theft, said Steve Cleary, executive director of the Alaska Public Interest Research Group.

State lawmakers are considering toughening identity-theft penalties. Cleary's group is urging them to go even further to help Alaskans guard against being ripped off when their personal information falls into the wrong hands.

ChoicePoint is sending letters to all the affected consumers, notifying them they may be at risk. They should all be delivered within 10 days, said Chuck Jones, a spokesman for the Georgia-based company.

The company will offer affected consumers free credit reports and credit-monitoring service for a year, and it is setting up a single point of contact where they can place security alerts on their credit files maintained by all three major credit reporting companies: Experian, Trans-Union and Equifax, Jones said.

Identity theft occurs when someone steals your personal information, such as a Social Security number and date of birth, and uses it to commit fraud.

There has been one confirmed case of identity theft resulting from the incident, and Jones said investigators have determined that the suspects have tried to defraud at least 750 others. He would not say where they live, referring specific questions about the investigation to officials at the Los Angeles County Sheriff's Department, who did not return phone calls Wednesday.

ChoicePoint was formed in 1997 as a spin-off of Equifax. It makes money by selling information in its massive database of personal information to a wide range of businesses, including corporations conducting pre-employment background checks and insurance companies assessing the risk of potential clients.

The company discovered last fall that it had opened up portions of its database to scam artists in the Los Angeles area who were posing as legitimate businesses. ChoicePoint alerted the county sheriff's department, which began an investigation. It delayed notifying consumers at the request

of authorities, who didn't want to jeopardize their investigation, Jones said.

News of the security breach broke last week as some 35,000 Californians began receiving notification that their personal information might have been compromised. That is the only state that requires such notification, according to the U.S. Public Interest Research Group.

The company began notifying the rest of the affected consumers after the attorneys general of dozens of other states, including Alaska, jointly sent a letter to ChoicePoint's top lawyer demanding that the company notify potential victims in their states as well.

Jones said the company initially notified Californians only because it thought the fraud had been isolated to that state, not because of the state law requiring it to do so.

AkPIRG's Cleary didn't buy that argument. "It just doesn't seem plausible," he said.

State lawmakers this session already are considering a bill that would make identity theft in Alaska a felony rather than a misdemeanor offense.

AkPIRG is urging them to add two measures to that bill that would protect Alaskans against identity theft if a security breach similar to the one that happened at ChoicePoint happens again, Cleary said.

The group has submitted legislation, modeled on other state laws, to members of the House Judiciary Committee, which is working on the identity-theft bill.

It would require companies that keep personal information on file to notify consumers if it knows their information is at risk of being compromised, similar to the requirement in California's law. It also would allow consumers more control over who can access their credit reports, which the group said is similar to laws in California, Louisiana, Texas and Vermont.

Staff members for Rep. Tom Anderson, R-Anchorage and the bill's sponsor, and Judiciary Committee chairwoman Lesil McGuire, R-Anchorage, said they hadn't had a chance to review AkPIRG's proposal, which they received Wednesday morning, and couldn't comment on its merits.

Daily News reporter Richard Richtmyer can be reached at rrichtmyer@adn.com or 257-4344.

Identity crisis?

If you think you might be a victim of identity theft, the best way to check is to look at your credit report.

• A recent change in federal laws requires that each of the major credit reporting bureaus provide free of charge one credit report per year to any consumer who asks for it. They're available at www.annualcreditreport.com, or by phone, toll-free, at 1-877-322-8228.

• A quick review of your credit report will enable you to detect fraudulent credit-card accounts and loans taken out by identity thieves. If you find something amiss on any one of the three reports, contact the credit reporting bureau and place a security alert on your file. That will warn the bureaus to look for fraudulent credit applications submitted in your name and require lenders to contact you personally before extending any credit.

• Here are the toll-free numbers of the major credit reporting bureaus to call if you suspect you're an identity theft victim: Equifax: 1-800-525-6285 Experian: 1-888-397-3742 TransUnion: 1-800-680-7289

The article "14 tips to avoid identity theft" is by reformed con artist Frank W. Abagnale, subject of the movie "Catch Me If You Can."

This Federal Trade Commission page has more advice for consumers looking to avoid identity theft.

Victims of ID theft fight for years to repair sprawling mess

IDENTITY: "You're guilty until proven innocent," says woman who was hurt by a criminal.

By JAMES JAMES
Chicago Tribune

WASHINGTON — Since falling victim to identity theft four years ago, John Harrison has learned the hard way that the crime is like a chronic disease that goes into remission, only to flare up again when least expected.

"I dealt with my latest debt collector just a week ago," the 44-year-old salesman for a firearms maker said.

"And the Army actually just garnisheed my retirement pay for the third time," said Harrison, a retired infantry captain who lives in Connecticut.

The man who misused Harrison's personal information not only obtained credit using Harrison's name but also opened checking accounts and wrote more than 126 bad checks as Harrison, some of them on government installations.

"The ones that were written on military bases become government debt," Harrison said. "And because I'm retired and get a government paycheck, when those things start to, I just get a government letter in the mail saying, 'We're taking your money.'"

The Federal Trade Commission estimated 10 million people were victimized by the crime in 2002, the most recent year for which it has data.

Recent disclosures by consumer-data collection companies including ChoicePoint, LexisNexis and Bank of America that sensitive information about millions of consumers was compromised have fueled concerns that many more people could be victimized like Harrison.

If those failures to protect consumers' personal data lead to more identity theft, the victims would be added to what experts consider the fastest-growing financial crime in the United States.

The Federal Trade Commission estimated 10 million people were victimized by the crime in 2002, the most recent year for which it has data.

No credible expert believes that number has fallen. Identity theft costs the U.S. economy billions of dollars annually.

See Page A-5, IDENTITY

John Harrison says it has taken him years to straighten out the mess caused when he became a victim of identity fraud.

Anchorage Daily News 4/3/05

IDENTITY: *As credit industry, politicians debate costs, victims struggle*

Continued from A-1

While federal and state governments and businesses that extend credit have made progress in helping victims regain their financial footing, the experience of victims shows much more is left to be done.

COUNTERMEASURES

In January, for example, a Springfield, Ill., police officer made a routine traffic stop of a 78-year-old woman, an identity-theft victim, according to Illinois Attorney General Lisa Madigan.

The officer ran the motorist's name through the state's criminal database, which turned up a warrant for writing bad checks. It was the identity thief, however, who wrote the checks.

Nevertheless, "the poor, little old lady was hauled off to the police station," Madigan said. That occurred even though the identity theft took place in 1998 and she had reported it to state law-enforcement officials.

The arrest also happened even though the attorney general two years ago had pushed legislation through the Illinois General Assembly meant to prevent that kind of humiliation.

Such an arrest might have been avoided if there had been a statewide database of identity-theft victims, something Madigan is trying to implement.

The financial services industry has raised concerns about such databases, fearing that unscrupulous borrowers could falsely claim to be identity-theft victims to avoid paying debts.

Something that could help victims and nonvictims alike would be to give them the ability to deny prospective credit providers access to credit bureau files for the purpose of issuing new credit. That could stop identity thieves.

Victim advocates say a federal law to that effect would help greatly. So far, only California and Texas allow victims to place security freezes on their files maintained by the three largest national credit bureaus.

But a dozen states are considering following suit, said Gail Hillebrand, a senior attorney with Consumers Union, an advocacy group.

Banks, car dealers and other businesses have opposed such legislation, however, raising doubts about such laws' effectiveness.

And such freezes could deny consumers the instant gratification of walking into stores, getting rapid credit approvals and leaving with cars, televisions or refrigerators.

CRITICAL STAGE

"The problem is, let's say mortgage interest rates dropped and I wanted to refinance," said Kirsten Fedda, senior federal counsel at the American Bankers Association.

"It's going to be an impediment. It's an unnecessary cost. It would probably end up frustrating more customers than helping them," Fedda said.

Creditors say they have taken steps to fight identity theft. Using advanced computer technology, companies can often spot fraud by detecting unusual spending patterns, for instance.

But victim advocates say the financial-services industry isn't moving aggressively enough, in part because they say the industry can pass along the costs of identity theft to other customers through fees and additional charges.

Identity-theft experts add that while the financial industry often advises consumers to protect themselves from the crime by shredding credit-card statements and the like, consumers are helpless in most cases of identity theft since lax security at companies or unscrupulous employees are often to blame.

Identity-theft victims and their advocates acknowledge the situation has improved in recent years for many victims, who sometimes include children whose Social Security numbers are misused by dishonest parents to obtain credit. They ruin the children's credit, making it hard for them to get loans later.

The improvement started with increased sensitivity to the victims among many law-enforcement officials, government policy makers and financial industry executives who once appeared to operate as though identity theft were a victimless crime.

A 2003 federal law resulted in changes phased in over the past year requiring businesses taken in by identity thieves to provide victims with the fraudulent credit applications. Before, victims routinely were denied such information.

California has a security-breach law in which consumer-data companies must notify consumers when security around sensitive consumer information has been compromised.

It was that law that required ChoicePoint to go public with its problem. About 20 states are considering similar laws.

Some states also have passed laws requiring police departments to take crime reports from identity-theft victims. Illinois allows victims to go to court to obtain a factual declaration of innocence.

Still, numerous proposals that would have helped identity-theft victims have been rebuffed in Congress and state legislatures.

'YOU'RE GUILTY'

During the recent Senate debate over legislation to tighten bankruptcy rules, Sen. Ben Nelson, D-Neb., tried to pass an amendment exempting debtors who could prove their financial problems were caused by identity theft. He failed.

Meanwhile, Linda Foley, executive director of the Identity Theft Resource Center and herself a victim of identity theft, asked, "Why don't we have all states requiring that victims of identity theft are allowed to have police reports taken, that the police must take police reports in the jurisdiction where the victim lives?"

She said even more understanding is needed of the "secondary wounding" that occurs after someone is targeted.

She blames the collection agencies, credit issuers and credit bureaus — as well as law enforcement — for requiring victims to provide copious documentation, which can be time consuming and expensive.

"It's frustrating," Foley said. "You're guilty until proven innocent."

Harrison, the firearms company salesman, said he stopped keeping track of the time he spent trying to clear his name after he hit 2,000 hours in early 2003, more than a year after he learned his identity was stolen in November 2001.

He blames losing an earlier sales job to the theft when his productivity dropped from having to field calls from collection agents at work.

He suffered from depression and anxiety.

His consumer debt interest rates tripled, and insurance premiums soared inexplicably.

"It's a difficult thing to explain," Harrison said. "I've always been a real strong person. I was a company commander in the 82nd Airborne. I actually kind of thrived in stressful situations.

"But this is (a) different deal because you really don't have any control over what these other people do or don't do," he said. "With identity theft you're not bleeding ... you haven't lost an arm or a leg. It's real difficult for people to see your loss or your damage."

Harrison had trouble finding another job; potential employers were scared off after conducting the standard credit checks. His solace was that the identity thief was caught and served 38 months in prison.

But the thief was released Dec. 15, giving Harrison pause.

"He could still have my Social Security number right in his wallet," he said.

InformationWeek
BUSINESS INNOVATION POWERED BY TECHNOLOGY

Law Requires ChoicePoint To Disclose Fraud

An identity-theft ring gained access to 145,000 consumer records held by ChoicePoint, which later notified consumers as required under California law SB-1386.

By Thomas Claburn, InformationWeek
Feb. 17, 2005
URL: http://www.informationweek.com/story/showArticle.jhtml?articleID=60401882

In its privacy statement, data-aggregation company ChoicePoint Inc. says that it is "dedicated to protecting the privacy of individuals," which includes "strict standards regarding the use and dissemination of personal informa ion."

Yet such dedication is only exceeded by the determination of identity thieves who, by setting up some 50 fictitious businesses, duped the company into granting them access to 145,000 consumer-data profiles it maintains among its store of roughly19 billion public records.

In Los Angeles County Superior Court last week, a Nigerian national who participated in the identity-theft scheme was sentenced to 16 months in state prison. ChoicePoint was alerted of the breach last October. But some 35,000 California consumers didn't realize they were potential victims until they received a letter about the breach from ChoicePoint last week, per California law.

Disclosure of the incident was required under California's SB-1386, which took effect July 1, 2003. According to the law, any state agency, person, or business that does business in California and owns or licenses electronic data that includes personal information, is required to disclose any data security breach to California residents whose unencrypted personal information may have been accessed by an unauthorized person.

While the extent of the fraud arising from the incident may not be known for months, ChoicePoint said it would send out 110,000 more notifications to individuals outside California.

"That's certainly good practice and most responsible companies are going to do that, if no other reason than of mitigating any damages that might result," says Kevin Lyles, partner in the privacy practice at law firm Jones Day. Lyles says another privacy-related law, the Health Insurance Portability and Accountability Act, requires organizations to mitigate any damages as a result of security breaches, and there are similar provisions in the Gramm-Leach-Bliley law.

Gail Hillebrand, senior attorney for Consumers Union, a nonprofit testing and information organization that publishes *Consumer Reports*, suggests such provisions aren't enough. "This is a reminder to all consumers how insecure our personal financial information is when it's held by someone else who makes their own decisions about how much to spend on security," she says. "It highlights the need for consumers to have additional rights to protect themselves, particularly the need for state security freeze laws."

A security freeze lets a consumer prevent people or businesses from accessing a credit reports for the purpose of granting credit. In turn, it prevents identity thieves from accessing a credit report.

Currently, Hillebrand says, freeze laws are being considered in 11 states: Colorado, Connecticut, Hawaii, Illinois, Indiana, Maine, Maryland, Massachusetts, Oregon, Utah, and Washington. California, Louisiana, Texas, and Vermont already have passed some form of freeze law.

Consumers Union is pushing for federal laws th.. would require all companies to inform customers nationwide of data breaches. "We think that will help consumers to protect themselves but also will create a business environment that encourages more investment in security," says Hillebrand. Massachusetts already has a disclosure provision similar to California's, and Illinois may be next.

Yet many oppose a legislative approach to the problem. California state Sen. Debra Bowen's effort last year to expand the data-breach notification requirement to cover disclosures of data in any form, not just electronic data, was voted down amid lobbying by business groups such as the California Chamber of Commerce and the American Electronics Association.

Quinn Jalli, director of privacy and Internet service provider relations at E-marketing company Digital Impact Inc., says that that while data breaches often lead to calls for federal legislation, companies such as ChoicePoint already have a strong incentive to protect their data. "As we saw with spam, legislation is not going to solve the problem," Jalli says.

"This obviously means companies need to do a better job with their information security," Lyles says. "But having a law that says to do that doesn't really help. The problem is technology, and the ability of hackers is moving faster than some companies can move to keep information secure."

Laws don't dictate what companies need to do from a security standpoint, Lyles says. "Almost all the laws that I've seen just say you'll take reasonable security precautions," he explains. "It very well could be that ChoicePoint was using reasonable precautions and that wasn't good enough. The real key is what you do after it. And I think the lesson here for companies is if you have a breach you know about, whether you have a [disclosure] law in the state or not, you ought to let individuals know."

ChoicePoint could not be reached for comment regarding the data breach.

Last year, according to the Federal Trade Commission, consumers reported fraud losses of more than $547 million. Internet-related fraud accounted for 53% of all reported fraud complaints. According to the Better Business Bureau, 9.3 million Americans were victims of identity-theft fraud in 2004.

The New York Times
nytimes.com

March 9, 2005

LexisNexis Says Thieves May Have Taken Data on Consumers

By TOM ZELLER Jr.

In yet another apparent theft of consumers' personal data, the LexisNexis Group, a major compiler of legal and consumer information, said today that about 30,000 of its records - including names, addresses and Social Security numbers of individuals - may have fallen into the hands of thieves.

The announcement follows the recent disclosure several other cases of the loss or theft of consumer data. ChoicePoint, another leading data broker, said last month that it had inadvertently sold the records of more than 140,000 individuals to con artists. And Bank of America said more recently that backup computer tapes containing information on more than a million of its customers had been lost.

The Federal Bureau of Investigation and the Treasury Department are investigating the LexisNexis incident, people close to the inquiry said. The concern in such cases is that criminals can use the information to open credit card accounts in other people's names or engage in various other forms of so-called identity theft.

The LexisNexis breach is almost certain to accelerate calls from privacy advocates and state and federal officials for greater scrutiny of the companies that buy, store and sell consumer data. The issue will be taken up on Thursday in a hearing before the Senate Banking, Housing and Urban Affairs Committee, and next Tuesday at a similar hearing before the House Energy and Commerce Committee.

"I personally see no socially redeeming value in anyone having the right to give away and sell my personal information unless I approve it," the chairman of the House Energy and Commerce Committee, Representative Joe Barton, Republican of Texas, said today.

"Under current law these companies have a legal right to package it and do almost anything they want to do with it," Mr. Barton said. "I just think that's fundamentally wrong. And in the Internet age, it's dangerous."

Some other lawmakers expressed similar sentiments.

"We need to think proactively and treat these data troves with the same level of care and protection that we would any other valuables," Senator Patrick Leahy, Democrat of Vermont, wrote in an e-mail statement. On behalf of the Senate Judiciary Committee, Mr. Leahy is scheduled to testify before the Senate Banking Committee hearing this afternoon. "Our peace of mind, our economy and even our nation's security depend on it," he wrote. The Judiciary Committee also plans to conduct hearings on the issue soon.

As it is, the industry is governed by a hodgepodge of state and federal laws. Critics have argued that because those laws are often at odds and sufficiently ill-defined, the rules permit companies like ChoicePoint and LexisNexis to police themselves as they market consumer data to insurance agencies, background screeners, private detectives, law firms and even the federal government.

Some control is provided by the federal Gramm-Leach-Bliley Act of 1999, which governs the use of personal information maintained by financial institutions. And the Fair Credit Reporting Act of 1970, along with its 2003 amended version, the Fair and Accurate Credit Transactions Act, establishes rules for gaining access to and disseminating consumer reports.

But it has been a matter of debate over how those rules apply to vast information warehouses like ChoicePoint and LexisNexis, which provide a blend of both public and private information, only some of which is of interest to identity thieves. The information services industry has lobbied hard in the past to stall legislation that would put curbs on the kinds of information that can be peddled and to whom. But the succession of large-scale breaches, and the sheer number of consumers being affected by each new incident, will make it harder for the industry to resist some sort of legislative yoke.

"This is going to be hotly fought by people who are gathering and packaging this information," Mr. Barton said. "But I don't see why you have to have Social Security numbers available that are really extraneous to the product at hand."

Several new bills have been introduced in Congress to address the growing problem of consumer privacy, including three submitted in January by Senator Dianne Feinstein, Democrat of California. Mr. Barton has said that he and colleagues from both sides of the aisle have been discussing possible legislative approaches. Senator Charles E. Schumer, Democrat of New York, who chastised another data compiler, WestLaw, in February for making sensitive information like Social Security numbers to easily available, said he plans to introduce legislation next week.

"If we do nothing, identity theft is going to go through the roof," Mr. Schumer said today. "It really means we should get on the stick and do something here. We're in the wild west where companies can do anything they want."

LexisNexis and its parent company in London, the publishing and information services giant Reed Elsevier, said the recent breach involved databases acquired last July through the $775 million purchase of Seisint, a Florida-based compiler of consumer background and asset information.

Seisint has two main products: Accurint, a service for locating people and determining their financial assets, and Securint, a background screening service. LexisNexis has been in the process of folding those Seisint databases into its fleet of legal, news and consumer data archives.

Exactly how thieves gained access to the Seisint databases remains murky. LexisNexis said that the breach was discovered as part of "an ongoing extensive review of the verification, authorization and security procedures and policies" and that it appeared to have occurred well after the Seisint acquisition. The company also said it has been asked by law enforcement officials investigating the matter not to reveal too many details of the crime.

But Kurt Sanford, the chief executive for corporate and federal markets at LexisNexis, which is based in Dayton, Ohio, emphasized that the company's own computer systems did not appear to have been broken into by hackers. Instead, Mr. Sanford said, it appeared that thieves were able to gain access to the log-in names and passwords used by what he described as a handful of legitimate subscribers to the Seisint databases.

Mr. Sanford would not comment on whether the passwords were somehow stolen by hackers breaking into those customers' computers or compromised by less technical means. But once they logged in, the thieves were able to sift through a trove of consumer data without being detected until the legitimate subscribers were billed for their monthly activity.

In early February, Mr. Sanford said, those customers notified LexisNexis of odd activity on their bills. The company took about two weeks to investigate the billing questions, Mr. Sanford said, and then notified law enforcement officials when it became clear that a breach had been made. Reed Elsevier disclosed the breach in a public announcement this morning in London.

The timing is of particular interest in the wake of the breach at ChoicePoint, which has been criticized for delaying notification of the 145,000 affected consumers for more than five months. In that case, the company learned that it had been fooled by thieves posing as legitimate subscribers to its service in late September of last

year. Law enforcement officials were notified, and they asked the company to delay a public announcement until Jan. 1. But ChoicePoint did not publicly disclose the breach until mid-February.

LexisNexis says it plans to begin sending letters to the 30,000 affected consumers in the next few days, similar to the notification process that ChoicePoint recently completed. More than one-third of the people whose data was compromised in the LexisNexis case appear to reside in California, according to a state-by-state breakdown provided by the company. Massachusetts, New York, Florida and Texas were also heavily hit.

All 30,000 consumers will be offered free credit monitoring for one year, according to Mr. Sanford. ChoicePoint made a similar gesture in notification letters that it mailed out in the wake of the security breach there.

But privacy advocates argue that such gestures are not commensurate with the damage such security breaches can bring to consumers' lives.

"Thieves will just put this stuff on the shelf until the heat is off," said Beth Givens, the director of the Privacy Rights Clearinghouse, a consumer advocacy group in San Diego. "They know that there is increased scrutiny of these individuals at this time, and if they read the newspapers, they know that ChoicePoint and Lexis have purchased credit monitoring for one year," Ms. Givens said.

"They need to tell these individuals that they need to be monitoring their credit for the rest of their lives."

LexisNexis Data on 300,000 People Feared Stolen

By Jonathan Krim
Washington Post Staff Writer
Tuesday, April 12, 2005; 12:22 PM

Information broker giant LexisNexis announced today that previously announced security breaches at the company could affect roughly 300,000 consumers, making it one of the largest potential identity theft incidents on record.

When the company announced last month that its Seisint unit had been compromised by identity thieves in a series of incidents, it estimated that Social Security numbers, drivers' license numbers, names and addresses of 32,000 consumers were exposed.

The new figure, the company said yesterday, reflects internal investigations that analyzed data over the past two years and found that identity thieves used IDs and passwords of legitimate Seisint customers to purchase the information.

Last year LexisNexis bought Florida-based Seisint Inc., which sells data gathered from extensive searches of public records to businesses, law-enforcement agencies, private investigators and others.

"We regret that consumers, who traditionally are the primary beneficiaries of our risk management products and services, may have been affected by these events," Kurt Sanford, head of the company's corporate and federal markets group, said in a statement. "We have taken a number of significant actions in recent weeks to further guard against these types of fraudulent intrusions at our customer sites and to enhance our security procedures and policies overall."

The company said that affected consumers would be offered a free credit report and monitoring for a year.

The announcement is yet another blow to the largely unregulated marketplace of sensitive personal information that involves mega-brokers such as LexisNexis, ChoicePoint and Acxiom to smaller re-sellers, some private investigators and others. Each of the three large brokers has announced at last one major breach, as have universities, banks and other organizations that store consumer data.

More than two dozen states are now examining identity theft legislation, while several members of Congress have introduced legislation or are preparing to do so.

washingtonpost.com

Data Brokers Vow to Protect Personal Information

By Jonathan Krim
Washington Post Staff Writer
Wednesday, March 16, 2005; Page E01

Two captains of the information-broker industry told a congressional panel yesterday that they would support new regulations to better protect sensitive personal data that they collect and sell on virtually every adult American.

But the executives balked at what appears to be a growing bipartisan consensus among key House and Senate members that the sale of Social Security numbers for commercial purposes should be banned unless individuals give their permission.

"When my [Social Security] number and my information is routinely given out without my permission, it's just wrong," said Rep. Joe Barton (R-Tex.), who heads the House Energy and Commerce Committee. "And in the Internet age, it's dangerous."

Barton said Congress would probably consider a measure to require permission for the trading or sale of such data except to law enforcement agencies, in addition to other steps to increase oversight of the largely unregulated data-broker industry that has been rocked by a series of security breaches.

Last month, ChoicePoint Inc., one of the nation's largest brokers, announced that personal information on at least 145,000 consumers was bought from the company by thieves who masqueraded as legitimate business people.

Last week, LexisNexis Group, another big broker that specializes in business and legal data, announced that its systems had been penetrated by thieves who obtained data on 32,000 consumers.

Kurt Sanford, chief executive of LexisNexis Corporate and Federal Markets, endorsed a proposal by the head of the Federal Trade Commission, Deborah Platt Majoras, that would extend the same security guidelines to data brokers that financial institutions must follow.

Sanford also agreed with calls for a federal law requiring notification of consumers if their personal information has been obtained by thieves. Only California has such a law.

But Sanford said banning all sales of Social Security numbers would be a mistake, because "there are circumstances where the sale is in the consumers' best interests." For example, he said, independent investigative agencies might need such data to help fight identity fraud. Businesses, he added, need it to help collect unpaid debts.

Derek V. Smith, chief executive of ChoicePoint, agreed.

"I believe that only by adding a more formal structure to the current scheme of information use will we realize the value of technology-based tools to society," Smith said. Both he and Sanford used the hearing as a platform to apologize to consumers whose data have been compromised, and to assure Congress that they have tightened their systems to try to prevent such fraud.

But several members of the House subcommittee on commerce, trade and consumer protection were unimpressed by the companies' efforts.

Raising his voice in a series of rapid-fire questions, Rep. Edward J. Markey (D-Mass.) pressed Smith on whether he would lengthen the credit-alert monitoring period that ChoicePoint has offered to consumers whose information was stolen.

"What about lifetime monitoring?" Markey asked. "One year is not enough. What about five years? Can you guarantee that?" He said thieves might simply lie low for a year before trying to access consumers' accounts.

Smith, appearing rattled, said he would consider extending the service but refused to commit.

AARP Alaska

April 13, 2005

The Honorable Tom Anderson, Chair
House Labor and Commerce Committee
Alaska State Capitol, Room 408
Juneau, AK 99801-1182

RE: HB 226 (Gara)--Support

Dear Chair Anderson:

On behalf of the members of AARP in Alaska, we encourage you and your colleagues on the House Labor and Commerce Committee to support HB 226, authored by Representative Les Gara and co-sponsored by Majority Leader Coghill and Representatives McGuire and Kerttula.

As you know, earlier this year ChoicePoint admitted that it had lost personal information affecting 150,000 customers, including some Alaskans. Although the information was illegally stolen from the company, the company failed to notify their customers at the time they first discovered the information was taken last fall.

HB 226 will mandate that any company that has had its customer financial information stolen must notify those customers that they could be victimized.

HB 226 also requires the three companies that have credit information on all of us to offer security freeze protection. Security freeze protections allow the consumer to determine which companies will be allowed credit information which can be used for lines of credit. This will provide an effective tool to prevent false applications for credit because of stolen information/identity theft.

While your Committee is hearing this bill today, the United States Senate is conducting hearings on the millions of Americans who are victims of identity theft and the billions of dollar they have lost.

This issue needs to be addressed and HB 226 is one good way to help Alaskans.

We urge an "AYE" vote on HB 226.

Should you have any questions about our position, please feel free to contact me (586-3637) or Patrick Luby, AARP Advocacy Director (907-762-3314).

Thank you for your consideration.

Sincerely,

Marie Darlin

Marie Darlin, Coordinator
AARP Capital City Task Force
415 Willoughby Avenue, Apt. 506
Juneau, AK 99801
586-3637 (voice)
463-3580 (fax)

CC: Vice-Chair Pete Kott
Representative Gabrielle LeDoux
Representative Bob Lynn
Representative Norman Rokeberg
Representative Harry Crawford
Representative David Guttenberg
Representative Les Gara

AKPIRG
ALASKA PUBLIC INTEREST RESEARCH GROUP WWW.AKPIRG.ORG
PO Box 101093 • Anchorage, Alaska 99510-1093 • Ph: (907) 278-3661 • Fax: (907) 278-9300 • email: akpirg@akpirg.org

April 4th, 2005

AkPIRG Statement of Support for:

HB 226 / SB 148: Personal Information Breach / Security Freeze

The Alaska Public Interest Research Group (AkPIRG), an Alaska membership organization dedicated to protecting consumers, urges quick passage of HB 226 / SB 148. These bills are an appropriate response to the ChoicePoint Inc. security breach that occurred in February. Consumers across the nation were alarmed to find out that nearly 150,000 people across the nation had their personal information stolen and were at high risk for identity theft. Yet only California had laws on the books that mandated ChoicePoint Inc. to notify those who fell victim.

The total included some 251 Alaskans. This bill will help better protect those individuals and all Alaskans if and when a similar security breach occurs in the future

HB 226 / SB 148 are based on two provisions in California law.

First, the bills require that any business that collects this personal customer information as part of their business must notify consumers if the security of that information is compromised. This common sense step will make sure that companies like Choicepoint Inc. will disclose when consumers are at risk

When a consumer's personal information has been compromised, that person should be able to block access to credit reports and credit scores. Blocking access to a credit report prevents an identity thief from fraudulently opening new lines of credit in his or her name, one of the many dangers of identity theft.

The second section of the bills contains this "security freeze" provision. The three credit reporting agencies - Experian, Equifax and TransUnion - act as consumer financial information clearinghouses The security freeze provision allows consumers to prevent the clearinghouses from sharing their information. Without access to a consumer's credit report, an identity thief will not be able to open a new account. The provision will allow a consumer to regulate who will receive a copy of their credit report. The security freeze provision allows consumers to use an access code to release their report to a company wishing to extend a line of credit.

Any company that makes a profit from trading financial and personal information has the responsibility to protect that information. HB 226 / SB 148 have strong measures that the Alaska Legislature can enact to better protect consumers. We urge you to pass HB 226 / SB 148

Sincerely,

Steve Cleary, AkPIRG Executive Director

NATIONAL ASSOCIATION OF
State PIRGs

Kerry Smith
Senior Consumer Attorney
National Association of
State PIRGs
1334 Walnut St, 8th Floor
Philadelphia, PA 19107
Phone: (215) 732-3747
Fax: (215) 732-3747
ksmith@pirg.org

March 3, 2005

Representative Les Gara
State Capitol, Room 418
Juneau, AK 99801-1182
Fax: 907-465-3518

Dear Representative Gara:

This letter is in response to your inquiry about state level consumer protections against identity theft.

In December 2003, Congress passed the Fair and Accurate Credit Transactions Act (FACT Act). With the FACT Act, Congress significantly amended the Fair Credit Reporting Act (FCRA), which provides consumer protections regarding the use, accuracy, and privacy of consumer credit reports. Through its passage, the financial industry won its primary goal: permanent preemption of stronger state credit and privacy laws in several, but importantly, not all, areas.

In the wake of the ChoicePoint Inc. security breach, mandatory notification is an available and advisable step for states to take to protect consumers. A state law requiring companies to notify consumers about a security breach should not be preempted by the federal Fair Credit Reporting Act. Currently, California is the only state with mandatory notification, but several other states are considering legislation including Connecticut, Georgia, Illinois, Massachusetts, and Texas.

It is imperative that consumers' personal, sensitive information be protected and we urge you to enact mandatory notification. There are many other important consumer protections set forth in: *The Clean Credit and Identity Theft Protection Act: Model State Laws*, which we produced along with Consumers Union. I would be happy to provide you with a copy of those model laws if AkPIRG has not already done so.

I would be happy to answer any questions that you and your colleagues in the Alaska Legislature may have. Thank you for your time and interest in this matter.

Sincerely,

Kerry C. Smith

Kerry Smith
Senior Consumer Attorney

Consumers Union

West Coast Office
1535 Mission St., San Francisco, CA 94103
415-431-6747 (phone) 415-431-0906 (fax)
www.consumersunion.org

April 7, 2005

Representative Les Gara
State Capitol
Room 418
Juneau, AK 99801-1182
907-465-3518 (fax)

Re: Support for HB 226, Breaches of Security and Security Freeze for Credit Reports

Dear Representative Gara:

Consumers Union, the independent, nonprofit publisher of *Consumer Reports*, supports HB 226, relating to Breaches of Security and Security Freeze for Credit Reports. A security freeze is a key tool to prevent identity thieves from getting credit in the consumer's name, by allowing consumers to lock up, or "freeze" access to their consumer credit files for credit granting purposes. A requirement to notify consumers of a breach of security will enable consumers to take preventative steps, including placing a security freeze, at a time when they may be able to ward off an identity thief before the consumer experiences ruined credit and other harmful consequences of ID theft.

Security freeze

Identity theft is one of the fastest growing financial crimes. According to a 2003 report to the Federal Trade Commission, nearly 10 million Americans fall victim to identity theft annually. The Identity Theft Resource Center reports that victims spend an average of $1,495 and 600 hours to restore their credit histories and their good names. Other estimates of the amount of time spent by victims vary, but it is clear that an incursion upon a consumer's good name by an identity thief is a troubling and time-consuming experience. A 2003 report to the Federal Trade Commission estimated that identity theft costs U.S. businesses nearly $48 billion annually and costs U.S. consumers both $5 billion and 297 million hours annually.

A security freeze will help to prevent the damage from identity theft because businesses are highly unlikely to issue new credit to an individual without first reviewing information from his or her credit report. When an individual freezes his or her credit file, this prevents the imposter from using that credit file to get credit in the consumer's name. Because the potential creditor is highly likely to deny the imposter's credit application if it can't see the frozen credit file, a security freeze can prevent the harm that would otherwise occur from the identity theft.

Under this bill, people who choose to freeze access to their credit files may temporarily lift the freeze for new loans and credit that they apply for themselves. When a consumer initially activates the freeze, the credit bureau will issue a unique PIN to the consumer that can be used to

"thaw" or lift the security freeze for a particular creditor. Credit bureaus must release the report within three business days of such a request.

Federal law is inadequate to prevent identity theft

The credit reporting industry may assert that the federal FACT Act, which revised the federal Fair Credit Reporting Act, gives sufficient protection to consumers. We respectfully disagree. Federal law confers the rights of fraud alerts and blocking. Both partially address an identity theft *after* there has been a theft of identity or of information. Nothing in federal law creates a right in the consumer to stop anyone from seeing the consumer's credit file.

The rights available to consumers under federal law are not as effective as a security freeze. Federal law allows identity theft victims to block from the contents of their credit files specific information that is the result of identity theft. But fraud blocking does not block the furnishing of a credit report. It does not prevent identity theft. Similarly, a fraud alert does not prevent a credit report from being issued. Under the federal Fair Credit Reporting Act, when a fraud alert is attached to a credit file, creditors must take additional steps to verify a credit applicant's identity before extending credit. The fraud alert, however, does not prevent the potential creditor from seeing the report, and it does not prevent the credit bureau from selling or sharing the credit report. Only a security freeze can do this.

Consumers can make a choice weighing the protective value of a security freeze against any inconvenience it may pose

The consumer credit reporting industry may also assert that a security freeze will inconvenience consumers who are shopping for credit, as they will have to lift the freeze with respect to each potential creditor. This is a choice Alaskans will be free to make for themselves if the security freeze bill is enacted. Each consumer can decide if the protection of knowing that only creditors authorized by the consumer can review the file for credit granting purposes outweighs the slight delay in requesting that the freeze be lifted for particular potential creditors. This bill will simply give Alaskans the right to make this choice for themselves.

The consumer reporting industry has made it hard for consumers to learn about and use freezes

Consumer reporting agencies have argued in some state legislatures that not many consumers have used the security freeze in the two states where it is already in effect. In one of those states, the freeze is not available to all consumers, but only to ID theft victims. In the other state, California, the Legislature had to go back and amend the statute to cap the fees for placing a freeze after one consumer reporting agency, Experian, was charging consumers $60 for a freeze. This kind of pricing would depress initial usage of the freeze tool.

The bill would be stronger if it exempted ID theft victims from the fee to place a security freeze. Many of the states which are considering security freeze legislations are consider providing this important tool to their consumers who have already been victims of ID theft. The California Legislature is considering eliminating its $10 fee authorization for consumers who have received

a notice of a security breach. While Consumers Union supports the bill in its current form, these changes would strengthen it.

Notice of security breach

The purpose of the required notice is to enable individuals whose information has been accessed by an unauthorized person to take steps to protect their identity, a process that usually entails establishing initial fraud alerts with the three credit bureaus and then checking one's credit report on a regular basis to watch for signs of fraud. If this bill becomes law, Alaskans who receive a notice of security breach could also decide if they wish to take the preventative step of placing a security freeze.

The notice of security breach bill appropriately requires notice to all individuals whose information has been accessed by an unauthorized person. In other states, some opponents of giving notice have argued that notice should be limited to breaches which result in a misuse of information, but this argument is not realistic in light of how ID theft works. An identity thief may steal information from one company and use that information to impersonate a consumer at another company. The company who has the security breach will never be able to ascertain with any certainty whether or not the information has been misused. Further, all stolen information is susceptible to misuse. Indeed, misuse is the usual purpose of the theft of information. Every Alaskan affected by a security breach should get notice, so that the individual can choose to take proactive, preventive steps such as establishing a fraud alert, monitoring his or her credit file and placing a security freeze.

Consumers nationwide learned of the ChoicePoint breach only because one state law required notice of security breaches affecting its residents. Almost daily we hear of new instances of security fraud impacting thousands upon thousands of consumers. Legislation to give consumers control over who can see their consumer credit files through the tool of a security freeze, and to require that companies who have a security breach notify the consumers whose information was accessed is an idea which time has come. For these reasons, Consumers Union supports the passage of this bill.

Very truly yours,

Gail Hillebrand

Gail Hillebrand

Consumers Union

West Coast Office
1535 Mission St., San Francisco, CA
94103
415-431-6747 (phone) 415-431-0906

State Security Freeze Laws are Not Preempted by the Federal FCRA

Assertions by the opponents of state security freeze legislation that it is preempted by federal Fair Credit Reporting Act are wrong. Congress amended FCRA section 625, codified at 15 U.S.C. sec. 1681t, to specifically include identity theft prevention and mitigation in the listing of categories of state laws *not* preempted. Section 1681t(a), the general rule against preemption, preserves state law, except to the extent this rule is modified by (b) and (c). The general rule of section 1681(t)(a), preserves "the laws of any State with respect to the collection, distribution, or use of any information on consumers, or for the prevention or mitigation of identity theft, except to the extent that those laws are inconsistent with any provision of this title, and then only to the extent of the inconsistency." (emphasis added)

Consumer reporting agencies have claimed in some states that a state security freeze law would be preempted by FCRA's provisions on fraud alerts or trade line blocking. This is wrong. Fraud alerts and trade line blocking, Sec. 605A and 605B, are listed in sec. 625(b)(5)(B) and (C), and preempt state law only "with respect to the conduct required by the specific provisions of" 605A and 605B. See 625(b)(5), codified at 15 U.S.C. sec. 168t(b)(5). In other words, the fraud alert and trade line blocking sections preempt states from imposing other fraud alert and other trade line blocking requirements on the same entities reached by the federal statute. However, the preemption extends ONLY to the conduct required by these specific sections. Other "conduct," including a state-created obligation to freeze access to a credit record, falls under the general preservation of state laws in 1681t(a).

The Federal Trade Commission and the Federal Reserve Board, in a regulatory preamble, have emphasized the narrowness of the "conduct required" type of preemption, which is the type that applies to fraud alerts and to trade line blocking, in a regulation relating to the effective date of "conduct required" preemption under section 1681t(b)(5).

In the Joint Final Rule on Effective Dates, 12C.F.R. sec 222; 16 C.F.R. sec. 602, the introductory material emphasizes that FACTA preemption under the "conduct required" formula in section 1681t(b)(5) is narrow. The FTC and Federal Reserve Board state:

> The Agencies note that section 711(2) of the FACTA Act adds a new provision to the FCRA that bars any requirement or prohibition under any state laws "with respect to the conduct required by the specific provisions" of the FCRA, as amended by the FACTA Act. The joint final rules are based on the Agencies' view that the specific protections afforded under the FCRA override state laws only when the referenced federal provisions that require conduct by the affected persons are in effect because that is the time when conduct is required by those provisions of the FCRA.

This analysis was made in connection with the issue of the effective date of conduct required preemption. Read in conjunction with the addition of ID theft to the general no-preemption except for inconsistency rule, it strongly supports the position that if FACTA does not require

conduct in an area related to ID theft, then states remain free to require conduct in that area. This is precisely the case with a security freeze law, a subject simply unaddressed by FACTA.

An extensive legal analysis of the various types of preemption under FACTA, and how those provisions do, and do not, apply to various state legislative measures, by Consumers Union attorney Gail Hillebrand is posted at
http://www.consumersunion.org/creditmatters/creditmattersupdates/001640.html
and printed in: After the FACTA: State Power to Prevent Identity Theft, 17 Loyola Consumer Law Review 53 (2004).

G:\Groups\Credit & Finance\Gr ii\Wallet\2005\noFCRApreemption.doc

LEGISLATIVE RESEARCH REPORT

MARCH 11, 2005

REPORT NUMBER 05.196

CHOICEPOINT AND SECURITY BREACHES OF PERSONAL INFORMATION

PREPARED FOR REPRESENTATIVE LES GARA

BY CHERIE NIENHUIS, LEGISLATIVE ANALYST

You asked about security breaches of personal information. You inquired specifically about the recent security breach involving ChoicePoint, Incorporated.

In February 2005, newspapers around the country reported that ChoicePoint, Inc., an "information clearinghouse," had sent letters to thousands of Californians informing them that their personal information may have been compromised in a fraud scheme. According to ChoicePoint, the scammers posed as legitimate businesses, and acquired the names, Social Security numbers, driver's license numbers, and credit reports of close to 145,000 people nationwide. To date, at least 750 people have been defrauded as a result of the scheme, which the company knew about since the fall of 2004.[1]

CHOICEPOINT, INCORPORATED

ChoicePoint, Inc. is one of several businesses that make money from selling consumer information. Such enterprises generally have no transactions with consumers directly. Rather, they gather data on individuals, from otherwise public records such as home purchases, bankruptcy filings, criminal convictions, and professional licensing boards, for the purpose of brokering the information to other businesses. Other businesses interested in this information include lending companies, insurance agencies, and corporations conducting pre-employment background checks. According to one news source, data brokers like ChoicePoint do not need permission from members of the public to collect and sell their personal information. Further, the

[1] "Response to Customer Fraud Litigation," from the ChoicePoint website, *http://www.choicepoint.com/news/statement_0205_1.html.*

they bypass the rules of the Fair Credit Reporting Act (FCRA)—a law intended to give consumers more control over who can view information that credit agencies collect about them and the right to examine and dispute such information.[2]

Various products sold by ChoicePoint, however, appear to fit the criteria for inclusion under the FCRA, and indeed, ChoicePoint claims they are "FCRA-compliant." The Electronic Privacy Information Center (EPIC), a public interest research center that informs the public about civil liberty, privacy, and constitutional issues, believes that other data products sold by ChoicePoint should be included under the FCRA. In a letter to the Federal Trade Commission dated December 2004 (prior to the public disclosure of the ChoicePoint security breach) the EPIC urged the FTC to investigate two products for inclusion under the federal law, arguing that they meet the criteria of "consumer reports" specified by the FCRA.[3] We include the EPIC's letter, describing products sold by ChoicePoint as Attachment A.

Filings with the Securities and Exchange Commission indicate that among the products ChoicePoint sells are claims history data, motor vehicle records, police records, and credit information. They also provide services related to employment background screenings, drug testing administration, public record searches, vital record services, credential verification, due diligence information, Uniform Commercial Code searches and filings, DNA identification services, authentication services and people and shareholder locator information searches. In addition to private businesses, ChoicePoint has provided personal information to law enforcement agencies and other government entities.[4]

The March 2005 issue of the *Privacy Journal*, a monthly publication that covers legislation and public attitudes affecting the confidentiality of personal information, reports that ChoicePoint is a spin-off of Equifax, one of the nation's three major credit reporting agencies. Chronicles of Equifax, and, indirectly, ChoicePoint, detailed in the article, show that Equifax has on more than one occasion faced charges by the Federal Trade Commission of violating the Fair Credit Reporting Act. We include the *Privacy Journal* article as Attachment B.

CONSUMERS AFFECTED BY CHOICEPOINT SECURITY BREACH

ChoicePoint estimates that the personal information of up to 145,000 consumers could have been compromised by the recently announced security breach. The company also provides information about how many individuals by state may have been affected by the incident. According to the ChoicePoint website, information about 251 Alaskans may have been compromised in the fraud scheme.

Although California is currently the only state that requires companies to notify persons whose information may have been stolen in a security breach, officials with ChoicePoint indicate that

[2] Kim Zetter, "California Woman Sues ChoicePoint," *Wired News*, February 24, 2005, available on the Internet at *http://www.wired.com/news/privacy/0,1848,66710,00.html*

[3] Letter, Chris Jay Hoofnagle and Daniel J. Solove, EPIC, to the Federal Trade Commission, December 16, 2004, as posted at the EPIC website, *http://www.epic.org/privacy/choicepoint/fcraltr12.16.04.html*.

[4] ChoicePoint Inc., "Notes to the Consolidated Financial Statements," September 30, 2004, available online at *http://www.sec.gov/Archives/edgar/data/1040596/000095014404010687/g91731e10vq.htm*.

they sent out letters to all 145,000 consumers they believe may have been affected. This action may have been prompted by a letter from 19 state attorneys general to ChoicePoint, requesting that the company disclose additional information about the incident. Alaska's attorney general was one of the signers of the letter.[5] We include information about ChoicePoint's actions, including a list showing the number of consumers affected by state, as Attachment C.

BREACH OF INFORMATION LEGISLATION

The National Conference of State Legislatures (NCSL) reports that as of early March 2005, legislators in 20 states are considering legislation pertaining to the breach of personal information. One common provision in the recently-introduced legislation is the reporting of security breaches to affected persons. According to NCSL, these provisions are being considered in Arizona, Colorado, Georgia, Idaho, Illinois, Indiana, Minnesota, Missouri, Montana, New Jersey, New York, Ohio, Oregon, Rhode Island, Tennessee, Texas Virginia, Washington, and West Virginia.[6] We provide a copy of NCSL's compilation of breach of information legislation as Attachment D.

I hope you find this information to be useful. Please do not hesitate to contact us if you have questions or need additional information.

---

[5] Todd R. Weiss, "State Officials Push ChoicePoint on ID Theft Notifications," *Computerworld*, February 18, 2005, available on the Internet at *http://www.computerworld.com/printthis/2005/0,4814,99886,00.html*.

[6] California, which already has provisions for notification of affected persons, is considering additional breach of personal information legislation.

Attachment A

Letter, Chris Jay Hoofnagle and
Daniel J. Solove, EPIC, to the
Federal Trade Commission,
December 16, 2004

ELECTRONIC PRIVACY INFORMATION CENTER

December 16, 2004

Federal Trade Commission
600 Pennsylvania Ave. NW
Washington, DC 20580

Re: Request for investigation into data broker products for compliance with the Fair Credit Reporting Act

Dear Commissioners,

In recent years, there has been an explosion in the creation and use of dossiers of personal information to evaluate individuals. Some of these dossiers, known as "data products," in the information brokerage industry, are designed to be sold so that they avoid triggering the provisions of Fair Credit Reporting Act of 1970 (FCRA), a landmark law that ensures that compilations of personal information used for many different purposes are accurate, correctable, fairly collected. Additionally, the FCRA mandates that information collectors be accountable for their practices.

Commercial data broker ChoicePoint, for instance, is selling data products that are used by law enforcement, government, and the private sector to make important decisions about people. ChoicePoint, [1] one of the largest data aggregation companies, became independent from Equifax, a leading U.S. credit rating agency, in 1997.[2] ChoicePoint has bought more than 40 companies and competitors, and obtains 40,000 new public records daily for its database of more than 19 billion records.[3] Choicepoint contracts with about 35 federal agencies to supply data.[4]The company's slogan is "Smarter Decisions. Safer World." However, decisions cannot be smarter, and we cannot be safer, if these new data products are not subject to the basic fairness requirements incorporated in the FCRA.

In 1970, Congress passed the FCRA in response to a litany of problems and complaints about credit reporting agencies.[5] The opening of the FCRA states:

> The Congress makes the following findings:
>
> (1) The banking system is dependent upon fair and accurate credit reporting. Inaccurate credit reports directly impair the efficiency of the banking system, and unfair credit reporting methods undermine the public confidence which is essential to the continued functioning of the banking system.
>
> (2) An elaborate mechanism has been developed for investigating and evaluating the credit worthiness, credit standing, credit capacity, character, and general reputation of consumers.
>
> (3) Consumer reporting agencies have assumed a vital role in assembling and evaluating consumer credit and other information on consumers.
>
> (4) There is a need to insure that consumer reporting agencies exercise their grave responsibilities with fairness, impartiality, and a respect for the consumer's right to privacy.
>
> 15 U.S.C. § 1681(a) (1970).

Americans face a return to the pre-FCRA era if companies like ChoicePoint can amass dossiers on

Americans without compliance with any regime of Fair Information Practices. That era was marked by unaccountable data companies that reported inaccurate, falsified, and irrelevant information on Americans, sometimes deliberately to drive up the prices of insurance or credit.[6] To some extent, this pre-FCRA area has returned. For instance, erroneous ChoicePoint data sold without the FCRA's protections were relied upon in Florida to cleanse voting registration rolls of felons prior to the 2000 election, resulting in the disenfranchisement of thousands of eligible voters.[7]

In an appendix to this letter, we explain ChoicePoint's business activities.[8] ChoicePoint sells a number of FCRA products in the employment screening, tenant screening, and criminal background check fields. But the company also sells two products, "AutoTrackXP" and "Customer Identification Programs" outside of the FCRA's protections. AutoTrackXP is a database of 17 billion records that includes Social Security Number, addresses, property and vehicle information, and other information.[9] The company's anti-fraud "Customer Identification Programs" are a suite of data products that have been created in order to verify the identity and perform background checks on individuals who open new financial services accounts. [10] From its description, Customer Identification Programs appears to be an AutoTrackXP report with additional identity verification services.

These two products are sold to financial institutions, members of the public (private investigators, law firms, etc.) and to law enforcement agencies. These are the same institutions which rely on credit reports and investigative consumer reports, but these new products are sold outside the protections of the FCRA, yet are often used for related (and sometimes identical) purposes.

It is difficult to determine what sources ChoicePoint used to create AutoTrackXP and Customer Identification Programs. However, both of these non-FCRA products have similar data elements and descriptions as ChoicePoint's FCRA products. The similarities between the information in an AutoTrackXP report and the company's FCRA products is striking; it suggests that AutoTrackXP was generated from FCRA sources.[11]

Under a well-developed line of cases, courts interpreting the FCRA have held that if a data product originates from a consumer report database, the product remains protected by the FCRA. For instance, the D.C. Circuit held in *Trans Union v. FTC* that marketing lists drawn from a credit reporting agency's master databases were "credit reports" for purposes of the FCRA.[12]

If ChoicePoint had created AutoTrackXP or its Customer Identification Programs from FCRA sources, the products should be considered "consumer reports" for purposes of the FCRA. Consumers could exercise a series of important rights with respect to their ChoicePoint reports that are not currently available. Only the FTC can determine the "information flows" or sources of data used by ChoicePoint, and whether the company has leaked data from the FCRA products to AutoTrackXP and Customer Identification Programs. We urge the Commission to engage in this inquiry.

Even if these products are not consumer reports for purposes of the FCRA, it is incumbent on the FTC to analyze them and make recommendations to Congress concerning possible expansion of the FCRA. If these products are found not to be within the FCRA, the FTC should recommend to Congress to expand the scope of the Act.

Many of the public policy purposes underlying the FCRA are being circumvented by data brokers who have artfully constructed databases to avoid the Act's provisions. For instance, the use of data products for voter registration list cleansing implicates the most important right in a democracy—access to the polls. If such a use is not covered by the FCRA, this creates an absurd consequence. Someone denied access to a credit card would enjoy access, correction, and other FCRA rights, while another person denied access to the voting polls would have no federal information privacy rights.

Other absurd consequences emerge from this end-run around the protections of the FCRA. Although the

FCRA regulates law enforcement access to consumer report information,[13] the FBI has concluded that information it buys from ChoicePoint is not subject to the FCRA.[14] In effect, the FBI has circumvented the FCRA by purchasing data from AutoTrackXP -- data that is often identical to what appears in a credit report from one of the "big three" agencies. Why would law enforcement agencies continue to comply with fair procedures in the FCRA for access to consumer data when they can get unaccountable, open-door access to the same information at ChoicePoint?

The use of these data products by law enforcement officials, government agencies, private investigators, and others raise the same concerns that prompted Congress to pass the FCRA. Errors in reports provided by ChoicePoint and similar companies can find their way into other databases, resulting in the potential for improper arrest and even imprisonment. People have been wrongly arrested and jailed due to errors in law enforcement databases.[15] Since information often circulates between law enforcement records and commercial databases, erroneous information in a database such as AutoTrackXP can make its way into a series of other databases, with profoundly harmful effects on people's lives. For example, consider the following incident:

> [A] Maryland woman wrongly arrested for a burglary was not cleared from the state's criminal databases. Her name and SSN also migrated to a Baltimore County database relating to child protective services cases. She was fired from her job as a substitute teacher, and only after she could establish that the information was in error was she rehired. When she later left that job to run a day care center for the U.S. military, she was subject to questioning about the erroneous arrest. Later on, when employed at as a child care director at a YMCA, she was terminated when her arrest record surfaced in a background clearance check. Since she could not have the error expunged in sufficient time, the job was given to another person. Only after several years was the error finally cleared from the public records.[16]

Finally, we note that under the self-regulatory scheme erected by the now defunct Individual Reference Services Group, commercial data brokers choose who is eligible to buy personal information. This is a subtle but important deviation from the Fair Credit Reporting Act's approach, which tends to approve record disclosure based on the use of the information, rather than the identity of the purchaser. The importance of this difference becomes clear when it is understood that private investigators, major buyers of personal information, are not licensed in all fifty states, and in some states that require licensure, it is a pro forma process.[17] As a result, ChoicePoint and other information brokers can create ties with marginal businesses or private investigators with dubious backgrounds. Based on their status of being a private investigator, a paralegal, or a law enforcement agent, ChoicePoint's customers can pull information on almost anyone without having to declare their legal justification or entitlement to the data.

We encourage the Commission to examine access to commercial data broker information in light of the Amy Boyer case, where a Florida information broker sold data to the man who stalked and killed Amy Boyer.[18] If the sale of Ms. Boyer's Social Security Number and other information to a complete stranger were conditioned upon one of the FCRA's permissible uses of data, perhaps she would be alive today. The FCRA's reasonable limitations on the use of data, if applied to this sector of data brokers, could protect individuals from unwarranted access to and sale of personal information.

Again, we urge the Commission to engage in a serious inquiry on the status of data brokers' products. We believe that some of these products may be "consumer reports" for purposes of the FCRA, thus subjecting both the seller and the buyer to regulation under the Act. We also think it incumbent upon the Commission to analyze whether the sale of these new data products circumvents the FCRA, giving businesses, private investigators, and law enforcement access to data that previously had been subjected to Fair Information Practices.

We look forward to hearing from you on this matter, and please contact us if we can provide more information.

Sincerely,

Chris Jay Hoofnagle
Associate Director
Electronic Privacy Information Center

Daniel J. Solove*
Associate Professor
George Washington University Law School

*Title and affiliation listed for identification purposes only.

---

[1] See EPIC ChoicePoint Page, available at http://www.epic.org/privacy/choicepoint/. For more information about ChoicePoint, *see* Robert O'Harrow, No Place to Hide: Behind the Scenes of Our Emerging Surveillance Society (Free Press Jan. 2005).

[2] Duane D. Stanford, *All our lives are on file for sale*, Atlanta J. Const., Mar. 21, 2004 at 1A.

[3] *Id.*

[4] Daniel J. Solove, The Digital Person. Technology and Privacy in the Information Age 169 (NYU 2004).

[5] Robert Ellis Smith, Ben Franklin's Web Site, Privacy and Security from Plymouth Rock to the Internet 316-318 (Privacy Journal 2000).

[6] *Id.*

[7]Solove, Digital Person, 170.

[8] See also, Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C.J. Int'l L. & Com. Reg. 595 (Summer 2004).

[9] ChoicePoint, AutoTrackXP and ChoicePoint Online, http://www.choicepoint.com/industry/retail/public_cbi_1.html.

[10] ChoicePoint, Customer Identification Programs, http://www.choicepoint.com/business/financial/patriotact.html.

[11] *See* Appendix.

[12] 245 F.3d 809 (D.C. Cir. 2001), *cert. denied*, 536 U.S. 915 (2002); *Bakker v. McKinnon*, 152 F.3d 1007, 1012 (8th Cir. 1998) ("even if report is used or expected to be used for non-consumer purpose, it may still fall within definition of consumer report if it contains information that was originally collected by consumer reporting agency with expectation that it would be used for consumer purpose"); *Ippolito v. WNS, Inc.*, 864 F.2d 440, 453 (7th Cir. 1988) ("even if a report is used or expected to be used for a non-consumer purpose, it may still fall within the definition of a consumer report if it contains information that was originally collected by a consumer reporting agency with the expectation that it would be used for a consumer purpose"); *Rice v Montgomery Ward & Co.*, 450 F. Supp. 668 (M.D.N.C. 1978).

[13] Law enforcement access to "credit headers" or information from a full report is subject to substantive and procedural protections. See, *e.g.*, 15 U.S.C. § 1681b(a)(1).

[14] Memorandum from Office of the General Counsel, National Security Law Unit, FBI, to National Security, FBI (Sept. 17, 2001) (document obtained from the FBI), available at http://epic.org/privacy/choicepoint/cpfbia.pdf.

[15] Solove, Digital Person, 109-110.

[16]Solove, Digital Person, *supra*, at 46-47 (citing Eugene L. Meyer, "Md. Woman Caught in Wrong Net; Data Errors Link Her to Probes, Cost 3 Jobs," Wash. Post, Dec. 15, 1997, at C1). Another example includes the case of Scott Lewis, an innocent person who was labeled a criminal because of an administrative error. After he was able to fix the error, information brokers continued to circulate erroneous conviction information. Beth Givens, Identity Theft: The Growing Problem of Wrongful Criminal Records, Jun. 1, 2000, http://www.privacyrights.org/ar/wcr.htm.

[17] "Some States have few requirements [for private investigator licensure], and 6 States—Alabama, Alaska, Colorado, Idaho, Mississippi, and South Dakota—have no statewide licensing requirements while others have stringent regulations." U.S. Department of Labor, Bureau of Justice Statistics, Private Detectives and Investigators, Mar. 21, 2004, available at http://www.bls.gov/oco/ocos157.htm.

[18] *Remsburg v. Docusearch, Inc.* 149 N.H. 148 (N.H. 2003). More information about the Amy Boyer case is online at http://epic.org/privacy/boyer/.

Appendix

I. ChoicePoint

ChoicePoint,[1] one of the largest data aggregation companies, became independent from Equifax, a leading U.S. credit rating agency, in 1997.[2] ChoicePoint has bought more than 40 companies and competitors, and obtains 40,000 new public records daily to insert into its database of more than 19 billion records.[3] Its business and government services division offers through its AutoTrackXP product identity verification, property records, bankruptcy records, licenses, liens, judgments, and other records to local, state and federal law enforcement,[4] including the Drug Enforcement Administration and the Federal Bureau of Investigation.[5] It also advertises the AutoTrackXP product as a solution for financial services anti-fraud and anti-money laundering compliance.[6]

ChoicePoint's roots are in information services to the insurance sector. The company stated in its initial Securities and Exchange Commission filing that:

> ChoicePoint's operations have historically consisted of database information and inspection and investigative services supplied primarily to the insurance industry. ChoicePoint believes it can enhance future growth and profitability by offering a broader range of risk assessment services, fraud management information and technology solutions to clients outside of the insurance industry. Although Equifax believes that significant growth opportunities exist for ChoicePoint's products and services, it anticipates that marketing and promotion of these services will be necessary. The public perceives, however, that credit reporting services and the more privacy sensitive services offered by ChoicePoint should not be available from a single provider.[7]

Since its spinoff from Equifax, ChoicePoint has acquired a number of information collection and processing companies.[8] As a provider of personal information to the insurance sector, from its inception, ChoicePoint's activities have been subject to the FCRA.[9]

II. ChoicePoint's FCRA Business Activities

ChoicePoint sells a number of information products in the employment screening, tenant screening, and personal insurance areas. Many of these information products are FCRA databases and require both ChoicePoint and the company's clients to comply with the Act. This section summarizes ChoicePoint's FCRA employment screening, tenant screening, and personal insurance products. The next section turns to AutoTrackXP and "Customer Identification Programs," ChoicePoint's non-FCRA data products that are similar to the company's FCRA employment, tenant, and insurance screening products.

A. ChoicePoint's "CP Online" Product

On its website, ChoicePoint markets a pre-employment screening service named "CP Online." The company claims that that product is FCRA-compliant:

> ChoicePoint Online is a comprehensive Web-based screening interface designed to help employers meet their pre-employment screening needs regarding background verification and drug testing administration. ChoicePoint Online is FCRA-compliant and offers easy-to-use data entry screens, duplicate request notification and alerts for possible criminal records. Using ChoicePoint Online's interactive ordering system, flexible reporting options, process monitoring and online billing, users can gain valuable information to help make better decisions and employ more efficient hiring practices.[10]
>
> ...* FCRA Summary of Consumer Rights attached to all decisional reports

ChoicePoint lists the following databases as being available for pre-employment search through the CPOnline product:

Stanton® Assessments
State Law Reference Library
National Criminal File
Driver Qualification File
Criminal Background Checks
Identity Verification
MVRs
Credit History
Employment Verification
Education Verification
Military History
Worker's Compensation
License, Credentials and Certification Verification
Business or Personal Reference Verification[11]

B. ChoicePoint's "National Criminal File" Product

On its website, ChoicePoint markets a pre-employment screening service named "National Criminal File." The company claims that that product is FCRA-compliant:

> ChoicePoint National Criminal File is a comprehensive search of multiple criminal record sources, including fugitive file, state and county criminal record repositories, ChoicePoint proprietary criminal record information, prison, parole and release files from state Department of Corrections, Administrative Office of Courts and other state agencies.
>
> Key Features & Benefits

* Access to more than 100 million criminal conviction records across all 50 states

* National reach at an economically feasible price

* FCRA Compliant...[12]

C. ChoicePoint's "Resident Data" Screening Product

On its website, ChoicePoint markets a tenant screening service named "Resident Data." The company claims that that product is FCRA-compliant:

> Resident Data is an industry leader in apartment resident screening and debt collections. Our mission is to maximize customer profitability by managing resident profile risk, collecting maximum payments from residents who default, and creating an environment of resident accountability.
>
> Our integrated screening, skip watch and collections solutions enable apartment owners and managers to better direct their properties by providing flexible solutions that adapt to the individual needs of the community.
>
> Resident Data helps reduce liability by improving compliance with FCRA and Fair Housing requirements.[13]

ChoicePoint lists the following data elements as being available for tenant screening through the "Resident Data" product:

> Access to Criminal, Registered Sex Offender and Eviction Databases.
>
> [...]
>
> * Online access to more than 77 million criminal records, State and county criminal record repositories.
>
> * 39 States of Registered Sex Offender Records.
>
> * FBI Terrorism Watch List - Including FBI Most Wanted list and FBI Terrorist database list.
>
> * Proprietary records from ChoicePoint's other screening business results.
>
> * Offender and offense descriptions.
>
> [...]
>
> National Eviction Search
>
> ChoicePoint has more than 10 million current records from 45 states. The data includes initial filings, dispossessory warrants and property actions. Resident Data searches every state where the applicant has a prior address as part of its search, not just the state where the applicant is applying.
>
> [...]

Unit Application Analysis

For roommates or multiple applicants, the Resident Data system evaluates all applicants on a per-unit basis and presents a recommendation for the group. Individual screening outcomes are also noted on the report.

[...]

Occupant Processing

Resident Data also offers occupant screening to protect your property from potential problem residents who are not financially responsible for a lease. We can provide legally compliant screening services on potential occupants without initiating a credit check.

[...]

Maximum Evaluation of the Credit Report

The Resident Data review of the credit report includes fraud alerts, SafeScan warnings for possible Social Security Number problems, landlord or utility debt, address matching and full review of payment performance.[14]

D. ChoicePoint's CLUE Personal Auto Product

On its website, ChoicePoint markets a personal insurance screening service named "CLUE Personal Auto:"

> C.L.U.E. (Comprehensive Loss Underwriting Exchange) is a claim history information exchange that enables insurance companies to access prior claim information in the underwriting and rating process. C.L.U.E. Personal Auto reports contain up to five years of personal automobile claims matching the search criteria submitted by the inquiring insurance company. Data provided in C.L.U.E. reports includes policy information such as name, date of birth and policy number; claim information such as date of loss, type of loss and amounts paid; and vehicle information.
>
> More than 95 percent of insurers writing automobile coverage provide claims data to the C.L.U.E. Personal Auto database. By providing immediate interactive information, C.L.U.E. Personal Auto helps insurers and agents make immediate business decisions.[15]

The data elements in the CLUE Personal Auto report include: names of other drivers possible associated with the person applying for insurance, claims information, vehicle descriptions, and vehicle ownership. [16]

E. ChoicePoint's "Motor Vehicle Records" Product

On its website, ChoicePoint markets a personal insurance screening service named "Motor Vehicle Records:"

> ChoicePoint provides driving records, including standard violation codes, from all 50 states and three Canadian provinces in an easy-to-read standardized format. Online access to driving records is available for 40 states and two provinces, and ChoicePoint continues to add to the list of states with online access.[17]

The data elements in the Motor Vehicle Records report include: contact information, driver license

number, physical descriptions of drivers, and additional drivers that may be associated with the data subject.[18]

F. ChoicePoint's "National Credit File" Product

On its website, ChoicePoint markets a product named "National Credit File:"

> ChoicePoint's National Credit File provides insurance carriers with online consumer credit reports obtained from the three major credit bureaus. Carriers then consider the financial history of the applicant and assess the applicant's risk for quoting, underwriting and renewal purposes.[19]

The data elements in the National Credit File report include: contact information, bankruptcies, public records, liens, collection items, employment information, and tradelines.[20]

III. ChoicePoint's Apparent Non-FCRA Products

In addition to the FCRA products described above, ChoicePoint markets two additional, popular data products to law enforcement, financial services companies, private investigators, law firms, and other businesses. These products are known as "AutoTrackXP" and "Customer Identification Programs."

A. ChoicePoint's "AutoTrackXP" Product

On its website, ChoicePoint markets "AutoTrackXP", which is described as:

> AutoTrackXP and ChoicePoint Online provide Internet access to more than 17 billion current and historical records on individuals and businesses, and allow users to browse through those records instantly. With as little information as a name or Social Security number, both products cross-reference public and proprietary records including identity verification information, relatives and associates, corporate information, real property records and deed transfers. In addition, access is available to a staff of field researchers who perform county, state and federal courthouse searches.[21]

The advertised data elements in AutoTrackXP include:

> Discovery PLUS!™ - through ChoicePoint Online
>
> * Compiles a comprehensive report on an individual including current and previous addresses, relatives, assets, corporate involvement and derogatory information.
>
> * Returns list where no matches were found.
>
> * Also available Discovery PLUS! with Vehicle Identification Number.
>
> Info:PROBE™ - through ChoicePoint Online
>
> * *Checks millions* of records *simultaneously* and provides a "shopping list" of databases, which contains records that match the search criteria. A client can then choose which databases to view.
>
> [...]

National Comprehensive Report – through AutoTrackXP

* Searches national and state databases for a summary of assets, driver licenses, professional licenses, real property, vehicles, and more.

* Each report offers the ability to add associates to the report, which include relatives, others linked to the same addresses as the subject and neighbors.[22]

A sample AutoTrackXP report on the ChoicePoint web site shows that it contains Social Security Numbers; driver license numbers; address history; phone numbers; property ownership and transfer records; vehicle, boat, and plane registrations; UCC filings; financial information such as bankruptcies, liens, and judgments; professional licenses; business affiliations; "other people who have used the same address of the subject," "possible licensed drivers at the subject's address," and information about the data subject's relatives and neighbors.[23] The AutoTrackXP report is very similar in content to a standard credit report issued by one of the "big three" credit reporting agencies.

However, there is no indication that AutoTrackXP is sold within the FCRA's procedural and substantive safeguards. ChoicePoint seems to have treated the data product outside the FCRA and subject only to the now-defunct Individual Reference Service Group self-regulatory principles. This means that anyone with a ChoicePoint account can buy an AutoTrackXP account.

It appears that both ChoicePoint and federal law enforcement share the view that AutoTrackXP is outside the FCRA's protections. In a document obtained by EPIC under the Freedom of Information Act from the Federal Bureau of Investigation, the agency concluded that ChoicePoint's products are not covered by the FCRA: "In this instance, none of the information which the FBI would seek to review has been collected by ChoicePoint for any of the [FCRA] purposes."[24]

B. ChoicePoint's Customer Identification Programs

On its website, ChoicePoint offers "Customer Identification Programs," described as a PATRIOT Act compliance mechanism with many data elements similar to AutoTrackXP:

Identification Solutions

Basic identification solutions ensure that name, address, date of birth and Social Security numbers match. This includes a check against required government sanctions lists. Enhanced due diligence solutions include telephone numbers, historical information, criminal records, key relationships, international information and comprehensive individual and business reports.

[...]

You'll benefit from our unique offerings, including:

* Access to more than 17 billion public records and three major credit bureaus.

* An extensive proprietary identity database.

* National real property information.

* Nationwide corporate and business information.

* A vast database of drivers' license data and motor vehicle records.

* National criminal history database.

* Access to the Office of Foreign Asset Control and other government sanctions and enforcement actions, including international information.[25]

---

[1] See EPIC ChoicePoint Page, available at http://www.epic.org/privacy/choicepoint/. For more information about ChoicePoint, *see* Robert O'Harrow, No Place to Hide: Behind the Scenes of Our Emerging Surveillance Society (Free Press Jan. 2005).

[2] Duane D. Stanford, *All our lives are on file for sale*, Atlanta J. Const., Mar. 21, 2004 at 1A.

[3] *Id.*

[4]ChoicePoint, AutoTrackXP and ChoicePoint Online, http://www.choicepoint.com/industry/government/public_le_1.html (accessed Oct. 25, 2004).

[5] Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C.J. Int'l L. & Com. Reg. 595 (Summer 2004).

[6]ChoicePoint, All Financial Solutions, http://www.choicepoint.com/business/financial/allfinan.html (accessed Oct. 25, 2004).

[7] ChoicePoint Corporation, SEC Registration of securities [Section 12(b)], Jun. 9, 1997.

[8] These include: National Data Retrieval, Inc., a provider of public records information; List Source, Inc., d/b/a Kramer Lead Marketing Group, a marketing company in the life and health insurance and financial services markets; Mortgage Asset Research Institute, Inc., a mortgage fraud monitoring company; Identico Systems, LLC, a customer identity verification company; Templar Corporation; insuranceDecisions, Inc., an insurance industry claims administration company; Bridger Systems, Inc., a USA PATRIOT Act compliance company; CITI NETWORK, Inc. d/b/a Applicant Screening and Processing, a tenant screening company; TML Information Services, Inc., a provider of motor vehicle reports. ChoicePoint Corporation, SEC Form 10-K, Mar. 5, 2004. With respect to TML Information Service, ChoicePoint purchased "certain assets" of the company. Drug Free, Inc., a drug testing company; National Drug Testing, Inc., a drug testing company; Application Profiles, Inc., a background check company; Informus Corporation; a company enabling ChoicePoint to offer products online; Tyler-McLennon, Inc., a background screening company; ChoicePoint Direct Inc., formerly known as Customer Development Corporation, a database marketing company; EquiSearch Services, Inc.; DATEQ Information Network, Inc., an insurance underwriting services company; Washington Document Service, Inc., a court record retrieval service; DataTracks Technology, Inc., a public record information company; DataMart, Inc., a database software company; Statewide Data Services, Inc; NSA Resources, Inc., a drug testing company; DBT Online, Inc., a public record services provider; RRS Police Records Management, Inc., a provider of police reports and related services; VIS'N Service Corporation; Cat Data Group, LLC; Drug Free Consortium, a drug testing company; BTi Employee Screening Services, Inc., an employee pre-screening services company; ABI Consulting Inc., a drug screening company; Insurity Solutions, Inc., an insurance rating company; National Medical Review Offices, Inc.; Bode Technology Group, Inc., a DNA identification company; Marketing Information & Technology, Inc., a direct marketing company; Pinkerton's, Inc., a preemployment screening company; Total eData Corporation, an e-mail database company; L&S Report Service, Inc., a provider of police records; Resident Data, Inc., a residential screening services provider; Vital Chek Network, Inc., a provider of vital records; Accident Report Services, Inc., a provider of police records. ChoicePoint Corporation, SEC Form 10-K, Mar. 26, 2003.

Programming Resources Company, insurance software company; Professional Test Administrators, Inc., a drug testing company; CDB Infotek, a seller of public records; Medical Information Network, LLC, an online physician verification service. ChoicePoint Corporation, SEC Form 10-K, Feb. 16, 2001. Rapsheets.com, an online provider of criminal records data. *ChoicePoint acquired Rapsheets, a provider of online criminal records data*, Information Today, Inc., Sept. 1, 2004.

[9] "Certain data and services provided by ChoicePoint are subject to regulation by the Federal Trade Commission under the Federal Fair Credit Reporting Act, and to a lesser extent, by various other federal, state and local regulatory authorities. Compliance with existing federal, state and local laws and regulations has not had, and is not anticipated to have, a material adverse effect on the results of operations or financial condition of ChoicePoint. Nonetheless, federal, state and local regulations in the United States designed to protect the public from the misutilization of personal information in the marketplace may increasingly affect the operations of ChoicePoint, which could result in substantial regulatory compliance and litigation expense, adverse publicity and a loss of revenue. *Id.*

[10]ChoicePoint, CP Online, http://www.choicepoint.com/business/pre_employ/pre_employ_2.html.

[11] *Id.* ChoicePoint offers similar information for employment purposes under the product names "ScreenNow," "Screening Network," and "Secure Point."

[12]ChoicePoint, National Criminal File, http://www.choicepoint.com/business/pre_employ/pre_employ_4_1.html. In November 2001, ChoicePoint introduced the National Criminal File database, one that then contained, "more than 20 million conviction records from jurisdictions around the country." David J. Cook, then ChoicePoint vice president, was quoted saying that the National Criminal File was created for employment screening purposes: "We have two large clients who want to run a large national criminal search on every one of their employees." Lisa Guernsey, What Did You DO Before the War?, New York Times, Nov. 22, 2001.

[13] ChoicePoint, Resident Data, http://www.choicepoint.com/business/public/cbi_5.html.

[14] ChoicePoint, Screening Unique Services and Features, http://www.residentdata.com/services/screening_features.asp.

[15] ChoicePoint, CLUE Personal Auto, http://www.choicepoint.com/business/pc_ins/us_1.html. ChoicePoint markets a similar product for other property as "CLUE Personal Property."

[16] ChoicePoint, CLUE Personal Auto Report, http://www.choicepoint.com/sample_rpts/CLUEAutoUnderwriter.pdf.

[17] ChoicePoint, Motor Vehicle Records, http://www.choicepoint.com/business/pc_ins/us_5.html.

[18] ChoicePoint, Motor Vehicle Records Report, http://www.choicepoint.com/sample_rpts/mvrhowtoread.pdf.

[19] ChoicePoint, National Credit File, http://www.choicepoint.com/business/pc_ins/us_9.html.

[20] ChoicePoint, National Credit File Report, http://www.choicepoint.com/sample_rpts/NCF.pdf.

[21] ChoicePoint, AutoTrackXP and ChoicePoint Online, http://www.choicepoint.com/industry/retail/public_cbi_1.html

[22] *Id.*

[23] ChoicePoint, AutoTrackXP Report, http://www.choicepoint.com/sample_rpts/AutoTrackXP.pdf.

[24] Memorandum from Office of the General Counsel, National Security Law Unit, FBI, to National Security, FBI (Sept. 17, 2001) (document obtained from the FBI), available at http://epic.org/privacy/choicepoint/cpfbia.pdf

[25] ChoicePoint, Customer Identification Programs, http://www.choicepoint.com/business/financial/patriotact.html.

Attachment B

"ChoicePoint—An Ignoble Corporate History,"
Privacy Journal, March 2005,
Volume 31, Number 5

Privacy Journal
AN INDEPENDENT MONTHLY ON PRIVACY IN A COMPUTER AGE
PO Box 28577
Providence RI 02908

March 2005, Volume 31, Number 5

Identity Theft Happens Mainly in America

Identity theft is largely an American phenomenon. There are reasons for that. Other nations don't rely on an identifying number – like a number to keep track of pension accounts or government benefits – for other purposes, like identifying consumers in credit reports.

Since the early 1990s credit bureaus have been collecting Social Security numbers and relying on the numbers to confirm a match when a lender requests a credit report on an applicant. By the same token, credit bureaus usually ask a consumer who wants to see his or her own credit report, as permitted by law, to provide a Social Security number to confirm his or her identity. The Federal Trade Commission, which regulates credit bureaus, actually encouraged this in the 1990s.

Strangers can get Social Security numbers from payroll records or buy them from Internet sites.

Thus, it's not hard to see why theft of identity is easy in the U.S. A stranger need only get a Social Security number to match a name and then ask a credit bureau to provide a copy of "his"

(Continued on page four)

ChoicePoint – An Ignoble Corporate History

1974 Two and a half years after the Fair Credit Reporting Act is enacted, the Federal Trade Commission accuses Retail Credit Co. of violating it. Its consumer investigative operation misrepresents itself to consumers and to sources, continues to report obsolete adverse information on consumers, pressures its staff to produce negative information, hassles consumers who seek access to their own files, and fails to reinvestigate the accuracy of information challenged by consumers. All of this violates the FCRA.

1976 The credit-bureau side of Retail Credit Co.'s business also faces a cease-and-desist order by the FTC and a 1971 federal court anti-trust injunction, as well as consumer lawsuits. As a consequence, the company hires a consultant, who recommends a name change to **Equifax**. The consultant says that the new name connotes fairness and factual accuracy.

1980 The consumer investigative side of Equifax, which compiles narrative reports on consumers for employers and insurance companies, now controls more than 75 percent of the market.

1982 After a federal court upheld the FTC charges of FCRA violations and ordered Equifax to comply with a cease-and-desist order, the FTC finds that instructions to employees have not changed. It orders the company to circulate the court's order among its employees.

1989 Equifax claims great success with its Comprehensive Loss Underwriting Exchange (CLUE), which indexes millions of past auto- and property-insurance claims so that 280 insurance companies may query the system when a person applies for coverage. There is no way for an individual, in spite of the Fair Credit Reporting Act, to check the accuracy of a CLUE record.

1991 One of several consumer lawsuits against the company finds that Equifax had not complied with the 1982 FTC directive. "Court order? What order?" said one employee questioned in a lawsuit.

1992 The New York City Department of Consumer Affairs condemns CLUE, saying there is no way to determine the accuracy of its vast files. The Data Protection Registrar in the United Kingdom questions its fairness.

1995 The Federal Trade Commission ***again*** cites the consumer investigative arm of Equifax for violations, including failure to reinvestigate complaints of inaccuracy and ignoring consumers' documenta-

(Continued on page three)

ISSN 0145-7659

ChoicePoint – An Ignoble Corporate History

(Continued from page one)

inaccuracies. Equifax did not challenge the FTC findings. Under a settlement with the FTC, the company is ordered to discontinue these violations and make periodic reports to the FTC showing its progress improving its accuracy rate. Under the order, Equifax is to cease providing credit reports to a discredited information broker in California named CDB Infotek.

1996 CDB Infotek advertises in e-mails that it will sell information at the top of a credit report – "header information" like Social Security number, date of birth, phone number, and "a/k/a's." It offers access to Social Security account information, the change-of-address lists of the Postal Service, lists of registered voters (in violation of state laws in California and elsewhere), and data on personal assets. It sells criminal and civil-court records, demographics of a target's closest neighbors, California driving records, employment reports, and much more. In 1992 CDB had been cited by the FTC for major violations of the credit-reporting law. CDB did not challenge the FTC findings.

1996 Seven months after CDB's ad appears, Equifax purchases 70 percent of CDB Infotek and folds it into its Insurance and Special Services unit.

1997 An Equifax shareholder, in a formal demand for due diligence by the parent company, cites "law-breaking, fraud and unethical conduct" by CDB.

1997 Alarmed by its negative reputation with the acquisition of Infotek, its FTC cease-and-desist orders, and consumer lawsuits, Equifax spins off its Insurance and Special Services unit and calls it ChoicePoint. The new unit absorbs CDB's files. It also takes on driver and motor-vehicle, divorce, marriage, corporate, property-ownership, and other data of questionable reliability owned by a company called Database Technologies, Inc., in Boca Raton, Fla. ChoicePoint's independence is questionable. The chair of Equifax, Inc., during the 1990s is chair of the executive committee of ChoicePoint's board of directors. ChoicePoint's new president was executive vice president of Equifax.

1998 ChoicePoint jettisons the rogue founder of CDB Infotek, former private investigator Rick Rozar, who says that he will use his $95 million in capital gains to work with organizations seeking to locate missing children. He donates $100,000 to the Republican National Committee. In October, Rozar, 44, dies in a fall from the roof of his house. He was removing a satellite TV dish.

1999 The FBI and Drug Enforcement Administration suspend contracts with Database Technologies (DBT Online), because of evidence that the company's founder, Hank Asher, had ties to drug smuggling from the Bahamas in the 1980s. (Asher later with a company called Seisint in Boca Raton develops anti-terror software called Matrix, which purports to mine hundreds of private and public databases with personal information. In 2003, with the help of Florida Gov. Jeb Bush, Asher will provide a show-and-tell in the White House for top Bush Administration officials and they are impressed.)

2000 Despite its record, federal and state agencies continue to enter into contracts with ChoicePoint. But

PRIVACY JOURNAL
Founded in 1974
Robert Ellis Smith
Publisher
401/274-7861 fax 401/274-4747
orders@privacyjournal.net
www.privacyjournal.net

PRIVACY JOURNAL is published monthly, reporting on legislation, legal trends, new technology, and public attitudes affecting the confidentiality of personal information. $125 a year, $165 overseas. PRIVACY JOURNAL is available by postal mail, or by electronic mail, or in selected news and bookstores in the U.S. Back issues are available by mail in hard copy or in electronic form, by e-mail, or at our Web site. MasterCard, Visa, American Express, and Discover credit cards are accepted for payment. CIRCULATION MANAGER: Shauna Van Dongen.

the Pennsylvania Department of Transportation terminates a 10-year agreement that granted ChoicePoint access to drivers' records and specified that the data could not be transmitted via the Internet. The company violated that provision. It was advertising Pennsylvania driver records on-line and selling them to persons not entitled to them under the agreement with the state. ChoicePoint pays a $1.4 million fine.

2000 Two of ChoicePoint's senior managers donate $4,000 to a Republican fund launched by Sen. Richard Shelby, R-Ala., to support GOP candidates. Shelby is chair of the Senate committee overseeing the Fair Credit Reporting Act.

2000 ChoicePoint's stock increases by 50 percent in value; its earning surpass $400 million. It has contracts with the IRS, Health Care Financing Administration, the Secret Service, and the City of New York. It makes its database available to the federally funded National Center for Missing and Exploited Children, Rick Rozar's favored non-profit association.

2000 The Florida Secretary of State hires Database Technologies, now a wholly owned subsidiary of ChoicePoint, to come up with the names of felons in Florida, because felons are forbidden by law from voting in Florida. But the lists include the names of many eligible voters. As a result, nearly 2000 Florida voters, most of them African-Americans, are wrongfully disqualified from voting and 5600 people tagged as likely felons ended up voting anyway.

2001 After just two months in office, the Bush Administration suspends an eleventh-hour Clinton Administration regulation that would deny federal contracts to companies that appear to have violated federal laws repeatedly.

2002 The company vigorously fights for "homeland security" funds from federal and state agencies. It seeks to be the provider of personal information for filtering airline passengers before they may board an airplane without further scrutiny. "ChoicePoint's core competency is verifying and authenticating individuals and their credentials," says Chairman and CEO Derek V. Smith.

2002 ChoicePoint hires a friend of George W. Bush, James Langdon, who raised more than $100,000 for Bush's campaign in 2000, as its lobbyist in Washington. In a few months the company secures an $11 million contract with the U.S. Department of Justice to provide access to the company databases.

2005 Because of California's security breach law, the company is forced to reveal that thieves posing as legitimate businesses were able to access profiles that include Social Security numbers, credit histories, criminal records and other sensitive personal information. The company discovered the breach in October 2004. Negative publicity forces the company to make disclosures of the breach to 100,000 persons nationwide. The number of victims may reach 500,000. Some victims have already experienced symptoms of identity theft like changes of address by strangers.

2005 A U.S. Senate committee announces hearings on information brokers, focusing on ChoicePoint.

ID Theft (Continued from page one)

credit report. Or the stranger can apply for credit under the target's name and use the victim's Social Security number to "authenticate" identity. Sometimes the stranger will change the address on the victim's credit account (and use the stolen SSN to "authenticate" identity. Credit bureaus are not required to send a notice to a consumer before activating a change of address, and so they don't do so.

This can't happen, of course, if credit bureaus discontinue using SSNs as a match. Credit bureaus in Europe and Australia do not do so, and so identity theft is virtually non-existent. "Outside the U.S.A., my impression is that ***identity theft*** is very uncommon (although the U.K. authorities carry on as though there were some)," Roger Clarke, long-standing privacy expert in Australia, told **PRIVACY JOURNAL**. "There have been only half-a-dozen reported cases in Australia over a period of quite some years."

Clarke, of Xamax Consultancy and Australian National University, monitors identity theft and identity fraud worldwide. In fact, he distinguishes between ***identity theft*** ("the adoption of an established identity by a second person, polluting the records of that identity with various organizations, typically retailers, finance companies and hence credit bureaus"), and ***identity fraud*** (the use of manufactured false IDs for immigration, fraud, money laundering, and possibly terrorism).

"There is a very high level of ***identity fraud***

Attachment C

ChoicePoint, "Response to Customer Fraud Litigation,"
February 23, 2005, from the ChoicePoint website,
http://www.choicepoint.com/news/statement_0205_1.html

NEWS CENTER

News Features

- > ChoicePoint Books
- > Print Articles
- > Online Articles
- > Videos
- > Acknowledgements and Awards

Response to Customer Fraud Litigation

02/23/2005

Like most U.S. businesses, we respond to the specifics of litigation in court proceedings, not the media.

The reality is, ChoicePoint is going to extraordinary lengths to assist people whose identities may have been compromised by the crimes committed against the company and will continue to do so. We have gone far beyond what the California law requires by voluntarily notifying individuals nationwide who may be impacted, by providing free credit reports, and credit monitoring for a year, and by setting up a dedicated support center to help consumers who receive a notification letter.

> How to Check your Credit Report

> Click here to view the state by-state distribution of consumer notices

Additional Information

ChoicePoint is actively engaged with local and federal law enforcement agencies in the continuing investigation of a fraud committed against us, through which a small number of very organized criminals posing as legitimate companies gained access to personal information about consumers. **This incident was not a breach of ChoicePoint's network or a "hacking" incident, and did not involve any of ChoicePoint's customer information.**

We want you to know we take this criminal activity seriously and are aggressively addressing it.

In addition to assisting law enforcement officials, we are taking voluntary actions at company expense to help affected consumers protect their identity. We want to tell you what we believe occurred and what information was released. We also want to provide you with details about what we are doing to inform and assist consumers that may be affected, and what we are doing to ensure we have reduced the possibility of future unauthorized access to personal information by criminals.

What we know about the crime:
top

In October 2004, we detected possible signs of fraudulent activities in several small business accounts based in the Los Angeles area. We alerted the Los Angeles County Sheriff's Department and they subsequently confirmed our suspicions and began an investigation.

These criminals were able to pass our customer authentication due diligence processes by using stolen identities to create and

produce the documents needed to appear legitimate. As small business customers of ChoicePoint, these fraudsters accessed products that contained basic telephone directory-type data (name and address information) as well as a combination of Social Security numbers and/or driver's license numbers and, at times, abbreviated credit reports. They were also able to obtain other public record information including, but not limited to bankruptcies, liens, and judgments; professional licenses; and real property data.

In late January, we were cleared to begin informing the consumers whose personal information may have been accessed. We then began production of notification letters to approximately 35,000 potentially effected California consumers. Mailing to these consumers was completed last week.

After the start of the California notification process, investigators informed us they believed consumers outside of California may also have been impacted. We immediately began the process of preparing and issuing approximately 110,000 additional letters to consumers in other states that may have also been impacted. We expect to complete these mailings by the end of the week.

We do not know how many of these approximately 145,000 consumers may be actual victims of identity theft but we have been informed by law enforcement officials that they have identified and directly notified approximately 750 consumers nationwide that some part of their identity information has been compromised.

Additionally, a Nigerian citizen last week pled no contest in California state court and was sentenced to 16 months in prison in connection with this incident.

What we are doing to inform and protect Consumers:
top

Our primary focus remains assisting those consumers whose confidential data may have been fraudulently obtained by these criminals.

We expect that all of the approximately 145,000 notices will be mailed by the end of the week.

We have set up a special toll-free number for use by consumers who receive these notices. Our notices urge consumers to check their credit reports for suspicious activity and provide information on how to obtain their credit reports from each of the three credit bureaus via phone, mail, or web.

To be of further assistance we have purchased tri-bureau credit reports and a one-year credit monitoring service at our expense for each individual. Our notification letters also inform consumers how to obtain these services, free of cost to them, via phone or web.

What we are doing to minimize the likelihood of future occurrences:
top

Financial fraud and identity theft are pervasive problems in the economy. While ChoicePoint offers a wide range of tools to help detect fraud, no one - including us - is immune from it.

ChoicePoint has acted quickly to address the circumstances that led to the unauthorized access. We are continually updating our customer credentialing and enrollment processes, on-going

account monitoring analytics and our periodic customer auditing programs to help ensure the integrity of our systems and the information they contain.

We are taking the following additional steps:

- We have asked Mr. Robert McConnell, to serve as our liaison to law enforcement officials and to provide insight for developing additional protections to guard against future fraud. Mr. McConnell, is a retired 28 year veteran of the United States Secret Service. During his last five years with the Secret Service, Mr. McConnell supervised the interagency task force responsible for the investigation of Nigerian Organized Crime.

- We are presently going through a rigorous re-credentialing of broad categories of customer accounts, including small business customers. We have made, and will continue to make, product changes that limit the information these customers are able to obtain before, and after, this re-credentialing is completed. These changes include masking or truncating sensitive personal identifier information (including social security numbers and driver's license numbers). Most of this fraud occurred in our small busine. public record product segment, representing less han five percent of our annual revenue. All of these customers will be impacted by our data restrictions and re-credentialing efforts.

We have always restricted and controlled access to personal data. What's prompting us to go even further is we now know that organized crime may have hijacked our legitimate data uses. We believe an effective way to protect sensitive data from these highly organized criminals is to re-credential our customers and remove information in those segments where organized crime fraud is likely to occur. We hope others in our industry will do the same.

This unfortunate and regrettable criminal act has instilled in us a determination to lead this fight within the broader information industry as well. We have already begun sharing our experiences, observations and ideas with several of the other major corporations in our industry, and we will seek to lead an industry-wide initiative to develop, adopt, and deploy new measures that will identify and halt identity theft and fraud.

As part of an industry-wide initiative, ChoicePoint is also renewing its call for a national discussion on how to ensure information is used responsibly to ensure the positive benefits of information use are preserved and the illegal uses of data are severely punished. For nearly two years, ChoicePoint has called for a broad national discussion about how to protect personal privacy and society's right to know. We specifically support:

- Independent oversight and increased accountability of data users and providers to help increase consumer confidence

- Increased penalties for the intentional misuse of personal information by businesses and individuals

- Mandatory notification by government and businesses of unauthorized access to personal data

Distribution of Consumer Notices

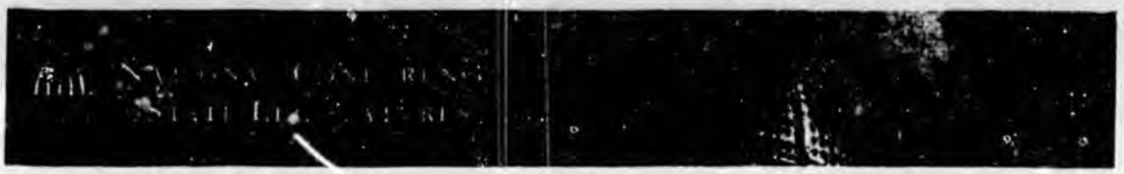
State	Notice Count
Alabama	1,338
Alaska	251
Arizona	1,730
Arkansas	696
California	34,114
Colorado	4,500
Connecticut	5,952
Delaware	1,072
District of Columbia	338
Florida	10,216
Georgia	2,805
Guam	4
Hawaii	677
Idaho	3,216
Illinois	5,025
Indiana	2,307
Iowa	809
Kansas	1,613
Kentucky	2,130
Louisiana	1,261
Maine	257
Maryland	2,750
Massachusetts	1,122
Michigan	2,318
Minnesota	2,338
Mississippi	1,317
Missouri	1,635
Montana	107
Nebraska	572
Nevada	739
New Hampshire	205
New Jersey	4,793
New Mexico	935
New York	9,370
North Carolina	6,983
North Dakota	137
Ohio	2,680
Oklahoma	795
Oregon	1,947
Pennsylvania	1,864
Puerto Rico	35
Rhode Island	203
South Carolina	2,372
South Dakota	140
Tennessee	1,153
Texas	11,081

Utah	986
Vermont	111
Virgin Islands	2
Virginia	1,494
Washington	3,189
West Virginia	210
Wisconsin	830
Wyoming	54
Total	144,778

Legal / Privacy

Attachment D

National Conference of State Legislatures,
"2005 Breach of Information Legislation"



2005 Breach of Information Legislation

Last update: March 7, 2005

In February 2005, ChoicePoint, a corporation that collects and compiles information that includes personal and financial information on millions of consumers, disclosed that it been the victim of a security breach wherein it had sold personal information of almost 145,000 people to a criminal enterprise. The company first disclosed the breach only to California residents, as required by California's Notice of Security Breach law, enacted in 2002. However, the company later disclosed that residents in other states, the District of Columbia and three territories also may have been affected by the ChoicePoint breach (see *List of states affected by ChoicePoint*).

Since these disclosures, additional states are considering legislation requiring that companies and/or state agencies disclose to consumers security breaches involving personal information. NCSL's Identity Theft Web page has additional information on related legislation.

***Summary**: Legislation is being considered in at least 20 states as of March 4, 2005.*
(See also 2004, 2003, and 2002 legislation.)

2005 Legislation

Arizona
S.B. 1114
Requires an entity disposing of records to take reasonable steps to ensure the destruction of personal financial and health information and personal identification numbers that are issued by governmental entities. Directs an entity discovering that personal identifying information has been stolen or improperly obtained, the entity must, within the most expedient time possible and without unreasonable delay: a) transmit notice to the person that there has been a breach of security regarding that person's personal identifying information. b) Provide information to that person regarding steps to be taken to protect against the unauthorized use of personal identifying information. Immunizes the entity from liability if it returned custody and control of the records back to the individual to whom the records pertain. Specifies that this legislation does not apply to the disposal of records by a transfer of the records to another entity. Allows an individual, who believes he or she may be injured by an entity's actions or failure to act, to request that a court stop an entity's actions or failure to act pursuant to this legislation. Permits the court to grant an injunction to stop an entity's actions or failure to act. Authorizes the attorney general to bring a civil action for damages and/or injunctive relief against an entity that fails to comply with this legislation. Specifies that any bank, financial institution, health care organization or other entity subject to and in compliance with certain federal regulations regarding protecting identifying information is in compliance with this legislation. Provides that the rights and remedies of this legislation are in addition to other rights or remedies provided by law. Defines "destroy," "entity," "individual," "personal identifying information" and "record."

California
A.B. 786
Requires the California State University system to provide an employee, upon request, with four hours of time off with pay following a disclosure by the university that there is, or could have been, a breach of security of employee personal information data, as specified.

S.B. 433
Existing law contains two identical provisions of law requiring any person or business that conducts business in California and that owns or licenses computerized data that includes personal information to disclose any breach of the security system following discovery or notification of the breach in the security of the data to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Repeals one of those two identical provisions, thereby making a technical, nonsubstantive change.

S.B. 852
Requires an agency, or a person or business conducting business in California, that possesses any data that includes the personal information of a California resident, to notify the resident of any breach of the security of the data, as specified. The bill also repeals

duplicative provisions of law.

Colorado

S.B. 137

Permits a consumer to apply or remove a security freeze to his or her consumer/credit report; requires that consumers be notified of the right to place the security freeze; compels a consumer reporting agency to notify the consumer after the credit information was released in violation of the security freeze; and allows consumers, in cases where the security freeze was violated, to pursue civil action and penalties up to $10,000 for each violation plus damages available under other civil laws. Requires government agencies, corporations, financial institutions and others who own or use personal information to notify consumers when there has been a breach of the security of data.

Georgia

H.B. 638

Relates to selling and other trade practices, so as to provide definitions; to require investigative consumer reporting agencies to give notice to consumers of certain security breaches; to provide for a standard of care to be exercised by investigative consumer reporting agencies; to provide for rules, regulations, and guidelines; to provide for related matters; to provide an effective date; to repeal conflicting laws; and for other purposes.

H.B. 648

Requires a person or business that conducts business in this state and that owns or licenses computerized data that includes personal information to disclose in specified ways any breach of the security of the data to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person; to permit notification to be delayed if a law enforcement agency determines that it would impede a criminal investigation; to require a person or business that maintains computerized data that includes personal information owned by another to notify the owner or licensee of the information of any breach of the security of the data; to provide for certain civil actions.

S.B. 230

Relates to selling and other trade practices, so as to provide definitions; requires investigative consumer reporting agencies to give notice to consumers of certain security breaches.

S.B. 245

Relates to business records, so as to require a person or business that conducts business in this state and that owns or licenses computerized data that includes personal information to disclose in specified ways any breach of the security of the data to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person; permits notification to be delayed if a law enforcement agency determines that it would impede a criminal investigation; requires a person or business that maintains computerized data that includes personal information owned by another to notify the owner or licensee of the information of any breach of security of the data; provides for certain civil actions; defines certain terms; to amends Chapter 18 of Title 50 of the Official Code of Georgia Annotated, relating to state printing and documents, so as to require an agency that owns or licenses computerized data that includes personal information to disclose in specified ways any breach of the security of the data to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person; permits notification to be delayed if a law enforcement agency determines that it would impede a criminal investigation; requires an agency that maintains computerized data that includes personal information owned by another to notify the owner or licensee of the information of any breach of security of the data; defines certain terms; provides for legislative findings and declarations.

S.B. 251

Relates to selling and other trade practices; requires certain business entities to give notice to consumers of certain security breaches; to provide for causes of actions and damages for unauthorized or improper access of personal information of consumers; to provide for certain criminal penalties; to provide for related matters; to provide an effective date; to repeal conflicting laws; and for other purposes.

Idaho

H.B. 555

Adds to existing law to provide legislative intent relating to the protection of personal information; to provide for disclosure upon breach in the security of personal information by certain agencies, persons and businesses; to provide for delayed notification in the event of certain criminal investigations; to provide for means of notice; to provide an exception; and to provide certain rights and remedies for

breach in the security of personal information

Illinois

H.B. 3743

Creates the Security Breach Notification Act. Requires any person or business conducting business in the State, and that owns or licenses computerized data that includes personal information, to disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any person whose unencrypted personal information was, or is reasonably believed to have been acquired by an unauthorized person. Requires any person or business that maintains computerized data that includes personal information that the person or business does not own, to notify the owner or licensee of the information of any breach of the security of the data immediately following discovery of such breach, if the personal information was, or is reasonably believed to have been acquired by an unauthorized person. Provides that notice may be provided to a customer in one of the following ways: (1) written notice; (2) electronic notice; or (3) substitute notice if the person or business demonstrates that the cost of providing notice would exceed $250,000, or the affected class of persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information. Provides a private right of action for a violation of the Act.

S.B. 209

Creates the Personal Information Protection Act. Requires each financial institution to provide an annual disclosure statement to all persons for which the financial institution maintains unencrypted personal information concerning measures the financial institution has taken to prevent (I) a breach of the security system and (II) any unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the financial institution. Requires each financial institution to maintain duplicate records of all computerized data at a back-up site located at least 90 miles from the primary site at which the data is stored. Provides that the effectiveness of the back-up site shall be tested annually and requires the results o that test to be included in the annual disclosure statement.

S.B. 1479

Creates the Identity Theft Notification Act. Requires any data collector that owns or uses personal information in any form that includes personal information concerning an Illinois resident, to disclose any breach of the security of the system following discovery or notification of the breach in the security of the data, without regard for whether the data has been accessed by an unauthorized third party for legal or illegal purposes. Provides that notice may be provided in one of the following ways: (1) written notice; (2) electronic notice; or (3) substitute notice if the person or business demonstrates that the cost of providing notice would exceed $250,000, or the affected class of persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information. Provides a private right of action for a violation of the Act.

S.B. 1798

Creates the Personal Information Protection Act. Requires any person, business, or State agency conducting business in the State, and that owns or licenses computerized data that includes vulnerable personal information, to disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any person whose unencrypted personal information was, or is reasonably believed to have been acquired by an unauthorized person. Requires any person, business, or State agency that maintains computerized data that includes vulnerable personal information that the person, business, or State agency does not own, to notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the vulnerable personal information was, or is reasonably believed to have been acquired by an unauthorized person. Provides that notice may be provided to a customer in one of the following ways: (1) written notice; or (2) substitute notice if the person or business demonstrates that the cost of providing notice would exceed $250,000, or the affected class of persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information.

S.B. 1799

Amends the Department of Revenue Law of the Civil Administrative Code of Illinois. Requires the Department of Revenue to notify an individual if the Department discovers or reasonably suspects that another person has used that individual's Social Security number.

S.B. 1899

Creates the Identity Theft Notification Act. Requires any agency, person, or business that conducts business in Illinois and owns or licenses data that includes personal information concerning an Illinois resident to notify the resident that there has been a breach of the security of that data following discovery or notification of the breach. Requires any agency, person, or business that maintains data that includes personal information concerning an Illinois resident and that the agency, person, or business does not own to notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been acquired by an unauthorized person. Provides that notice may be provided in one of the

following ways: (1) written notice; (2) electronic notice; or (3) substitute notice if the agency, person, or business demonstrates that the cost of providing notice would exceed $250,000, or the affected class of persons to be notified exceeds 500,000, or the agency, person, or business does not have sufficient contact information.

Indiana

S.B. 503

Prohibits a state agency from releasing the Social Security number of an individual unless the release is: (1) required by state law, federal law, or court order; (2) authorized in writing by the individual; (3) made to comply with the USA Patriot Act or Presidential Executive Order 13224; or (4) made to a commercial entity for permissible uses set forth in the Drivers Privacy Protection Act, the Fair Credit Reporting Act, or the Financial Modernization Act of 1999. Provides that disclosure of the last four digits of a Social Security number is not considered a disclosure of the Social Security number. Requires a state agency to notify an individual of a security breach of the agency's computer system if the individual's unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person. Makes it a Class D felony to knowingly make a false representation to obtain a Social Security number or for an agency employee to knowingly disclose a Social Security number. Provides that an agency employee who negligently discloses a Social Security number commits a Class A infraction. Requires an individual who prepares a document for recording to certify that the individual reviewed the entire document and took reasonable care to redact Social Security numbers in the document. After December 31, 2007, requires a county recorder or an employee of a county recorder to search documents using the redacting technology to redact Social Security numbers before the documents are release for public inspection. Establishes a pilot project beginning July 1, 2005, to develop procedures and test technology and equipment for searching recorded documents and redacting Social Security numbers.

S.B. 544

Prohibits a state agency from releasing the Social Security number of an individual unless the release is: (1) required by state law, federal law, or court order; (2) authorized in writing by the individual; (3) made to comply with the USA Patriot Act or Presidential Executive Order 13224; or (4) made to a commercial entity for permissible uses set forth in the Drivers Privacy Protection Act, the Fair Credit Reporting Act, or the Financial Modernization Act of 1999. Provides that disclosure of the last four digits of a Social Security number is not considered a disclosure of the Social Security number. Requires a state agency to notify an individual of a security breach of the agency's computer system if the individual's unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person. Makes it a Class D felony to knowingly make a false representation to obtain a Social Security number or for an agency employee to knowingly disclose a Social Security number. Provides that an agency employee who negligently discloses a Social Security number commits a Class A infraction. Requires an individual who prepares a document for recording to certify that the individual reviewed the entire document and took reasonable care to redact Social Security numbers in the document. After December 31, 2007, requires a county recorder or an employee of a county recorder to search documents using the redacting technology to redact Social Security numbers before the documents are release for public inspection. Establishes a pilot project beginning July 1, 2005, to develop procedures and test technology and equipment for searching recorded documents and redacting Social Security numbers.

Minnesota

H.F. 1410

Requires businesses maintaining personal information in electronic form to disclose to consumers breaches in security.

S.F. 1307

Requires disclosure to consumers of a breach in security by businesses maintaining personal information in electronic form.

Missouri

S.B. 506

Prohibits the sharing of personal financial information with any unauthorized person unless the individual consents to the share. Requires a business or person that conducts business in the state that owns or licenses computerized data, to disclose any breach of security of that data, to any citizen of this state whose information may, or may very well have been, acquired by an unauthorized person. Allows for individuals to place security alerts and security freezes on their credit report, notifying any recipient of the report that the individual may have been a victim of identity theft, and prohibiting the release of the individual's information without the express consent of the consumer. Details the obligations of consumer reporting agencies in response to this option.

Montana

H.B. 732

Adopts and revises laws to implement individual privacy and to prevent identity theft; requires a consumer reporting agency to block or expunge information on a report that results from a theft of identity; provides privacy protection provisions for credit card solicitations and renewals and telephone accounts; provides privacy protection for business records by requiring destruction of records; requires businesses to report a breach of computer security; requires a business that has an established business relationship with a customer and that has disclosed certain personal information to third parties to report that information to the customer; providing remedies and penalties for violation.

New Jersey

A.B. 1080

Requires that a financial institution that discovers or reasonably should discover that a consumer's nonpublic personal information maintained by the financial institution was compromised in any way shall promptly notify the consumer of the breach of the security or confidentiality of the information. In addition to promptly notifying a consumer of the security compromise, a financial institution is required to provide assistance to the consumer to remedy any such compromise; to reimburse the consumer for any losses the consumer incurred as a result of the compromise of the security or confidentiality of such information; and to provide information concerning the manner in which the consumer can obtain assistance. However, a financial institution may delay notifying a consumer of the compromise of the security or confidentiality of the information at the request of a law enforcement agency investigating such violation for a period determined by the law enforcement agency performing the investigation. Additionally, if an issuer of credit receives a request for an additional credit card for an existing cardholder no later than 30 days after receiving a change of address for the cardholder, the issuer of credit is required to notify the cardholder of the request at the new address and former address no later than five days after sending the additional card to the new address. The issuer of credit shall also provide the cardholder with a means of promptly reporting incorrect changes. Any violation of this bill shall be punished under either N.J.S.A.56:11-38 or N.J.S.A.56:11-39, or both.

A.B. 2048

Requires a business to take all reasonable steps to destroy customer records within its control containing personal information which is no longer to be retained by the business. The customer records shall be destroyed by shredding, erasing, or otherwise modifying the personal information to make them unreadable or undecipherable through any means. In addition, any business that conducts business in New Jersey and owns or licenses computerized data that includes personal information must disclose any breach of the security of the computer system within 15 days to any customer who is a resident of New Jersey whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. However, the disclosure may be delayed if a law enforcement agency determines that notification will impede a criminal investigation. Any business that maintains computerized data that includes personal information that the business does not own shall notify the owner or licensee of the information of any breach of the security of the system immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. For purposes of this bill, notice may be written or electronic. If the business demonstrates that the cost of providing notice would exceed $250,000, or that the affected class of subject persons to be notified exceeds 500,000, or the business does not have sufficient contact information, it may provide substitute notice, which must consist of all of the following: (1) e-mail notice when the business has an e-mail address; (2) conspicuous posting of the notice on the Web site page of the business, if the business maintains one; and (3) notification to major statewide media. However, a business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of the bill, shall be deemed to be in compliance with the notification requirements of this bill if the business notifies subject persons in accordance with its policies in the event of a breach of security of the system. Finally, a violation of any provisions of this bill shall be an unlawful practice subject to the penalties applicable to a violation of the consumer fraud law pursuant to N.J.S.A. 56:8-13. Under N.J.S.A. 56:8-13, any business who violates any of the provisions of this bill, in addition to any other penalty provided by law, shall be liable to a penalty of not more that $10,000 for the first offense and not more than $20,000 for the second and each subsequent offense.

New York

A.B. 1525

Requires any banking institution that owns or licenses data that includes personal identifying information to disclose any breach of security following discovery or notification of such breach to any person whose personal identification was, or is reasonably believed to have been, acquired by an unauthorized person; defines personal identifying information and breach of security.

A.B. 4254

Requires any state agency or business which owns or licenses a computerized database which includes vulnerable personal information shall disclose any breach of security of such system to any resident of New York state whose unencrypted personal information may have been acquired by an unauthorized person; provides enforcement provisions.

A.B. 5487
Enacts the "personal information protection act", requiring disclosure of breaches of security of data systems of business entities to affected persons; provides for administration by the department of state; requires use of best available technology to detect breaches of security; provides for a private right of action.

S.B. 2161
Requires any state agency or business which owns or licenses a computerized database which includes vulnerable personal information shall disclose any breach of security of such system to any resident of New York state whose unencrypted personal information may have been acquired by an unauthorized person; provides enforcement provisions.

S.B. 2906
Requires notice to residents when a computerized database security breach releases personal information.

Ohio
H.B. 104
Requires a state agency, person, or business to contact individuals if unencrypted personal information about those individuals that is maintained on the computers of the agency, person, or business is obtained by unauthorized persons.

S.B. 89
Requires a state agency, person, or business to contact individuals if unencrypted personal information about those individuals that is maintained on the computers of the agency, person, or business is obtained by unauthorized persons.

Oregon
S.B. 626
Requires a person who owns or uses personal information to notify an individual when there is an unauthorized acquisition of personal information that compromises security of information.

Rhode Island
H.B. 5893
Establishes a duty to disclose any breach of security of a computerized data system.

S.B. 880
Establishes a duty to disclose any breach of security of a computerized data system.

Tennessee
H.B. 2170
Requires persons, businesses or government agencies that discover a breach of information security resulting in disclosure of unencrypted personal information about persons to unauthorized third parties to provide notice of such disclosure.

S.B. 2220
Requires persons, businesses or government agencies that discover a breach of information security resulting in disclosure of unencrypted personal information about persons to unauthorized third parties to provide notice of such disclosure.

Texas
H.B. 1527
Requires those who own or license data that includes identifying information to promptly notify the resident of any alleged breach of the security of the person's data system, regardless of whether the resident's identifying information has been accessed by an unauthorized person.

Virginia
H.B. 2721
Requires agencies and businesses that maintain computerized data that includes personal information to notify the subject of that information when a breach of the database containing that information is discovered. No notice is required if an investigation determines that there is no reasonable belief that the information has been or will be used in an unlawful manner. Provides for various means of notifying the owner or licensee of that information and requires the agency or business to coordinate notification with

consumer reporting agencies if they indicated that the affected individual can obtain a credit report. Damages for an agency violating this requirement are provided in the Government Data Collection and Dissemination Practices Act (§ 2.2-3800 et seq.). Damages for a business violating this requirement are provided in the Personal Information Privacy Act or PIPA (§ 59.1-442 et seq.). Expands the damages available for violations of PIPA to include actual damages, if greater than $100 per violation, and injunctive relief.

Washington
S.B. 6043
Requires any agency that owns or licenses computerized data that includes personal information to disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Requires the disclosure to be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in this act, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. Requires any person or business that conducts business in this state and that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in this act, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

West Virginia
H.B. 2772
Requires commercial entities who maintain databases containing resident individuals' personal information, to notify a resident individual, in writing, whenever the individual's personal information has been compromised by unauthorized disclosure; and defines personal information.

NCSL Contact: Pam Greenberg, pam.greenberg at ncsl.org, NCSL Denver Office, 303-364-7700

Privacy Home

2004 Legislation

(Red highlight indicates legislation failed/was not enacted; green highlight indicates legislation passed/was enacted)

California
S.B. 1279
Passed Senate 5/24/04
Requires an agency, or a person or business conducting business in California, that possesses any data that includes the personal information of a California resident, to notify the resident of any breach of the security of the data, as specified.

Florida
H.B. 1189
Died in committee 4/30/04
Requires certain persons who maintain computerized data that contains personal information to notify any state resident whose unencrypted personal information may have been obtained as result of security breach; provides for forms of notice; provides exceptions and alternative forms of notice; provides for delays in notification in certain circumstances.

S.B. 2684
Died in committee 4/30/04
Requires certain persons who maintain computerized data that contains personal information to notify any state resident whose unencrypted personal information may have been obtained as result of security breach; provides for forms of notice; provides for delays in notification in certain situations.

Louisiana
S.B. 417
Legislature adjourned June 21, 2004
Requires businesses to notify customers of a breach of security of their computerized data.

New Jersey

A.B. 1080

10/4/2004 Reported out of Asm. Comm. with Amendments, and Referred to Assembly Financial Institutions and Insurance Committee

Requires that a financial institution that discovers or reasonably should discover that a consumer's nonpublic personal information maintained by the financial institution was compromised in any way shall promptly notify the consumer of the breach of the security or confidentiality of the information. In addition to promptly notifying a consumer of the security compromise, a financial institution is required to provide assistance to the consumer to remedy any such compromise; to reimburse the consumer for any losses the consumer incurred as a result of the compromise of the security or confidentiality of such information; and to provide information concerning the manner in which the consumer can obtain assistance. However, a financial institution may delay notifying a consumer of the compromise of the security or confidentiality of the information at the request of a law enforcement agency investigating such violation for a period determined by the law enforcement agency performing the investigation. Additionally, if an issuer of credit receives a request for an additional credit card for an existing cardholder no later than 30 days after receiving a change of address for the cardholder, the issuer of credit is required to notify the cardholder of the request at the new address and former address no later than five days after sending the additional card to the new address. The issuer of credit shall also provide the cardholder with a means of promptly reporting incorrect changes. Any violation of this bill shall be punished under either N.J.S.A.56:11-38 or N.J.S.A.56:11-39, or both.

A.B. 2048

2/5/2004 Introduced, Referred to Assembly Consumer Affairs Committee

Requires a business to take all reasonable steps to destroy customer records within its control containing personal information which is no longer to be retained by the business. The customer records shall be destroyed by shredding, erasing, or otherwise modifying the personal information to make them unreadable or undecipherable through any means. In addition, any business that conducts business in New Jersey and owns or licenses computerized data that includes personal information must disclose any breach of the security of the computer system within 15 days to any customer who is a resident of New Jersey whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. However, the disclosure may be delayed if a law enforcement agency determines that notification will impede a criminal investigation. Any business that maintains computerized data that includes personal information that the business does not own shall notify the owner or licensee of the information of any breach of the security of the system immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. For purposes of this bill, notice may be written or electronic. If the business demonstrates that the cost of providing notice would exceed $250,000, or that the affected class of subject persons to be notified exceeds 500,000, or the business does not have sufficient contact information, it may provide substitute notice, which must consist of all of the following: (1) e-mail notice when the business has an e-mail address; (2) conspicuous posting of the notice on the Web site page of the business, if the business maintains one; and (3) notification to major statewide media. However, a business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of the bill, shall be deemed to be in compliance with the notification requirements of this bill if the business notifies subject persons in accordance with its policies in the event of a breach of security of the system. Finally, a violation of any provisions of this bill shall be an unlawful practice subject to the penalties applicable to a violation of the consumer fraud law pursuant to N.J.S.A. 56:8-13. Under N.J.S.A. 56:8-13, any business who violates any of the provisions of this bill, in addition to any other penalty provided by law, shall be liable to a penalty of not more that $10,000 for the first offense and not more than $20,000 for the second and each subsequent offense.

New York

A.B. 9184

S.B. 6517

Requires any state agency or business which owns or licenses a computerized database which includes vulnerable personal information shall disclose any breach of security of such system to any resident of New York state whose unencrypted personal information may have been acquired by an unauthorized person; provides enforcement provisions.

A.B. 9431

S.B. 6615

Enacts the Personal Information Protection Act, requiring disclosure of breaches of security of data systems of business entities to affected persons; provides for administration by the Department of State; requires use of best available technology to detect breaches of security; provides for a private right of action.

A.B. 10295

S.B. 7121

Requires any banking institution that owns or licenses data that includes personal identifying information to disclose any breach of security following discovery or notification of such breach to any person whose personal identification was, or is reasonably believed to have been, acquired by an unauthorized person; defines personal identifying information and breach of security.

A.B. 11012
S.B. 6739
Requires notice to residents when a computerized database security breach releases personal information.

2003 Legislation

(Red highlight indicates legislation failed/was not enacted; green highlight indicates legislation passed/was enacted)

New York
A.B. 9184
S.B. 6517
Requires any state agency or business which owns or licenses computerized database which includes vulnerable personal information shall disclose any breach of security of such system to any resident of New York state whose unencrypted personal information may have been acquired by an unauthorized person; provides enforcement provisions.

2002 Legislation

(Green highlight indicates legislation passed/was enacted)

A.B. 700
Chaptered by secretary of state 9/29/02, Chapter 1054
Operative July 1, 2003, requires a state agency, or a person or business that conducts business in California, that owns or licenses computerized data that includes personal information, as defined, to disclose in specified ways, any breach of the security of the data, as defined, to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Permits the notifications required by its provisions to be delayed if a law enforcement agency determines that it would impede a criminal investigation. Requires an agency, person, or business that maintains computerized data that includes personal information owned by another to notify the owner or licensee of the information of any breach of security of the data, as specified. States the intent of the Legislature to preempt all local regulation of the subject matter of the bill. Makes a statement of legislative findings and declarations regarding privacy and financial security.

NCSL Contact: Pam Greenberg, pam.greenberg at ncsl.org, NCSL Denver Office, 303-364-7700

Privacy Home

Denver Office: Tel: 303-364-7700 | Fax: 303-364-7800 | 7700 East First Place | Denver, CO 80230 | Map
Washington Office: Tel: 202-624-5400 | Fax: 202-737-1069 | 444 North Capitol Street, N.W., Suite 515 | Washington, D.C. 20001

FISCAL NOTE

STATE OF ALASKA
2005 LEGISLATIVE SESSION

Fiscal Note Number:
Bill Version: HB226-LAW-C&FB-1-5-(
() Publish Date:

Revision Date/Time (Note if correction):
Dept. Affected: LAW
Title "An Act relating to breaches of security involving personal information; and relating to credit report..."
RDU CIVIL
Component Commercial & Fair Business
Sponsor Representative Gara
Requester House Labor and Commerce
Component No.

Expenditures/Revenues (Thousands of Dollars)

Note: Amounts do not include inflation unless otherwise noted below.

OPERATING EXPENDITURES	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
Personal Services						
Travel						
Contractual						
Supplies						
Equipment						
Land & Structures						
Grants & Claims						
Miscellaneous						
TOTAL OPERATING	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**
CAPITAL EXPENDITURES						
CHANGE IN REVENUES ( )						

FUND SOURCE (Thousands of Dollars)

1002 Federal Receipts						
1003 GF Match						
1004 GF						
1005 GF/Program Receipts						
1037 GF/Mental Health						
Other (Specify Type--Do not abbreviate)						
TOTAL	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**

Estimate of any current year (FY2005) cost: 0.0
Mark this box (X) if funding for this bill is included in the Governor's FY 2006 budget proposal:

POSITIONS

Full-time						
Part-time						
Temporary						

ANALYSIS: *(Attach a separate page if necessary)*

This bill ads a chapter to AS 45 that imposes disclosure requirements on businesses that collect and store personal information if there is a security breach of the businesses' information system. In the event of a security breach, notice of the breach must be made to consumers by either written or electronic means, with some exceptions if the notice will cost more than $250,000, or the number of affected consumers exceeds 500,000. Consumers can bring a court action for violations of this law to recover damages and injunctive relief.

The bill also ads a section that allows consumers to place a security freeze on his or her credit report. When a security freeze is in place, a credit reporting agency may not release information from the consumer's credit report to third parties unless requested by the consumer. There are several exemptions for access required to correct technical information, and for some agencies like the child

Prepared by: Kathryn Daughhetee, Director
Phone 465-3673
Division Administrative Services Division
Date/Time 4/5/05 3:23 PM
Approved by: Kathryn Daughhetee for Gregg D. Renkes, Attorney General
Date 4/5/2005
Agency Department of Law

FISCAL NOTE

STATE OF ALASKA
2005 LEGISLATIVE SESSION

BILL NO. _____

ANALYSIS CONTINUATION

support enforcement agency, Department of Health and Social Services, and Department of Revenue. Court action can be brought by consumers to enforce this law. Remedies include injunctive relief, damages (including lost wages and pain and suffering), and punitive damages up to $5000.

Violations of the provisions of this bill are not automatically violations of Alaska's Consumer Protection Act. Consumers will likely be left to their own enforcement efforts for violations of this Act except in the most egregious cases where the State may bring an action. I do not believe there will be any significant fiscal impact to the Department of Law from this bill.