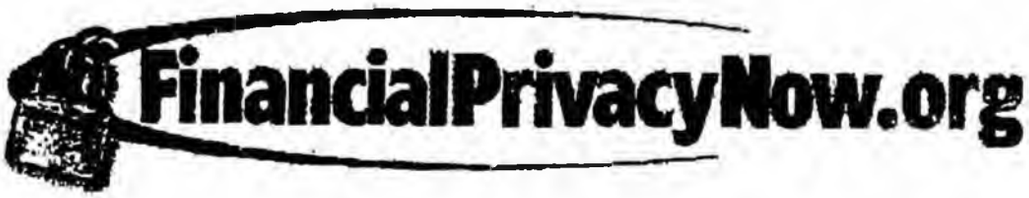

Consumer Reports Poll: Americans Are Concerned About the Widespread Use of Social Security Numbers & Want Lawmakers to Restrict the Practice

Consumer Reports National Research Center found that 89 percent of Americans want lawmakers to restrict the use and availability of Social Security numbers by businesses and government agencies. The poll, released Sept. 6, 2007, found that consumers are routinely asked to provide their Social Security numbers and that requests come from a wide variety of businesses, many of which have no clear need to collect these numbers. The poll found that:

87 percent of consumers have been asked in the past year to provide their Social Security number in whole or in part by a business or government agency.

- In the past year, 60 percent of consumers have been asked by a financial institution or retailer issuing credit to provide their Social Security number, while 49 percent have been asked to disclose their number to health care providers.
- Consumers also reported being asked to provide their Social Security number in the past year to a wide variety of other entities, including: employers or potential employers (44%); insurance companies (38%); government agencies other than the IRS or a state tax body (32%); college or other school (28%); service provider such as cable TV or cell phone carrier (26%); utilities (17%), and merchant or retailer (16%).
- More than four in ten Americans (42%) have been asked to provide their full or partial Social Security number on the phone or Internet to access goods or services or to verify their identity to customer service representatives.
- One in seven Americans (14%) had received postal mail (other than tax documents) bearing their own or a family member's Social Security number in the past year.
- Fifty two percent of Americans carry a card in their wallets that has their number on it.

The *Consumer Reports* poll found that nearly one-quarter of adults (23%) have been victims of identity theft themselves or have a family member whose identity has been stolen in the past five years. Americans are concerned about the widespread availability of Social Security numbers and how businesses are using them:

- 78 percent would prefer not to provide their number, but are concerned about the consequences of refusing to do so.
- 91 percent agreed they are more vulnerable to identity theft when a business has their number.
- 89 percent agreed that companies should stop using Social Security numbers to identify customers.
- 96 percent agreed that companies should not be able to sell SSNs.

An overwhelming majority of Americans want to be notified when their Social Security number has been involved in a data security breach. Ninety eight percent agreed that companies and

government agencies should always be required to notify them if a database containing their Social Security number has been compromised.

Virtually all Americans (97%) believe they should be provided with remedies to help thwart potential fraud if their Social Security number is involved in a data security breach. Among them:

- 68 percent agreed that they should be given the ability to freeze access to their credit files at no charge to stop new accounts from being opened unless they unlock the credit file with a PIN.
- Only 12 percent preferred free credit monitoring when Social Security numbers have been involved in breaches, which is the remedy often provided by companies that fail to keep sensitive files protected.

Independently of whether their sensitive information has been involved in data security breach, 97 percent of Americans want the ability to freeze access to credit files to prevent thieves from opening fraudulent accounts.

Consumers Union recommends that the sale and purchase of Social Security numbers be tightly restricted, that laws should prohibit using Social Security numbers on identification cards, and that businesses should be prohibited from soliciting Social Security numbers except where required by law or where needed for credit, employment, tax compliance, or investment purposes.

For a copy of Consumers Union's model Social Security number privacy bill, see:

http://www.consumersunion.org/pub/core_financial_services/004800.html

To find out what some states already have done with Social Security number use, see:

http://www.consumersunion.org/finance/StateSSNProtections.htm

To find out if your state already has a security freeze, and how to use it, see:

http://www.consumersunion.org/finance/SecurityFreeze.htm

Methodology of the *Consumer Reports* Poll: The Consumer Reports National Research Center conducted a telephone survey using a nationally representative probability sample of telephone households. 1,016 interviews were completed among adults aged 18+. Interviewing took place over August 16-19, 2007. The margin of error is +/- 3.1% at a 95 percent confidence level.

For more information on the *Consumer Reports* Social Security number poll, contact Gail Hillebrand (415-431-6747) or Jeannine Kenney (202-462-6262).

From AOL, Google, Monster.Com, NetChoice
Reed Elsevier, Verizon, Yahoo

January 18, 2008

1/23/08

The Honorable John Coghill
State Capitol, Room 214
Juneau, AK 99801-1182

Dear Representative Coghill:

We are writing to express our opposition to HB 65, which would impose security breach notification requirements and Social Security Number use restrictions that significantly diverge from laws enacted in other states. HB 65 would impose significant new compliance burdens on businesses without providing tangible benefits to the security and confidentiality of consumers' personal information.

The security breach notification provisions under HB 65 are vastly different from those imposed under similar state laws.

- **Overly Broad Definition of "Personal Information":** The bill would require notification for data elements that are not sensitive. Telephone numbers and addresses, for example, are not the types of sensitive data elements that would render an Alaska resident susceptible to identity theft, fraud, or financial harm. Additionally, in the absence of a financial account number, "account passwords or personal identification numbers" would not facilitate access to an individual's financial account, and thus would pose no risk of identity theft, fraud, or financial harm. Moreover, in requiring notification under circumstances where account passwords have been compromised, notifying entities would be unwittingly tipping off hackers and spammers who may have been responsible for compromising the e-mail or other Internet accounts of Alaskan residents, complicating efforts to identify and prosecute criminals. We urge you to eliminate these features of the definition of "personal information" to make it consistent with the definition of "personal information" found in almost all of the 39 existing state security breach laws.

- **Definition of "Personal Information" Does Not Exempt Publicly Available Records:** The definition of "personal information" does not exempt information that is lawfully made available in public records. This exception exists in almost all of the existing 39 state security breach laws. The exception recognizes the fact that because this information is already publicly available, its breach poses minimal risk.

- **Application to Both Electronic Data and Paper Records:** The security breach provisions in HB 65 apply to personal information "in any form". Identity thieves target databases that contain personal information about consumers because they present a rich and large universe of personal information. The same is not true with respect to paper records, which require physical theft and rarely provide identity thieves with easily ascertainable, sensitive personal information concerning a wide swath of individuals. The current version of the bill would likely require businesses to notify consumers if a

paper file or slip of paper was missing, which happens commonly even if there was no risk of harm to the consumer.

- **Notification Is Not Tied to a Risk of Harm:** Under the bill, businesses must notify consumers of any security breach, even where there is no risk of identity theft, fraud, or financial harm. Without a nexus to risk of harm, however, the bill would result in over-notification of consumers where no risk exists at all. A requirement to notify Alaska residents of security breaches in the absence of a risk of harm may have the unintended consequence of encouraging individuals to disregard notices after they receive several security breach notifications where there is no risk. A risk of harm standard ensures that Alaska residents are notified in instances when they should act on the notice -- where a security breach may cause monetary loss.

- **Enforcement Provisions Would Encourage Costly Litigation:** HB 65 provides that a failure to notify affected residents of a security breach constitutes an unfair or deceptive act or practice. Alaska residents may enforce violations of the unfair and deceptive acts or practices law through class action lawsuits with statutory damage awards of at least $500 per violation. Statutory damages are entirely inappropriate for violations of this law because nearly all security breaches result in no harm to consumers whatsoever. The only beneficiary of this provision would be the plaintiff's bar, which would extract large settlements from Alaska businesses without showing any actual harm to consumers.

- **Notification by E-Mail Not Authorized:** E-mail is often the exclusive means by which Internet companies communicate with consumers. Customers of Amazon or eBay, for example, would expect to receive a security breach notification via e-mail. The current version of the bill, however, only permits e-mail notice in accordance with the E-SIGN law, which requires businesses to obtain customers' express consent to e-mail notice *prior to the onset* of this breach. This is simply not practicable in many instances. Moreover, the vast majority of state security breach notification laws either implicitly or explicitly authorize notification by e-mail.

HB 65 would also impose restrictions on the use or disclosure of Social Security Numbers (SSNs) that far exceed those imposed by other state laws. Although several exemptions are provide for under the bill, businesses could would be prohibited from using third party authentication services to verify the identify of SSNs of individuals who furnish such information. This would actually weaken businesses' efforts to reduce the incidence of identity theft and fraud. Other legitimate business purposes for the disclosure of SSNs would be barred by the blanket prohibition language in the bill.

For all of these reasons, we strongly oppose HB 65. Thank you for your time and consideration.

Sincerely,

AOL
Google
Monster.com
NetChoice
Reed Elsevier
Verizon
Yahoo!

1/23/08

ID thieves may have hit Alaska - CHOICEPOINT: Information clearinghouse breach could have compromised privacy of 251.

Anchorage Daily News (AK) - February 24, 2005

Author: RICHARD RICHTMYER Anchorage Daily News ; Staff

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.

PROTECT YOURSELF: Learn how to get your free credit report and avoid identity theft at

www.adn.com

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

Caption: Photo 2: purple_heart2.sj_022405.jpg Graphic 1: Weblink CMYK_022405.eps

Edition: *Final*
Section: *Main*
Page: *A1*
Record Number: *723470002/24/05*

AARP Alaska

1/23/08

January 23, 2008

The Honorable Mike Chenault, Co-Chair
House Finance Committee
Alaska State Capitol, Room 505
Juneau, AK 99801-1182

The Honorable Kevin Meyer, Co-Chair
House Finance Committee
Alaska State Capitol, Room 515
Juneau, AK 99801-1182

HB 65 (Coghill and Gara)—Support

Dear Co-Chairs Chenault and Meyer:

On behalf of the members of AARP in Alaska, we urge you and your colleagues on the House Finance Committee to support HB 65, authored by Representative John Coghill and Representative Les Gara and co-sponsored by your Committee members Representative Mike Hawker and Kurt Olson and Representatives Lynn, Samuels, Ramras, Fairclough, Kawasaki, Kerttula, Gatto, Neuman. This bill builds on much of the excellent work done in a previous session by Senators Gene Therriault and Gretchen Guess.

As you can see, addressing the issue of identity theft has always been and still is a bi-partisan issue.

AARP believes HB 65 will be one of the most comprehensive identity theft bills in the United States. It should be. The Legislature should provide our citizens with effective protections against the unauthorized dissemination of information about their use of financial, credit, retail, and communications services. HB 65 will accomplish this.

Obviously, an issue that has attracted much attention is the unauthorized acquisition of, or access to, records containing the sensitive personal information of an individual as the result of a security break.

In 2006, AARP analyzed 244 publicly disclosed security breaches and found that, between January 1, 2005 and May 26, 2006, the names of 89.8 million people were potentially exposed to identity theft as a result of security breaches.

We also found that older users of the Internet were much less likely to participate in on-line commercial activities. Forty-three percent of our younger members, aged 50 to 64

do "not at all" trust companies providing information or services on the Internet; only nineteen percent indicated they "mostly" or "completely" trust such companies.

The widespread use of Social Security numbers in both the public and private sectors has raised important concerns about the ability of identity thieves to gain access to people's Social Security numbers. Many public records that contain SSNs are available on the Internet. A 2004 federal Government Accountability Office report estimates that up to 48 percent of our nation's population lives in a county that makes SSNs contained in public records accessible via the Internet.

You have all heard the horror stories of identity theft victims. How long it takes to clear their records, how much they have to spend in the process, the credit problems they often face for years. I'll give you another one that I hope will convince you to support HB 65: older identity theft victims have higher mortality rates than non-victims.

Will HB 65 solve all identity theft problems? No. Will it help? Yes. Should you support it? If you care to join in the fight against identity thieves, if you care about protecting yourselves, your families, and your constituents, we certainly hope so.

AARP strongly recommends an "AYE" vote on HB 65.

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 Bill Stoltze
Representative Richard Foster
Representative Mike Hawker
Representative Bill Thomas
Representative Harry Crawford
Representative Les Gara
Representative Reggie Joule
Representative Mike Kelly
Representative Mary Nelson
Representative Kurt Olson
Representative John Coghill
Senator Gene Therriault

AKPIRG

1/23/08

A ALASKA / LASKA PUBLIC INTEREST RES · ALASKA PUBLIC INTEREST RESEARCH
PO Box 101093 ♦ Anchorage, Alaska 99510-1093 ♦ Ph: (907) 278-3661 ♦ Fax: (907) 278-9300 ♦ email: akpirg@akpirg.org

AkPIRG Supports HB 65 – Identity Theft Protections for Alaskan Consumers

AkPIRG urges support for HB 65. Identity Theft is an increasing problem, particularly in Alaska. This bill's bi-partisan co-sponsorship shows the importance of this issue and AkPIRG is pleased that members of both parties are working to protect Alaskans from Identity Theft.

According to the Privacy Rights Clearinghouse, over 100 million data records of U.S. residents have been exposed due to security breaches since February 2005. Alaska topped the nation in fraud complaints in 2005: 249 per 100,000 people, according to the Federal Trade Commission (FTC). Identity theft topped the list of nationwide complaints for the sixth year in a row, according to the FTC's annual report. Alaskans lost an average of $1,062. According to the Privacy Rights Clearinghouse, the average consumer spends 175 hours clearing their name after an identity theft. Identity Theft also costs businesses, large and small, an incredible amount each year.

HB 65 will help Alaskan consumers better protect themselves. The two most important measures of HB 65 will mandate that consumers be notified after a security breach and will allow consumers to freeze their credit reports.

Twenty-five states currently have laws allowing consumers to restrict access to their credit reports, with more states taking this necessary step to protect consumers. This security freeze allows consumers to stop identity thieves before they can set up new accounts in the consumer's name without the consumer's knowledge. Alaskans deserve this protection.

Mandatory notification after a security breach has passed in at least 34 states. Indeed, it was the fact that California had such a law in place in early 2005 that Choicepoint Inc. put security breaches on all of our radar.

It is time for Alaska to take these steps to better protect Alaskan consumers. Other provisions in HB 65 will further shield consumers from identity thieves by protecting private information and assuring that victims of identity theft will be treated fairly in their attempts to clear their name.

Thank you for your attention to this matter and for doing what you . pass Identity Theft protection legislation as soon as possible.

Thank you for your support of HB 65.
Sincerely,

Steve Cleary

Steve Cleary
AkPIRG Director

Founded in 1974, the Alaska Public Interest Research Group (AkPIRG) is a non-profit, non-partisan, citizen-oriented statewide organization researching, educating and advocating on behalf of the public interest. AkPIRG has 1,000 Alaskan members.

1/23/08

HB 65 LIABILITY ISSUES

From: Ed Sniffen
Dept of Law
4/20/2007

The Department of Law does not oppose the concept behind HB 65, which will add significant protections for consumers against identity theft. The state does, however, oppose provisions in the bill that will impose liability on the state and its agencies.

The section that causes the Department the most concern is in Article 4 (protection of social security numbers) at Sec. 45.48.480 (penalties) beginning on page 21 of the bill. This section allows the recovery of ***actual damages or $5,000***, whichever is greater, for knowing violations of AS 45.48.400 – 45.48.430. The state's monetary exposure under this section could be enormous. The Department believes this exposure is completely unnecessary:

* **This penalty provision will not change the states conduct, and will not further any goals of this bill. The state is committed to securing all of the personal information it must collect and maintain, and has spent millions of dollars upgrading its systems. This effort will continue regardless of HB 65.**

* **The requirement that the violation be a "knowing" violation does not protect the state. The definition of "knowing" in AS 11.81.900 is broad, and includes only that you be "aware" of your conduct.**

* **No other state has imposed this kind of liability on its state agencies for these kinds of violations. And for good reason. There is no reason to expose state coffers to billions of dollars in potential damage awards.**

* **Removing the state from these penalty provisions WILL NOT create a "double standard" between private business and state government for a variety of reasons:**

1. **Unlike private business, the state does not profit from the sale or use of personal information.**

2. **Unlike private business, the state is REQUIRED to perform specific statutory duties under state law that require the use, disclosure, and sharing of personal information.**

3. **Unlike private business, the state cannot insure itself against a potential loss resulting from an inadvertent disclosure of a SSN. Private industry can build these risks into its business plan, and price its products accordingly.**

4. **The state is routinely treated differently than private business when liability is concerned. For example, the state enjoys "discretionary function" immunity for certain tort actions (AS 09.50.250); and state employees have qualified immunity for performing duties required by statute. The state is also exempt of punitive damage awards. The policy behind treating the state differently is clear, and does not create a "double standard."**

* **HB 65 will, therefore, create liability where none currently exists, and will have the effect of amending state law that currently provides immunity to the state.**

* **The state is always an attractive target for litigation. If the legislature creates state liability through this bill, the state will get sued. Regardless of the merit of any lawsuit, it will take significant resources to defend the lawsuit.**

* **Because the state must utilize, process, and maintain records that can contain personal information on hundreds of thousands of state residents, just one breach of the requirements in HB 65 could result in billions of dollars of exposure.**

* **The state has no objection to requiring its agencies to comply with the provisions of HB 65. But failure to comply should be addressed through the political process, not the legal process.**

The Department of law proposes the following amendment to Sec. 45.48.480(b) and (c):

(b) An individual may bring a civil action in court against a person, <u>other than a governmental agency</u>, who knowingly violates AS 45.48.400 – 45.48.430 and may recover actual damages or $5,000, whichever is greater, and court costs and attorney fees allowed by the rules of court.

(c) A person, <u>other than a governmental agency</u>, who knowingly violates AS 45.48.400 – 45.48.430 is guilty of a class A misdemeanor.

These changes will address the Department's concerns with liability.

Good morning Chairman Olson and other members of the committee

My name is Craig Dahl and I am the President & CEO for Alaska Pacific Bank, which is headquartered here in Juneau. Alaska has been my home for more than 45 years, which includes 34 years of community banking. I am a member and past president of the Alaska Bankers Association and a member of the American Bankers Association Government Relations Council for the past 18 years.

I am here this morning representing the Alaska Bankers Association and my comments will be made in reference to HB 65.

You should have all received a copy of a letter written to chairman Coghill by David Lawer, who is the current President of the Alaska Bankers Association but I would like to reinforce the message contained in Mr. Lawer's letter.

The Alaska Bankers Association, which represents all 9 banks in the state, supports the intention of HB 65 to protect customers' financial information, recognizing the legislature's desire to address these critical issues.

At the same time, we believe it is in the best interest of the bill itself to track as close to federal regulations as possible, and where appropriate, clearly acknowledge the federal preemption for those operating under those regulations.

Our industry already operates under more than 20 federal regulations all intended to address the issues surrounding the transfer and protection of customer information. The most prominent ones for the banks are:

- Gramm-Leach-Bliley Act of 1999
- Fair and Accurate Credit Transactions Act of 2003
- Fair Credit Reporting Act
- The Electronic Fund Transfer Act
- The Right to Financial Privacy Act
- The Telephone Consumer Protection Act

This binder is one of our desk references for "Safeguarding Customer Information"

Most relevant to the discussion on HB65 is **Section V of the Gramm-Leach-Bliley Act,** and the **Fair and Accurate Credit Transactions Act..or FACT Act.**

The FACT Act was a complex piece of federal legislation passed in November of 2003 that involved the efforts of the American Bankers Association, The Credit Union National Association, the Federal Reserve, The Securities and Exchange Commission and the Federal Trade Commission. This ACT addressed several key issues:

- Provided for the full and permanent reauthorization of seven existing key national uniformity provisions
- Added two national uniformity provisions for identity theft prevention measures
- Established permanent preemption of state law related to the nine uniformity provisions which were:
    - Fraud alerts
    - Red flag guidelines
    - Blocking of information resulting from identity theft
    - The truncation of credit card and debit card account numbers
    - The truncation of Social Security Numbers
    - Prohibition of the sale or transfer of debt caused by identity theft
    - Notice by debt collectors of fraudulent information
    - Coordination of identity theft complaint investigations
    - Prevention of re-pollution of consumer reports
- The Act also acknowledged the states' ability to address matters outside of these nine areas of national uniformity such as laws governing the sale or use of SSN's, alerts for database hacking and increased penalties for identity theft.

The point to be made is simply to assure the committee and those working on this bill, that the financial services industry is fully engaged in this process. At the very core of our industry is "**customer confidence**" with a common commitment to our customers to protect their financial resources and their privacy while meeting their expectations for service.

The Alaska Bankers Association has reviewed HB 65, and reduced our recommended changes to three amendments as outlined in Mr. Lawer's letter. We believe these changes will enable financial institutions to protect the privacy of our customers without inhibiting our ability to provide our customers with the benefits resulting from the responsible transfer of information – i.e. fraud protection, quick credit approvals and convenient ATM services

The first amendment addresses the need for consistent security breach requirements;

- On page 2, line 13, after "breach," insert:

  "made a reasonable determination at to whether misuse of the information has occurred or is likely to occur, and if so,"

- On page 3, strike lines 23 and 24 in their entirety
- On page 3, line 25, strike "(d)" and insert "(c)" in its place.
- On page 6, between lines 14 and 15, insert an entirely new section as follows:

  "**Sec. 45.48.095. Exemption.** This chapter does not apply to an information collector who is subject to 15 U.S.C. 6801-6827 (Gramm-Leach-Bliley Financial Modernization Act)."

The second amendment suggests language so that restrictions on the use of the SSN# would not inadvertently inhibit an institution to protect the customer;

- On page 19, strike lines 24 – 31 in their entirety.
- On page 20, strike lines 1- 18 in their entirety.
- In their place insert the following:

Sec. 45.48.420. Sale, lease, loan, trade, rental or disclosure. A person may not sell, lease, loan, trade, rent or otherwise intentionally disclose an individual's social security number to a third party unless (i) the person or entity has the written consent to the disclosure from the individual, or (ii) the disclosure is required or authorized by federal or state law. Nothing in this paragraph prohibits the sale,

transfer or disclosure of an individual's Social Security number to a third party if the sale, transfer or disclosure has no independent economic value and is incidental to a larger transaction and is necessary for the purpose of verifying the identity of the individual.

The third amendment offers language to conform this section to federal law and other state laws to prevent abuse of this provision.

On page 17, replace lines 25-26 with the following:

"...immediately (1) initiate an investigation in to the accuracy of such information, (2) indicate that the accuracy of such information has been disputed in any subsequent consumer report containing such information pending completion of the reinvestigation; and, if such information cannot be reverified within thirty days, correct or delete such information in any subsequent consumer reports."

So on behalf of the Alaska Bankers Association, I would urge the committee to consider these amendments as presented.

Thank you for the opportunity to comment on this bill.

Craig E. Dahl, President & CEO
Alaska Pacific Bank

790-5101

FISCAL NOTE

STATE OF ALASKA
2008 LEGISLATIVE SESSION

Fiscal Note Number:
Bill Version: CSHB 65(JUD)
() Publish Date:

Identifier (file name): CSHB065(JUD)-GOV-OMB-1-21-08
Title: Security Breaches -- Identity Theft
Sponsor: Rep. Coghill
Requester: House Finance Committee

Dept. Affected: All
RDU
Component
Component Number

Expenditures/Revenues (Thousands of Dollars)

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

	Appropriation Required	Information					
OPERATING EXPENDITURES	**FY 2009**	**FY 2009**	**FY 2010**	**FY 2011**	**FY 2012**	**FY 2013**	**FY 2014**
Personal Services							
Travel							
Contractual							
Supplies							
Equipment							
Land & Structures							
Grants & Claims							
Miscellaneous							
TOTAL OPERATING	...		...	...	...	...	...
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 Interagency Receipts							
TOTAL	...		...	...	...	...	...

Estimate of any current year (FY2008) cost:

POSITIONS

Full-time							
Part-time							
Temporary							

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

This legislation establishes a number of requirements and penalties relating to the protection and disclosure of personal information, such as social security numbers.

The bill, if enacted in its current form, would establish a provision in Sec. 45.48.480 that allows individuals to sue the state for actual damages, court costs, and full reasonable attorney's fees. Actual damages can include both economic and non-economic damages, such as emotional distress. AS 09.17.010 may cap these non-economic damages at $400,000, but it is unclear whether this cap would apply to a violation of this statute. Whenever a statute creates state liability, the state becomes an attractive target for litigation. It is reasonable to expect that plaintiffs, either individually or through class actions, will bring claims against the state whenever a state agency violates this section. (continued)

Prepared by: Jack Kreinheder, Senior Analyst — Phone 465-4676
Division: Office of Management and Budget — Date/Time 1/21/08 3:32 PM
Approved by: Karen J. Rehfeld, Director — Date 1/21/2008
Office of Management and Budget

(Revised 11/19/2007 OMB)

ANALYSIS CONTINUATION

Although the State is pursuing all prudent and practical security measures to protect personal information, it is possible that despite these security measures, a security breach could occur that would result in disclosure of over 500,000 records containing individual social security numbers. Under this scenario, the State's exposure to non-economic damages alone is **$200 billion**. Even if such a claim were settled at a penny on the dollar, the State's exposure is **$2 billion**. In addition, the State is also subject to an award of unlimited economic damages, costs, and full attorneys fees. The cost to defend these cases will also be substantial.

Several State agencies are required, in order to provide necessary services to Alaskans, to maintain databases containing personal information on hundreds of thousands of Alaskans. In some cases, these databases contain historical information that includes personal information on millions of people. Agencies that are required to maintain databases on large numbers of Alaskans include the Division of Motor Vehicles, the Division of Elections, the Permanent Fund Division, the Department of Health and Social Services, the Department of Public Safety, and the Department of Labor and Workforce Development.

The legislation would also require notification of affected individuals in the event of a security breach resulting in disclosure of personal information. Under a scenario in which the State was required to notify 500,000 individuals by mail, the cost could be as much as $123,000 for postage alone, plus any overtime and/or contractual assistance required to determine the affected individuals and locate current addresses.

FISCAL NOTE

STATE OF ALASKA
2008 LEGISLATIVE SESSION

Fiscal Note Number:
Bill Version: CSHB 65(JUD
() Publish Date:

Identifier (file name): CSHB65(JUD)-DOR-PFD-1-21-08
Dept. Affected: Revenue
Title: Personal Information & Consumer Credit
RDU: Permanent Fund Dividend Division
Component: Permanent Fund Dividend Division
Sponsor: Reps. Coghill, Gara
Requester: House Finance Committee
Component Number: 981

Expenditures/Revenues (Thousands of Dollars)

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

	Appropriation Required	Information					
OPERATING EXPENDITURES	**FY 2009**	**FY 2009**	**FY 2010**	**FY/2011**	**FY 2012**	**FY 2013**	**FY 2014**
Personal Services	50.0	0.0	50.0	50.0	50.0	50.0	50.0
Travel	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Contractual	75.0	0.0	25.0	25.0	25.0	25.0	25.0
Supplies	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Equipment	2.0	0.0	2.0	2.0	2.0	2.0	2.0
Land & Structures	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Grants & Claims	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Miscellaneous	0.0	0.0	0.0	0.0	0.0	0.0	0.0
TOTAL OPERATING	**127.0**	**0.0**	**77.0**	**77.0**	**77.0**	**77.0**	**77.0**
CAPITAL EXPENDITURES	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**
CHANGE IN REVENUES ( )	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**

FUND SOURCE (Thousands of Dollars)

1002 Federal Receipts	0.0	0.0	0.0	0.0	0.0	0.0	0.0
1003 GF Match	0.0	0.0	0.0	0.0	0.0	0.0	0.0
1004 GF	0.0	0.0	0.0	0.0	0.0	0.0	0.0
1005 GF/Program Receipts	0.0	0.0	0.0	0.0	0.0	0.0	0.0
1037 GF/Mental Health	0.0	0.0	0.0	0.0	0.0	0.0	0.0
1050 PFD Fund	127.0	0.0	77.0	77.0	77.0	77.0	77.0
TOTAL	**127.0**	**0.0**	**77.0**	**77.0**	**77.0**	**77.0**	**77.0**

Estimate of any current year (FY2008) cost: 97.5

POSITIONS

Full-time	1.0	0.00	1	1	1	1	1
Part-time		0					
Temporary		0					

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

HB65 has 1 primary component related to disclosure of applicant information on Permanent Fund Dividend Applications: Processing requests from requestors of information, verifying that the requester has a license under AS 43.70.020, that the person making the request has provided proof of his/her identity, that the requestor's normal course of business would be covered by the parameters sets forth under AS 43.23.017(b)(1) - (7), and delivery of the requested information or notification that the requestor's elements do not meet the requirements of AS 43.23.017(b).

The division will be required to establish an electronic interface for requestors of applicant information. The division is currently in the process of soliciting bids to determine the cost of establishing an electronic interface, for governmental agencies who already have the right to applicant information under current law.

Prepared by: Amy Skow, Division Manager
Phone 907 465-4784
Division: Permanent Fund Dividend Division
Date/Time 1/18/08 4:00 PM
Approved by: Jerry Burnett
Date 1/21/2008
department of Revenue

(Revised 11/15/2007 OMB)

HB

65

SFIN

FILE

SENATE FINANCE COMMITTEE REPORT

DATE: 4/4/08

FURTHER:

DATE TURNED
IN TO OFFICE: _____

Finance Committee considered CS FOR HOUSE BILL NO. 65(FIN)

HB 65 PERSONAL INFORMATION & CONSUMER CREDIT

"An Act relating to breaches of security involving personal information, credit report and credit score security freezes, protection of social security numbers, care of records, disposal of records, identity theft, credit cards, and debit cards, and to the jurisdiction of the office of administrative hearings; amending Rules 60 and 82, Alaska Rules of Civil Procedure; and providing for an effective date."

and recommends:

[X] be **replaced** with [X] **SCS** or [ ] **CS** HB65 (FIN)

[ ] adopt **previous** [ ] **SCS** or [ ] **CS** _____ (_____)

[ ] attached amendment(s)

[ ] adopt _____ Letter of Intent

[ ] further referral to _____ Committee

SENATE BILL:
[ ] Same Title
[ ] New Title
_____

HOUSE BILL:
[ ] Same Title
[ ] Technical Title Change
[X] New Title w/ SCR #_____

NEW FISCAL NOTE(S):

Department	Date	Fiscal	Indet.	Zero	FN#

PREVIOUS FISCAL NOTE(S):

Department	Date	Fiscal	Indet.	Zero	FN#
GOV	2/20/08		✓		3
ADM	2/14/08	✓			5

[ ] **APPROPRIATION - no fiscal note**

SIGNATURES AND RECOMMENDATIONS:	PRINTED LAST NAME	DO PASS	DO NOT PASS	NO REC	AMEND
	Elton	✓			
	Thomas	✓			
	OLSON			✓	
	Huggins	✓			
CO-CHAIR:	Hoffman			✓	
CO-CHAIR:	STEVENS			✓	

FISCAL NOTE

STATE OF ALASKA
2008 LEGISLATIVE SESSION

Fiscal Note Number: 5
Bill Version: SCS CSHB 65(L&C)
(S) Publish Date: 3/19/08

Identifier (file name): HB065CS(JUD)-DOA-ETS-2-14-08
Title "An Act Relating to Breaches of Security Involving..."
Sponsor Reps. Coghill, Gara
Requester

Dept. Affected: Administration
RDU Enterprise Technology Services
Component Enterprise Technology Services
Component Number 2082

Expenditures/Revenues (Thousands of Dollars)

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

	Appropriation Required	Information					
OPERATING EXPENDITURES	**FY 2009**	**FY 2009**	**FY 2010**	**FY 2011**	**FY 2012**	**FY 2013**	**FY 2014**
Personal Services	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Travel	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Contractual	275.0		319.0	319.0	319.0	319.0	319.0
Supplies	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Equipment	1,765.6	0.0	0.0	0.0	0.0	0.0	0.0
Land & Structures	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Grants & Claims	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Miscellaneous	0.0	0.0	0.0	0.0	0.0	0.0	0.0
TOTAL OPERATING	**2,040.6**	**0.0**	**319.0**	**319.0**	**319.0**	**319.0**	**319.0**
CAPITAL EXPENDITURES (GF)		**2,000.0**					
CHANGE IN REVENUES ( )							

FUND SOURCE (Thousands of Dollars)

1002 Federal Receipts							
1003 GF Match							
1004 GF	2,040.6		319.0	319.0	319.0	319.0	319.0
1005 GF/Program Receipts							
1037 GF/Mental Health							
Other Interagency Receipts							
TOTAL	**2,040.6**	**0.0**	**319.0**	**319.0**	**319.0**	**319.0**	**319.0**

Estimate of any current year (FY2008) cost: 0.0

POSITIONS

Full-time							
Part-time							
Temporary							

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

HB65 has two primary components related to security breaches: 1) Preventative and 2) Remediation. This fiscal note addresses the Preventative component by providing funding to continue the department's efforts to secure the state's networks and data.

For the past three years, the department has been working on strengthening the security components of our network. We have installed Cisco Security Agent (CSA) on desktop computers and servers throughout the state. We are also working to deploy a demilitarized zone (DMZ) that places all of our databases behind two firewalls, with our public-facing servers deployed between the two firewalls. This effort is scheduled to be completed by June 2009 and will involve the coordinated efforts of all state departments.

Prepared by: Dave Blaisdell, Deputy Director — Phone (907)465-5094
Division Enterprise Technology Services — Date/Time 2/14/2008
Approved by: Kevin Brooks, Deputy Commissioner — Date 2/14/2008
Department of Administration

(Revised 11/19/2007 OMB)

FISCAL NOTE # 5

STATE OF ALASKA
2007 LEGISLATIVE SESSION

BILL NO. SCS CSHB 65(L&C)

ANALYSIS CONTINUATION

The next phase of this security effort is deployment of encryption hardware and software to protect our network as well as legacy data stored and processed on the state's mainframe computer. This fiscal note will provide funding for security enhancements to insure that data used by state agencies to provide services is secure from known types of attack. This will be an ongoing effort as attackers have become more sophisticated over time.

Previous funding for security efforts is as follows:

FY05 Supplemental $5,002,500
FY06 Capital Project $3,537,500
FY07 Capital Project $2,000,000
FY08 Capital Project $4,400,000

FY09 Capital Project funding of $2,000.0 for network security is included in the Governor's budget.

FISCAL NOTE

STATE OF ALASKA
2008 LEGISLATIVE SESSION

Fiscal Note Number: 3
Bill Version: CSHB 65(FIN)
(H) Publish Date: 2/21/08

Identifier (file name): CSHB065(FIN)-GOV-OMB-2-20-08
Dept. Affected: All
Title: Security Breaches -- Identity Theft
RDU
Component
Sponsor: Rep. Coghill
Requester: House Finance Committee
Component Number

Expenditures/Revenues (Thousands of Dollars)

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

	Appropriation Required	Information					
OPERATING EXPENDITURES	**FY 2009**	**FY 2009**	**FY 2010**	**FY 2011**	**FY 2012**	**FY 2013**	**FY 2014**
Personal Services							
Travel							
Contractual							
Supplies							
Equipment							
Land & Structures							
Grants & Claims							
Miscellaneous							
TOTAL OPERATING	***		***	***	***	***	***
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 Interagency Receipts							
TOTAL	***		***	***	***	***	***

Estimate of any current year (FY2008) cost:

POSITIONS

Full-time							
Part-time							
Temporary							

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

This legislation would expose the State of Alaska to future costs; however, it is not possible to predict these costs with any certainty. Whenever a statute creates state liability, the state becomes an attractive target for litigation. It is reasonable to expect that plaintiffs, either individually or through class actions, will bring claims against the state whenever a state agency violates the provisions of this legislation. Depending on whether (and how many) State security breaches occur, notification costs could range from zero to approximately $1 million per year. State exposure to lawsuits under this bill is unpredictable, but in the event the state is sued, potential costs for actual economic damages sustained by plaintiffs could be in the $200.0 range, plus defense costs.

Prepared by: Jack Kreinheder, Senior Analyst
Phone 465-4676
Division: Office of Management and Budget
Date/Time 2/20/08 10:32 AM
Approved by: Karen J. Rehfeld, Director
Date 2/20/2008
Office of Management and Budget

25-LS0311\F.1
Bannister
4/11/08

Amended

AMENDMENT #1

OFFERED IN THE SENATE BY SENATOR STEDMAN

TO: SCS CSHB 65(FIN), Draft Version "F"

Page 1, line 3, following "**debit cards,**":

Insert "**disclosure of the names and addresses of permanent fund dividend applicants,**"

Page 2, following line 1:

Insert a new bill section to read:

"* **Sec. 2.** AS 43.23.017 is amended by adding a new subsection to read:

(b) Notwithstanding (a) of this section, the department may release the names and addresses of permanent fund dividend applicants to a legislator of this state and to the legislator's office staff." for official use.

Renumber the following bill sections accordingly.

Page 30, line 6:

Delete "sec. 3"

Insert "sec. 4"

Page 30, line 10:

Delete "sec. 3"

Insert "sec. 4"

Page 30, line 19:

Delete "sec. 3"

Insert "sec. 4"

Page 30, line 21:

Delete "Section 6"

Insert "Section 7"

Page 30, line 22:

Delete "secs. 7 and 8"

Insert "secs. 8 and 9"

Amend. pg 4

Adopted 4/11/08

25-LS0311\F
Bannister
4/10/08

SENATE CS FOR CS FOR HOUSE BILL NO. 65(FIN)

IN THE LEGISLATURE OF THE STATE OF ALASKA

TWENTY-FIFTH LEGISLATURE - SECOND SESSION

BY THE SENATE FINANCE COMMITTEE

Offered:
Referred:

Sponsor(s): REPRESENTATIVES COGHILL AND GARA, Hawker, Lynn, Samuels, Fairclough, Ramras, Kawasaki, Kerttula, Gatto, Neuman, Olson, Dahlstrom, Gardner, Johnson, Wilson, Guttenberg, Holmes, Nelson, Crawford, LeDoux, Keller, Doogan, Buch, Roses, Cissna, Meyer

SENATORS Therriault, Wilken

A BILL

FOR AN ACT ENTITLED

"An Act relating to breaches of security involving personal information, credit report and credit score security freezes, protection of social security numbers, care of records, disposal of records, identity theft, credit cards, and debit cards, and to the jurisdiction of the office of administrative hearings; amending Rules 60 and 82, Alaska Rules of Civil Procedure; and providing for an effective date."

BE IT ENACTED BY TI E LEGISLATURE OF THE STATE OF ALASKA:

*** Section 1.** AS 40.21.110 is amended to read:

Sec. 40.21.110. Care of records. Except for public records lawfully in the possession of a person other than the state, public records of existing or defunct agencies of the state, territorial, and Russian governments in Alaska are the property of the state and shall be created, maintained, preserved, stored, transferred, destroyed or disposed of, and otherwise managed in accordance with the provisions of this chapter and AS 45.48.500 - 45.48.530. Records shall be delivered by outgoing officials and employees to their successors, and may not be removed, destroyed or

disposed of, except as provided in this chapter **and AS 45.48.500 - 45.48.530**.

* Sec. 2. AS 44.64.030(a) is amended by adding a new paragraph to read:

(40) AS 45.48.080(c) (breach of security involving personal information).

* Sec. 3. AS 45 is amended by adding a new chapter to read:

Chapter 48. Personal Information Protection Act.

Article 1. Breach of Security Involving Personal Information.

Sec. 45.48.010. Disclosure of breach of security. (a) If a covered person owns or licenses personal information in any form that includes personal information on a state resident, and a breach of the security of the information system that contains personal information occurs, the covered person shall, after discovering or being notified of the breach, disclose the breach to each state resident whose personal information was subject to the breach.

(b) An information collector shall make the disclosure required by (a) of this section in the most expeditious time possible and without unreasonable delay, except as provided in AS 45.48.020 and as necessary to determine the scope of the breach and restore the reasonable integrity of the information system.

(c) Notwithstanding (a) of this section, disclosure is not required if, after an appropriate investigation or after written notification to the attorney general of this state, the covered person determines that there is not a reasonable likelihood that harm to the consumers whose personal information has been acquired has resulted or will result from the breach. The determination shall be documented in writing and the documentation shall be maintained for five years.

Sec. 45.48.020. Allowable delay in notification. An information collector may delay disclosing the breach under AS 45.48.010 if an appropriate law enforcement agency determines that disclosing the breach will interfere with a criminal investigation. However, the information collector shall disclose the breach to the state resident in the most expeditious time possible and without unreasonable delay after the law enforcement agency informs the information collector in writing that disclosure of the breach will no longer interfere with the investigation.

Sec. 45.48.030. Methods of notice. An information collector shall make the

disclosure required by AS 45.48.010

(1) by a written document sent to the most recent address the information collector has for the state resident;

(2) by electronic means if the information collector's primary method of communication with the state resident is by electronic means, or if making the disclosure by the electronic means is consistent with the provisions regarding electronic records and signatures required for notices legally required to be in writing under 15 U.S.C. 7001 et seq. (Electronic Signatures in Global and National Commerce Act); or

(3) if the information collector demonstrates that the cost of providing notice would exceed $150,000, that the affected class of state residents to be notified exceeds 300,000, or that the information collector does not have sufficient contact information to provide notice, by

(A) electronic mail if the information collector has an electronic mail address for the state resident;

(B) conspicuously posting the disclosure on the Internet website of the information collector if the information collector maintains an Internet site; and

(C) providing a notice to major statewide media.

Sec. 45.48.040. Notification of certain other agencies. (a) If an information collector is required by AS 45.48.010 to notify more than 1,000 state residents of a breach, the information collector shall also notify without unreasonable delay all consumer credit reporting agencies that compile and maintain files on consumers on a nationwide basis and provide the agencies with the timing, distribution, and content of the notices to state residents.

(b) This section may not be construed to require the information collector to provide the consumer reporting agencies identified under (a) of this section with the names or other personal information of the state residents whose personal information was subject to the breach.

(c) This section does not apply to an information collector who is subject to the Gramm-Leach-Bliley Financial Modernization Act.

Amendment 2

(d) In this section, "consumer reporting agency that compiles and maintains files on consumers on a nationwide basis" has the meaning given in 15 U.S.C. 1681a(p).

Sec. 45.48.050. Exception for employees and agents. In AS 45.48.010 - 45.48.090, the good faith acquisition of personal information by an employee or agent of an information collector for a legitimate purpose of the information collector is not a breach of the security of the information system if the employee or agent does not use the personal information for a purpose unrelated to a legitimate purpose of the information collector and does not make further unauthorized disclosure of the personal information.

Sec. 45.48.060. Waivers. A waiver of AS 45.48.010 - 45.48.090 is void and unenforceable.

Sec. 45.48.070. Treatment of certain breaches. (a) If a breach of the security of the information system containing personal information on a state resident that is maintained by an information recipient occurs, the information recipient is not required to comply with AS 45.48.010 - 45.48.030. However, immediately after the information recipient discovers the breach, the information recipient shall notify the information distributor who owns the personal information or who licensed the use of the personal information to the information recipient about the breach and cooperate with the information distributor as necessary to allow the information distributor to comply with (b) of this section. In this subsection, "cooperate" means sharing with the information distributor information relevant to the breach, except for confidential business information or trade secrets.

(b) If an information recipient notifies an information distributor of a breach under (a) of this section, the information distributor shall comply with AS 45.48.010 - 45.48.030 as if the breach occurred to the information system maintained by the information distributor.

Sec. 45.48.080. Violations. (a) If an information collector who is a governmental agency violates AS 45.48.010 - 45.48.090 with regard to the personal information of a state resident, the information collector

(1) is liable to the state for a civil penalty of up to $500 for each state

resident who was not notified under AS 45.48.010 - 45.48.090, but the total civil penalty may not exceed $50,000; and

(2) may be enjoined from further violations.

(b) If an information collector who is not a governmental agency violates AS 45.48.010 - 45.48.090 with regard to the personal information of a state resident, the violation is an unfair or deceptive act or practice under AS 45.50.471 - 45.50.561. However,

(1) the information collector is not subject to the civil penalties imposed under AS 45.50.531 but is liable to the state for a civil penalty of up to $500 for each state resident who was not notified under AS 45.48.010 - 45.48.090, except that the total civil penalty may not exceed $50,000; and

(2) damages that may be awarded against the information collector under

(A) AS 45.50.531 are limited to actual economic damages that do not exceed $500; and

(B) AS 45.50.537 are limited to actual economic damages.

(c) The Department of Administration may enforce (a) of this section against a governmental agency. The procedure for review of an order or action of the department under this subsection is the same as the procedure provided by AS 44.62 (Administrative Procedure Act), except that the office of administrative hearings (AS 44.64.010) shall conduct the hearings in contested cases and the decision may be appealed under AS 44.64.030(c).

Sec. 45.48.090. Definitions. In AS 45.48.010 - 45.48.090,

(1) "breach of the security" means unauthorized acquisition, or reasonable belief of unauthorized acquisition, of personal information that compromises the security, confidentiality, or integrity of the personal information maintained by the information collector; in this paragraph, "acquisition" includes acquisition by

(A) photocopying, facsimile, or other paper-based method;

(B) a device, including a computer, that can read, write, or store information that is represented in numerical form; or

(C) a method not identified by (A) or (B) of this paragraph;

(2) "covered person" means a

(A) person doing business;

(B) a governmental agency; or

(C) a person with more than 10 employees;

(3) "governmental agency" means a state or local governmental agency, except for an agency of the judicial branch;

(4) "information collector" means a covered person who owns or licenses personal information in any form if the personal information includes personal information on a state resident;

(5) "information distributor" means a person who is an information collector and who owns or licenses personal information to an information recipient;

(6) "information recipient" means a person who is an information collector but who does not own or have the right to license to another information collector the personal information received by the person from an information distributor;

(7) "personal information" means information in any form on an individual that is not encrypted or redacted, or is encrypted and the encryption key has been accessed or acquired, and that consists of a combination of

(A) an individual's name; in this subparagraph, "individual's name" means a combination of an individual's

(i) first name or first initial; and

(ii) last name; and

(B) one or more of the following information elements:

(i) the individual's social security number;

(ii) the individual's driver's license number or state identification card number;

(iii) except as provided in (iv) of this subparagraph, the individual's account number, credit card number, or debit card number;

(iv) if an account can only be accessed with a personal code, the number in (iii) of this subparagraph and the personal code; in

this sub-subparagraph, "personal code" means a security code, an access code, a personal identification number, or a password;

(v) passwords, personal identification numbers, or other access codes for financial accounts.

Article 2. Credit Report and Credit Score Security Freeze.

Sec. 45.48.100. Security freeze authorized. A consumer may prohibit a consumer credit reporting agency from releasing the consumer's credit report or credit score without the express authorization of the consumer by placing a security freeze on the consumer's credit report.

Sec. 45.48.110. Placement of security freeze. (a) To place a security freeze, a consumer shall make the request to the consumer credit reporting agency

(1) by mail to the address designated by the consumer credit reporting agency to receive security freeze requests; or

(2) as allowed by (b) of this section.

(b) A consumer may make a request under (a) of this section by telephone or by fax, the Internet, or other electronic media if the consumer credit reporting agency has developed procedures for using the telephone or an electronic medium to receive and process the request in an expedited manner.

(c) A consumer credit reporting agency shall place a security freeze within five business days after receiving a request under (a) or (b) of this section and proper identification from the consumer.

Sec. 45.48.120. Confirmation of security freeze. (a) Within 10 business days after a consumer makes the request under AS 45.48.110, a consumer credit reporting agency shall send a written confirmation of the placement of the security freeze to the consumer. The confirmation must also inform the consumer that the consumer credit reporting agency may charge, as allowed by AS 45.48.160, a fee for third-party access during the security freeze.

(b) At the same time that the consumer credit reporting agency sends a confirmation under (a) of this section, the consumer credit reporting agency shall provide the consumer with a unique personal identification number, password, or similar device to be used by the consumer when the consumer authorizes the release of

the consumer's credit report or credit score under AS 45.48.130.

Sec. 45.48.130. Access and actions during security freeze. (a) While a security freeze is in place, a consumer credit reporting agency shall allow a third party access to a consumer's credit report or credit score if the consumer requests that the consumer credit reporting agency allow the access.

(b) To make a request under (a) of this section, the consumer shall contact the consumer credit reporting agency by mail at the address designated by the consumer credit reporting agency to receive security freeze requests or as allowed by (c) of this section, authorize the consumer credit reporting agency to allow the access, and provide the consumer credit reporting agency with

(1) proper identification to verify the consumer's identity;

(2) the unique personal identification number, password, or similar device provided under AS 45.48.120(b); and

(3) the proper information necessary to identify the third party to whom the consumer credit reporting agency may allow the access or the time period during which the consumer credit reporting agency may allow the access to third parties who request the access.

(c) In addition to making the request by mail, a consumer may make a request under (a) of this section by telephone or by fax, the Internet, or other electronic media if the consumer credit reporting agency has developed procedures for using the telephone or an electronic medium to receive and process the request in an expedited manner.

(d) Except as provided by (e) of this section, a consumer credit reporting agency that receives a request from a consumer under (b) or (c) of this section shall comply with the request within 15 minutes after receiving the request by telephone or by an electronic medium or within three business days after receiving the request by mail.

(e) A consumer credit reporting agency is not required to comply with a request under (a) of this section within the 15 minutes required by (d) of this section if

(1) the consumer fails to satisfy the requirements of (b) of this section;

(2) one of the following events prevents the consumer credit reporting

agency from removing the security freeze within 15 minutes:

(A) an act of God, including a fire, earthquake, hurricane, storm, or similar natural disaster or phenomenon;

(B) an unauthorized or illegal act by another person, including terrorism, sabotage, riot, vandalism, labor strike, labor dispute disrupting operations, or similar occurrence;

(C) an operational interruption, including an electrical failure, unanticipated delay in equipment or replacement part delivery, computer hardware or software failure inhibiting response time, or similar disruption;

(D) governmental action, including an emergency order or regulation, a judicial law enforcement action, or a similar directive;

(E) regularly scheduled maintenance during other than normal business hours of the consumer credit reporting agency's systems, or updates to the consumer credit reporting agency's systems;

(F) commercially reasonable maintenance of, or repair to, the consumer credit reporting agency's systems that is unexpected or unscheduled; or

(3) the request is received outside of normal business hours.

(f) If a security freeze is in place, a consumer credit reporting agency may not release the credit report or credit score to a third party without the prior express authorization of the consumer.

(g) If a security freeze is in place on a consumer's credit report and credit score and if a third party applies to a consumer credit reporting agency to provide the third party with access to the consumer's credit report or credit score, the consumer credit reporting agency and the third party may treat the third party's application as incomplete unless the consumer authorizes the access under (a) of this section.

(h) If a security freeze is in place, a consumer credit reporting agency may not change the consumer's official information in the consumer's credit report and credit score without sending a written statement of the change to the consumer within 30 days after the change is made. A consumer credit reporting agency is not required to send a written statement if the consumer credit reporting agency makes a technical

change in the consumer's official information. If a consumer credit reporting agency makes a change, other than a technical change, in a consumer's address, the consumer credit reporting agency shall send the written statement to the consumer at both the new address and the former address. In this subsection,

(1) "official information" means name, birth date, social security number, and address;

(2) "technical change" means changing spelling, transposing numbers or letters, abbreviating a word, or spelling out an abbreviation.

(i) This section is not intended to prevent a consumer credit reporting agency from advising a third party that requests access to a consumer's credit report or credit score that a security freeze is in effect.

(j) The procedures used by a consumer credit reporting agency for implementing the provisions of this section may include the use of telephone, facsimile, or electronic means if making the disclosure by the electronic means is consistent with the provisions regarding electronic records and signatures required for notices legally required to be in writing under 15 U.S.C. 7001 et seq. (Electronic Signatures in Global and National Commerce Act).

Sec. 45.48.140. Removal of security freeze. (a) Except as provided by AS 45.48.130, a consumer credit reporting agency may not remove a security freeze unless

(1) the consumer requests that the consumer credit reporting agency remove the security freeze under (b) of this section; or

(2) the consumer made a material misrepresentation of fact to the consumer credit reporting agency when the consumer requested the security freeze under AS 45.48.110; if a consumer credit reporting agency intends to remove a security freeze on a consumer's credit report under this paragraph, the consumer credit reporting agency shall notify the consumer in writing before removing the security freeze.

(b) A consumer credit reporting agency shall remove a security freeze within three business days after receiving a request for removal from the consumer who requested the security freeze.

(c) To make a request under (b) of this section, the consumer shall contact the consumer credit reporting agency by mail or as allowed by (d) of this section, authorize the consumer credit reporting agency to remove the security freeze, and provide the consumer credit reporting agency with

(1) proper identification to verify the consumer's identity; and

(2) the unique personal identification number, password, or similar device provided under AS 45.48.120(b).

(d) In addition to mail, a consumer may make a request under (b) of this section by telephone or by fax, the Internet, or other electronic media if the consumer credit reporting agency has developed procedures for using the telephone or an electronic medium to receive and process the request in an expedited manner.

Sec. 45.48.150. Prohibition. When dealing with a third party, a consumer credit reporting agency may not suggest, state, or imply that a consumer's security freeze reflects a negative credit score, history, report, or rating.

Sec. 45.48.160. Charges. (a) Except as provided by (b), (c), or (d) of this section, a consumer credit reporting agency may not charge a consumer to place or remove a security freeze, to provide access under AS 45.48.130, or to take any other action, including the issuance of a personal identification number, password, or similar device under AS 45.48.120, that is related to the placement of, removal of, or allowing access to a credit report or credit score on which a security freeze has been placed.

(b) A consumer credit reporting agency may charge a consumer $5 for placing a security freeze.

(c) A consumer credit reporting agency may charge the consumer $2 for each access request made by the consumer. In this subsection, "access request" means a request made by the consumer under AS 45.48.130 to allow third-party access to the consumer's credit report or credit score on which a security freeze has been placed.

(d) If a consumer fails to retain a personal identification number, password, or similar device issued under AS 45.48.120, a consumer credit reporting agency may charge the consumer up to $5 for each time after the first time that the consumer credit reporting agency issues the consumer another personal identification number, password, or similar device because the consumer failed to retain the personal

identification number, password, or similar device.

(e) A consumer credit reporting agency may not charge a consumer a fee under (b) or (c) of this section if the consumer has been a victim of identity theft and provides the consumer credit reporting agency with a complaint filed by the consumer with a law enforcement agency.

Sec. 45.48.170. Notice of rights. When a consumer credit reporting agency is required to give a consumer a summary of rights under 15 U.S.C. 1681g of the Fair Credit Reporting Act, a consumer credit reporting agency shall also give the consumer the following notice:

Consumers Have the Right to Obtain a Security Freeze

You may obtain a security freeze on your credit report and credit score for $5 to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may not have to pay the $5 charge if you are a victim of identity theft. You have a right to place a security freeze on your credit report and credit score under state law (AS 45.48.100 - 45.48.290).

The security freeze will prohibit a consumer credit reporting agency from releasing your credit score and any information in your credit report without your express authorization or approval.

The security freeze is designed to prevent credit, loans, and other services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report and credit score may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, a mortgage, a governmental service, a governmental payment, a cellular telephone, a utility, an Internet credit card application, an extension of credit at point of sale, and other items and services.

When you place a security freeze on your credit report and credit score, within 10 business days you will be provided a personal

identification number, password, or similar device to use if you choose to remove the freeze on your credit report and credit score or to temporarily authorize the release of your credit report and credit score to a specific third party or specific third parties or for a specific period of time after the freeze is in place. To provide that authorization, you must contact the consumer credit reporting agency and provide all of the following:

(1) proper identification to verify your identity;

(2) the personal identification number, password, or similar device provided by the consumer credit reporting agency;

(3) proper information necessary to identify the third party or third parties who are authorized to receive the credit report and credit score or the specific period of time for which the credit report and credit score are to be available to third parties.

A consumer credit reporting agency that receives your request to temporarily lift a freeze on a credit report and credit score is required to comply with the request within 15 minutes, except after normal business hours and under certain other conditions, after receiving your request if you make the request by telephone, or an electronic method if the agency provides an electronic method, or within three business days after receiving your request if you make the request by mail. The consumer credit reporting agency may charge you $2 to temporarily lift the freeze.

A security freeze does not apply to circumstances where you have an existing account relationship and a copy of your credit report and credit score are requested by your existing creditor or its agents or affiliates for certain types of account review, collection, fraud control, or similar activities.

If you are actively seeking credit, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either

completely if you are shopping around, or specifically for a certain creditor, days before applying for new credit.

You have a right to bring a civil action against someone who violates your rights under these laws on security freezes. The action can be brought against a consumer credit reporting agency.

Sec. 45.48.180. Notification after violation. If a consumer credit reporting agency violates a security freeze by releasing a consumer's credit report or credit score, the consumer credit reporting agency shall notify the consumer within five business days after discovering or being notified of the release, and the information in the notice must include an identification of the information released and of the third party who received the information.

Sec. 45.48.190. Resellers. A consumer credit reporting agency that acts as a reseller of consumer information shall honor a security freeze placed on a consumer's credit report and credit score by another consumer credit reporting agency.

Sec. 45.48.200. Violations and penalties. (a) A consumer who suffers damages as a result of a person's violation of AS 45.48.100 - 45.48.290 may bring an action in court against the person and recover, in the case of a violation where the person acted

(1) negligently, actual economic damages, court costs allowed by the rules of court, and full reasonable attorney fees;

(2) knowingly,

(A) damages as described in (1) of this subsection;

(B) punitive damages that are not less than $100 nor more than $5,000 for each violation as the court determines to be appropriate; and

(C) other relief that the court determines to be appropriate.

(b) A consumer may bring an action in court against a person for a violation or threatened violation of AS 45.48.100 - 45.48.290 for injunctive relief, whether or not the consumer seeks another remedy under this section.

(c) Notwithstanding (a)(2) of this section, a person who knowingly violates AS 45.48.100 - 45.48.290 is liable in a class action for an amount that the court allows. When determining the amount of an award in a class action under this

subsection, the court shall consider, among the relevant factors, the amount of any actual damages awarded, the frequency of the violations, the resources of the violator, and the number of consumers adversely affected.

(d) In this section, "knowingly" has the meaning given in AS 11.81.900.

Sec. 45.48.210. Exemptions. (a) The provisions of AS 45.48.100 - 45.48.290 do not apply to the use of a credit report by

(1) a person, the person's subsidiary, affiliate, or agent, or the person's assignee with whom a consumer has or, before the assignment, had an account, contract, or debtor-creditor relationship if the purpose of the use is to review the consumer's account or to collect a financial obligation owing on the account, contract, or debt;

(2) a subsidiary, an affiliate, an agent, an assignee, or a prospective assignee of a person to whom access has been granted under AS 45.48.130 if the purpose of the use is to facilitate the extension of credit or another permissible use;

(3) a person acting under a court order, warrant, or subpoena;

(4) an agency of a state or municipality that administers a program for establishing and enforcing child support obligations;

(5) the Department of Health and Social Services, its agents, or its assigns when investigating fraud;

(6) the Department of Revenue, its agents, or its assigns when investigating or collecting delinquent taxes or unpaid court orders or when implementing its other statutory responsibilities;

(7) a person if the purpose of the use is prescreening allowed under 15 U.S.C. 1681b(c) of the Fair Credit Reporting Act;

(8) a person administering a credit file monitoring subscription service to which the consumer has subscribed;

(9) a person providing a consumer with a copy of the consumer's credit report or credit score at the consumer's request;

(10) a person if the data base or file of the consumer credit reporting agency consists entirely of information concerning and used solely for one or more of the following purposes:

(A) criminal record information;

(B) personal loss history information;

(C) fraud prevention or detection;

(D) tenant screening; or

(E) employment screening; or

(11) a person for use for insurance purposes in setting a rate, adjusting a rate, adjusting a claim, or underwriting, except that this paragraph may not be interpreted to authorize an insurance practice that is prohibited by other law; this paragraph may not be interpreted to affect AS 21.36.460 or AS 21.39.035.

(b) Except as provided by AS 45.48.190, the provisions of AS 45.48.100 - 45.48.290 do not apply to a person when acting only as a reseller of consumer information.

Sec. 45.48.290. Definitions. In AS 45.48.100 - 45.48.290,

(1) "account review" means activities related to account maintenance, account monitoring, credit line increases, and account upgrades and enhancements;

(2) "consumer" means an individual who is the subject of a credit report or credit score;

(3) "consumer credit reporting agency" has the meaning given in AS 45.48.990, but does not include a person who issues reports

(A) on incidents of fraud or authorizations for the purpose of approving or processing negotiable instruments, electronic funds transfers, or similar methods of payments; or

(B) regarding account closures because of fraud, substantial overdrafts, automated teller machine abuse, or similar negative information regarding a consumer to inquiring banks or other financial institutions for use only in reviewing consumer requests for deposit accounts at the inquiring banks or financial institutions;

(4) "reseller of consumer information" means a person who assembles and merges information contained in the data bases of consumer credit reporting agencies and does not maintain a permanent data base of consumer information from which new consumer credit reports are produced;

(5) "security freeze" means a prohibition against a consumer credit reporting agency's releasing a consumer's credit report or credit score without the express authorization of the consumer;

(6) "third party" means a person who is not

(A) the consumer who is the subject of the consumer's credit report or credit score; or

(B) the consumer credit reporting agency that is holding the consumer's credit report or credit score.

Article 3. Protection of Social Security Number.

Sec. 45.48.400. Use of social security number. (a) A person may not

(1) intentionally communicate or otherwise make available to the general public an individual's social security number;

(2) print an individual's social security number on a card required for the individual to access products or services provided by the person;

(3) require an individual to transmit the individual's social security number over the Internet unless the Internet connection is secure or the social security number is encrypted;

(4) require an individual to use the individual's social security number to access an Internet site unless a password, a unique personal identification number, or another authentication device is also required to access the site; or

(5) print an individual's social security number on material that is mailed to the individual unless

(A) local, state, or federal law, including a regulation adopted under AS 45.48.470, expressly authorizes placement of the social security number on the material; or

(B) the social security number is included on an application or other form, including a document sent as a part of an application process or an enrollment process, sent by mail to establish, amend, or terminate an account, a contract, or a policy, or to confirm the accuracy of the social security number; however, a social security number allowed to be mailed under this subparagraph may not be printed, in whole or in part, on a postcard or other

mailer that does not require an envelope, or in a manner that makes the social security number visible on the envelope or without the envelope's being opened.

(b) The prohibitions in (a) of this section do not apply if the person is engaging in the business of government and

(1) is authorized by law to communicate or otherwise make available to the general public the individual's social security number; or

(2) the communicating or otherwise making available of the individual's social security number is required for the performance of the person's duties or responsibilities as provided by law.

Sec. 45.48.410. Request and collection. (a) A person who does business in the state, including the business of government, may not request or collect from an individual the individual's social security number. This subsection does not prohibit a person from asking for another form of identification from the individual.

(b) The prohibition in (a) of this section does not apply

(1) if the person is authorized by local, state, or federal law, including a regulation adopted under AS 45.48.470, to demand proof of the individual's social security number, to request or collect the individual's social security number, or to submit the individual's social security number to the local, state, or federal government;

(2) if the person is engaging in the business of government and

(A) is authorized by law to request or collect the individual's social security number; or

(B) the request or collection of the individual's social security number is required for the performance of the person's duties or responsibilities as provided by law;

(3) to a person subject to or a transaction regulated by the Gramm-Leach-Bliley Financial Modernization Act for a purpose authorized by the Gramm-Leach-Bliley Financial Modernization Act;

(4) to a person subject to or a transaction regulated by the Fair Credit Reporting Act for a purpose authorized by the Fair Credit Reporting Act;

(5) if the request or collection is for a background check on the individual, for fraud prevention, for medical treatment, for law enforcement or other government purposes, for the individual's employment, including employment benefits, or for verification of the individual's age;

(6) if the request or collection does not have independent economic value, is incidental to a larger transaction or a larger anticipated transaction, and is necessary to verify the identity of the individual;

(7) to an insurer regulated by AS 21; in this paragraph, "insurer" has the meaning given in AS 21.90.900; or

(8) to a hospital service corporation or a medical service corporation regulated under AS 21.87; in this paragraph, "hospital service corporation" and "medical service corporation" have the meanings given in AS 21.87.330.

Sec. 45.48.420. Sale, lease, loan, trade, or rental. (a) A person may not sell, lease, loan, trade, or rent an individual's social security number to a third party.

(b) The prohibition in (a) of this section does not apply if the sale, lease, loan, trade, or rental is

(1) authorized by local, state, or federal law, including a regulation adopted under AS 45.48.470;

(2) by a person subject to or for a transaction regulated by the Gramm-Leach-Bliley Financial Modernization Act for a purpose authorized by the Gramm-Leach-Bliley Financial Modernization Act;

(3) by a person subject to or for a transaction regulated by the Fair Credit Reporting Act for a purpose authorized by the Fair Credit Reporting Act; or

(4) part of a report prepared by a consumer credit reporting agency in response to a request by a person and the person submitted the social security number as part of the request to the consumer credit reporting agency for the preparation of the report.

(c) Nothing in this section prevents a business from transferring social security numbers to another person if the transfer is part of the sale or other transfer of the business to the other person.

(d) A transfer of an individual's social security number for the sole purpose of

identifying a person about whom a report or database check is ordered, received, or provided is not a sale, lease, loan, trade, or rental of a social security number under this section.

(c) A person who knowingly violates (a) of this section is guilty of a class A misdemeanor. In this subsection, "knowingly" has the meaning given in AS 11.81.900.

Sec. 45.48.430. Disclosure. (a) A person doing business, including the business of government, may not disclose an individual's social security number to a third party.

(b) The prohibition in (a) of this section does not apply if

(1) the disclosure is authorized by local, state, or federal law, including a regulation adopted under AS 45.48.470;

(2) the person is engaging in the business of government and

(A) is authorized by law to disclose the individual's social security number; or

(B) the disclosure of the individual's social security number is required for the performance of the person's duties or responsibilities as provided by law;

(3) the disclosure is to a person subject to or for a transaction regulated by the Gramm-Leach-Bliley Financial Modernization Act, and the disclosure is for a purpose authorized by the Gramm-Leach-Bliley Financial Modernization Act or to facilitate a transaction of the individual;

(4) the disclosure is to a person subject to or for a transaction regulated by the Fair Credit Reporting Act, and the disclosure is for a purpose authorized by the Fair Credit Reporting Act;

(5) the disclosure is part of a report prepared by a consumer credit reporting agency in response to a request by a person and the person submits the social security number as part of the request to the consumer credit reporting agency for the preparation of the report; or

(6) the disclosure is for a background check on the individual, identity verification, fraud prevention, medical treatment, law enforcement or other government purposes, or the individual's employment, including employment benefits.

Sec. 45.48.440. Interagency disclosure. Notwithstanding the other provisions of AS 45.48.400 - 45.48.480, a state or local governmental agency may disclose an individual's social security number to another state or local governmental agency or to an agency of the federal government if the disclosure is required in order for the agency to carry out the agency's duties and responsibilities.

Sec. 45.48.450. Exception for employees, agents, and independent contractors. (a) Notwithstanding the other provisions of AS 45.48.400 - 45.48.480, a person may disclose an individual's social security number to an employee or agent of the person for a legitimate purpose established by and as directed by the person, but the employee or agent may not use the social security number for another purpose or make an unauthorized disclosure of the individual's personal information.

(b) Notwithstanding the other provisions of AS 45.48.400 - 45.48.480, and except as provided for an agent under (a) of this section, a person may disclose an individual's social security number to an independent contractor of the person to facilitate the purpose or transaction for which the individual initially provided the social security number to the person, but the independent contractor may not use the social security number for another purpose or make an unauthorized disclosure of the individual's personal information. In this subsection, "independent contractor" includes a debt collector.

Sec. 45.48.460. Employment-related exception. The provisions of AS 45.48.400 - 45.48.480 may not be construed to restrict a person's use or exchange of an individual's social security number

(1) in the course of the administration of a claim, benefit, or procedure related to the individual's employment by the person, including the individual's termination from employment, retirement from employment, and injury suffered during the course of employment; or

(2) to check on an unemployment insurance claim of the individual.

Sec. 45.48.470. Agency regulations. If regulations are necessary in order for a state agency to carry out the state agency's duties and responsibilities, a state agency may adopt regulations under AS 44.62 (Administrative Procedure Act) to establish when the state agency or a person regulated by the state agency may

(1) print an individual's social security number on material that is mailed to the individual;

(2) demand proof from an individual of the individual's social security number, collect from an individual the individual's social security number, or submit an individual's social security number to a local, state, or federal agency;

(3) ask an individual to provide the state agency with the individual's social security number;

(4) disclose an individual's social security number to a third party;

(5) sell, lease, loan, trade, or rent an individual's social security number to a third party.

Sec. 45.48.480. Penalties. (a) A person who knowingly violates AS 45.48.400 - 45.48.430 is liable to the state for a civil penalty not to exceed $3,000.

(b) An individual may bring a civil action in court against a person who knowingly violates AS 45.48.400 - 45.48.430 and may recover actual economic damages, court costs allowed by the rules of court, and full reasonable attorney fees.

(c) In this section, "knowingly" has the meaning given in AS 11.81.900.

Article 4. Disposal of Records.

Sec. 45.48.500. Disposal of records. (a) When disposing of records that contain personal information, a business and a governmental agency shall take all reasonable measures necessary to protect against unauthorized access to or use of the records.

(b) Notwithstanding (a) of this section, if a business or governmental agency has otherwise complied with the provisions of AS 45.48.500 - 45.48.590 in the selection of a third party engaged in the business of record destruction, the business or governmental agency is not liable for the disposal of records under AS 45.48.500 - 45.48.590 after the business or governmental agency has relinquished control of the records to the third party for the destruction of the records.

(c) A business or governmental agency is not liable for the disposal of records under AS 45.48.500 - 45.48.590 after the business or governmental agency has relinquished control of the records to the individual to whom the records pertain.

Sec. 45.48.510. Measures to protect access. The measures that may be taken

to comply with AS 45.48.500 include

(1) implementing and monitoring compliance with policies and procedures that require the burning, pulverizing, or shredding of paper documents containing personal information so that the personal information cannot practicably be read or reconstructed;

(2) implementing and monitoring compliance with policies and procedures that require the destruction or erasure of electronic media and other nonpaper media containing personal information so that the personal information cannot practicably be read or reconstructed;

(3) after due diligence, entering into a written contract with a third party engaged in the business of record destruction to dispose of records containing personal information in a manner consistent with AS 45.48.500 - 45.48.590.

Sec. 45.48.520. Due diligence. In AS 45.48.510(3), due diligence ordinarily includes performing one or more of the following:

(1) reviewing an independent audit of the third party's operations and its compliance with AS 45.48.500 - 45.48.590;

(2) obtaining information about the third party from several references or other reliable sources and requiring that the third party be certified by a recognized trade association or similar organization with a reputation for high standards of quality review; or

(3) reviewing and evaluating the third party's information security policies and procedures, or taking other appropriate measures to determine the competency and integrity of the third party.

Sec. 45.48.530. Policy and procedures. A business or governmental agency shall adopt written policies and procedures that relate to the adequate destruction and proper disposal of records containing personal information and that are consistent with AS 45.48.500 - 45.48.590.

Sec. 45.48.540. Exemptions. (a) A business or a governmental agency is not required to comply with AS 45.48.500 - 45.48.530 if federal law requires that the business or governmental agency act in a way that does not comply with AS 45.48.500 - 45.48.530.

(b) A business is not required to comply with AS 45.48.500 - 45.48.530 if

(1) the business is subject to and in compliance with the Gramm-Leach-Bliley Financial Modernization Act; or

(2) the manner of the disposal of the records of the business is subject to 15 U.S.C. 1681w of the Fair Credit Reporting Act and the business is complying with 15 U.S.C. 1861w.

Sec. 45.48.550. Civil penalty. (a) An individual, a business, or a governmental agency that knowingly violates AS 45.48.500 - 45.48.590 is liable to the state for a civil penalty not to exceed $3,000.

(b) In this section, "knowingly" has the meaning given in AS 11.81.900.

Sec. 45.48.560. Court action. An individual who is damaged by a violation of AS 45.48.500 - 45.48.590 may bring a civil action in court to enjoin further violations and to recover for the violation actual economic damages, court costs allowed by the rules of court, and full reasonable attorney fees.

Sec. 45.48.590. Definitions. In AS 45.48.500 - 45.48.590,

(1) "business" means a person who conducts business in the state or a person who conducts business and maintains or otherwise possesses personal information on state residents; in this paragraph,

(A) "conducts business" includes engaging in activities as a financial institution organized, chartered, or holding a license or authorization certificate under the laws of this state, another state, the United States, or another country;

(B) "possesses" includes possession for the purpose of destruction;

(2) "dispose" means

(A) the discarding or abandonment of records containing personal information;

(B) the sale, donation, discarding, or transfer of

(i) any medium, including computer equipment or computer media, that contains records of personal information;

(ii) nonpaper media, other than that identified under (i)

of this subparagraph, on which records of personal information are stored; and

(iii) equipment for nonpaper storage of information;

(3) "governmental agency" means a state or local governmental agency, except for an agency of the judicial branch;

(4) "personal information" means

(A) an individual's passport number, driver's license number, state identification number, bank account number, credit card number, debit card number, other payment card number, financial account information, or information from a financial application; or

(B) a combination of an individual's

(i) name; and

(ii) medical information, insurance policy number, employment information, or employment history;

(5) "records" means material on which information that is written, drawn, spoken, visual, or electromagnetic is recorded or preserved, regardless of physical form or characteristics, but does not include publicly available information containing names, addresses, telephone numbers, or other information an individual has voluntarily consented to have publicly disseminated or listed.

Article 5. Factual Declaration of Innocence after Identity Theft; Right to File Police Report Regarding Identity Theft.

Sec. 45.48.600. Factual declaration of innocence after identity theft. (a) A victim of identity theft may petition the superior court for a determination that the victim is factually innocent of a crime if

(1) the perpetrator of the identity theft was arrested for, cited for, or convicted of the crime using the victim's identity;

(2) a criminal complaint was filed against the perpetrator of the identity theft; and

(3) the victim's identity was mistakenly associated with a record of a conviction for a crime.

(b) In addition to a petition by a victim under (a) of this section, the

department may petition the superior court for a determination under (a) of this section, or the superior court may, on its own motion, make a determination under (a) of this section.

Sec. 45.48.610. Basis for determination. A determination of factual innocence under AS 45.48.600 may be heard and made on declarations, affidavits, police reports, or other material, relevant, and reliable information submitted by the parties or ordered to be made a part of the record by the court.

Sec. 45.48.620. Criteria for determination; court order. (a) A court may determine that a petitioner under AS 45.48.600 is factually innocent of a crime if the court finds beyond a reasonable doubt that

(1) the petitioner is a victim of identity theft;

(2) the petitioner did not commit the offense for which the perpetrator of the identity theft was arrested, cited, or convicted;

(3) the petitioner filed a criminal complaint against the perpetrator of the identity theft; and

(4) the petitioner's identity was mistakenly associated with a record of conviction for the crime.

(b) If a court finds under this section that the victim is factually innocent of a crime, the court shall issue an order indicating this determination of factual innocence and shall provide the victim with a copy of the order.

Sec. 45.48.630. Orders regarding records. After a court issues an order under AS 45.48.620, the court may order the name and associated personal information of the victim of identity theft that is contained in the files, indexes, and other records of the court that are accessible by the public labeled to show that the name and personal information of the victim of identity theft is incorrect.

Sec. 45.48.640. Vacation of determination. A court that has issued an order under AS 45.48.620 may, at any time, vacate the order if the petition, or any information submitted in support of the petition, is found to contain a material misrepresentation, omission, or false information.

Sec. 45.48.650. Court form. The supreme court of the state may develop a form to be used for the order under AS 45.48.620.

Sec. 45.48.660. Data base. The department may establish and maintain a data base of individuals who have been victims of identity theft and who have received an order under AS 45.48.620. The department shall provide a victim or the victim's authorized representative access to a data base established under this section to establish that the individual has been a victim of identity theft. Access to the data base established under this section is limited to criminal justice agencies, victims of identity theft, and individuals and agencies authorized by the victims

Sec. 45.48.670. Toll-free telephone number. The department may establish and maintain a toll-free telephone number to provide access to information in a data base established under AS 45.48.660.

Sec. 45.48.680. Right to file police report regarding identity theft. (a) Even if the local law enforcement agency does not have jurisdiction over the theft of an individual's identity, if an individual who has learned or reasonably suspects the individual has been the victim of identity theft contacts, for the purpose of filing a complaint, a local law enforcement agency that has jurisdiction over the individual's actual place of residence, the local law enforcement agency shall make a report of the matter and provide the individual with a copy of the report. The local law enforcement agency may refer the matter to a law enforcement agency in a different jurisdiction.

(b) This section is not intended to interfere with the discretion of a local law enforcement agency to allocate its resources to the investigation of crime. A local law enforcement agency is not required to count a complaint filed under (a) of this section as an open case for purposes that include compiling statistics on its open cases.

Sec. 45.48.690. Definitions. In AS 45.48.600 - 45.48.690,

(1) "crime" has the meaning given in AS 11.81.900;

(2) "department" means the Department of Law;

(3) "perpetrator" means the person who perpetrated the theft of an individual's identity;

(4) "victim" means an individual who is the victim of identity theft.

Article 6. Truncation of Card Information.

Sec. 45.48.750. Truncation of card information. (a) A person who accepts credit cards or debit cards for the transaction of business may not print more than the

last four digits of the card number or the expiration date on any receipt or other physical record of the transaction provided at the point of the sale or transaction.

(b) This section applies only to receipts that are electronically printed and does not apply to transactions in which the sole means of recording a credit card or debit card account number is by handwriting or by an imprint or copy of the card.

(c) A person may not sell a device that electronically prints more than the last four digits of a credit card or debit card number or expiration date on a consumer receipt for a business transaction or on a copy retained by a business person for a business transaction.

(d) An individual may bring a civil action in court against a person who knowingly violates (a) of this section and may recover actual economic damages, court costs allowed by the rules of court, and full reasonable attorney fees.

(e) A person who knowingly violates this section is liable to the state for a civil penalty not to exceed $3,000.

(f) In this section,

(1) "credit" means the right granted by a creditor to a debtor to defer payment of debt, to incur debts and defer payment of the debt, or to purchase property or services and defer payment of the purchase; in this paragraph. "creditor" means a person who regularly extends, renews, or continues credit, a person who regularly arranges for the extension, renewal, or continuation of credit, or an assignee of an original creditor who participates in the decision to extend, renew, or continue credit;

(2) "credit card" means a card, plate, coupon book, or other credit device existing for the purpose of obtaining money, property, labor, or services on credit;

(3) "debit card" means a card issued by a financial institution to a consumer for use in initiating an electronic fund transfer from the account of the consumer at the financial institution for the purpose of transferring money between accounts or obtaining money, property, labor, or services;

(4) "knowingly" has the meaning given in AS 11.81.900.

Article 7. General Provisions.

Sec. 45.48.990. Definitions. In this chapter, unless the context indicates

otherwise,

(1) "consumer" means an individual;

(2) "consumer credit reporting agency" means a person who, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing credit reports to third parties;

(3) "credit report" means a consumer report that a consumer reporting agency furnishes to a person that the consumer credit reporting agency has reason to believe intends to use the consumer report as a factor in establishing the consumer's eligibility for credit to be used primarily for personal, family, or household purposes; in this paragraph, "consumer report" has the meaning given to "consumer report" in 15 U.S.C. 1681a(d)(Fair Credit Reporting Act), except that "consumer reporting agency" in 15 U.S.C. 1681a(d) is to be read as "consumer credit reporting agency";

(4) "Fair Credit Reporting Act" means 15 U.S.C. 1681 - 1681x;

(5) "Gramm-Leach-Bliley Financial Modernization Act" means 15 U.S.C. 6801 - 6827;

(6) "identity theft" means the theft of the identity of an individual;

(7) "information system" means any information system, including a system consisting of digital data bases and a system consisting of pieces of paper;

(8) "person" has the meaning given in AS 01.10.060 and includes a state or local governmental agency, except for an agency of the judicial branch;

(9) "state resident" means an individual who satisfies the residency requirements under AS 01.10.055.

Sec. 45.48.995. Short title. This chapter may be cited as the Alaska Personal Information Protection Act.

* Sec. 4. AS 45.50.471(b) is amended by adding a new paragraph to read:

(53) an information collector, other than a governmental agency, violating AS 45.48.010 - 45.48.090 (breach of security involving personal information); in this paragraph,

(A) "governmental agency" has the meaning given in

AS 45.48.090;

(B) "information collector" has the meaning given in AS 45.48.090.

* Sec. 5. The uncodified law of the State of Alaska is amended by adding a new section to read:

INDIRECT COURT RULE AMENDMENTS. (a) AS 45.48.640, enacted by sec. 3 of this Act, has the effect of changing Rule 60(b), Alaska Rules of Civil Procedure, by allowing a court to vacate an order on its own motion and at any time and by establishing a specific criterion for vacating the order under AS 45.48.640.

(b) AS 45.48.200(a), 45.48.480(b), 45.48.560, and 45.48.750(d), enacted by sec. 3 of this Act, have the effect of changing Rule 82, Alaska Rules of Civil Procedure, by changing the criteria for determining the amount of attorney fees to be awarded to a party in an action under AS 45.48.200(a), 45.48.480(b), 45.48.560, or 45.48.750(d).

* Sec. 6. The uncodified law of the State of Alaska is amended by adding a new section to read:

TRANSITION: REGULATIONS. A state agency may proceed to adopt regulations necessary to implement this Act. The regulations take effect under AS 44.62 (Administrative Procedure Act), but not before the effective date of the law implemented by the regulation.

* Sec. 7. AS 45.48.470, enacted by sec. 3 of this Act, takes effect immediately under AS 01.10.070(c).

* Sec. 8. Section 6 of this Act takes effect immediately under AS 01.10.070(c).

* Sec. 9. Except as provided by secs. 7 and 8 of this Act, this Act takes effect July 1, 2009.

Adopted as Amended

25-LS0311\F.1
Bannister
4/11/08

AMENDMENT #1

OFFERED IN THE SENATE BY SENATOR STEDMAN

TO: SCS CSHB 65(FIN), Draft Version "F"

Page 1, line 3, following "**debit cards,**":

Insert "**disclosure of the names and addresses of permanent fund dividend applicants,**"

Page 2, following line 1:

Insert a new bill section to read:

"* **Sec. 2.** AS 43.23.017 is amended by adding a new subsection to read:

(b) Notwithstanding (a) of this section, the department may release the names and addresses of permanent fund dividend applicants to a legislator of this state and to the legislator's office staff." for official use.

Renumber the following bill sections accordingly.

Page 30, line 6:

Delete "sec. 3"

Insert "sec. 4"

Page 30, line 10:

Delete "sec. 3"

Insert "sec. 4"

Page 30, line 19:

Delete "sec. 3"

Insert "sec. 4"

Page 30, line 21:

Delete "Section 6"

Insert "Section 7"

Page 30, line 22:

Delete "secs. 7 and 8"

Insert "secs. 8 and 9"

25-LS0311\F.1
Bannister
4/11/08

Amended

AMENDMENT #1

OFFERED IN THE SENATE BY SENATOR STEDMAN

TO: SCS CSHB 65(FIN), Draft Version "F"

Page 1, line 3, following "debit cards,":

Insert "**disclosure of the names and addresses of permanent fund dividend applicants,**"

Page 2, following line 1:

Insert a new bill section to read:

"* **Sec. 2.** AS 43.23.017 is amended by adding a new subsection to read:

(b) Notwithstanding (a) of this section, the department may release the names and addresses of permanent fund dividend applicants to a legislator of this state and to the legislator's office staff." for official use.

Renumber the following bill sections accordingly.

Page 30, line 6:

Delete "sec. 3"

Insert "sec. 4"

Page 30, line 10:

Delete "sec. 3"

Insert "sec. 4"

Page 30, line 19:

Delete "sec. 3"

Insert "sec. 4"

Page 30, line 21:

Delete "Section 6"

Insert "Section 7"

Page 30, line 22:

Delete "secs. 7 and 8"

Insert "secs. 8 and 9"

ALASKA STATE HOUSE OF REPRESENTATIVES

Contact:
Interim Address:
3340 Badger Road
North Pole, AK 99705
(907)-488-5725
Fax# (907)-488-4271

Session

(907)-465-3719
FAX# (907)-465-3258
State Capitol
Room 204

REPRESENTATIVE JOHN COGHILL

SPONSOR STATEMENT
SENATE CS FOR CS FOR HB 65 (JUD) (25-LS0311\R)

"An Act relating to the breaches of security involving personal information, credit report and credit score security freezes, protection of social security numbers, care of records, disposal of records, identify theft, credit cards, and debit cards, and to the jurisdiction of the office of administrative hearings; amending Rules 60, and 82 Alaska Rules of Civil Procedure; and providing for an effective date."

In a time when information of every personal type is transmitted and stored electronically, it is necessary that those who have access to the use, storage, and disposal of sensitive consumer information be accountable and responsible.

This legislation deals with specific areas designed to secure a consumer's private information and ensure affordable access to their credit information.

This bill has 7 articles that deal with all areas of personal information and the rights and protections the consumer has and can expect from individuals that handle their personal information. The 7 articles are:

(1) **Breach of Security Involving Personal Information** - requires disclosure of breaches of security involving personal information.
(2) **Credit Report and Credit Score Security Freeze** – allows a consumer to freeze and unfreeze access to their credit information at their discretion.
(3) **Protection of Social Security Number** – by restricting sale and distribution.
(4) **Disposal of Records** – requires complete destruction of electronic and paper records that contain personal information.
(5) **Factual Declaration of Innocence after Identity Theft; Right to File Police Report Regarding Identity Theft** - allows a person that is a victim of identify theft to make a factual declaration of innocence.
(6) **Truncation of Card Information** – setting up guidelines for use of card numbers on receipts.
(7) **General Provisions** – provides definitions for terms within the chapter, cites the short title of this bill as the *Alaska Personal Information Protection Act*, and establishes effective dates.

Amended pg 4

Adopted 4/11/08

25-LS0311\F
Bannister
4/10/08

SENATE CS FOR CS FOR HOUSE BILL NO. 65(FIN)

IN THE LEGISLATURE OF THE STATE OF ALASKA

TWENTY-FIFTH LEGISLATURE - SECOND SESSION

BY THE SENATE FINANCE COMMITTEE

Offered:
Referred:

Sponsor(s): REPRESENTATIVES COGHILL AND GARA, Hawker, Lynn, Samuels, Fairclough, Ramras, Kawasaki, Kerttula, Gatto, Neuman, Olson, Dahlstrom, Gardner, Johnson, Wilson, Guttenberg, Holmes, Nelson, Crawford, LeDoux, Keller, Doogan, Buch, Roses, Cissna, Meyer

SENATORS Therriault, Wilken

A BILL

FOR AN ACT ENTITLED

"An Act relating to breaches of security involving personal information, credit report and credit score security freezes, protection of social security numbers, care of records, disposal of records, identity theft, credit cards, and debit cards, and to the jurisdiction of the office of administrative hearings; amending Rules 60 and 82, Alaska Rules of Civil Procedure; and providing for an effective date."

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF ALASKA:

* Section 1. AS 40.21.110 is amended to read:

Sec. 40.21.110. Care of records. Except for public records lawfully in the possession of a person other than the state, public records of existing or defunct agencies of the state, territorial, and Russian governments in Alaska are the property of the state and shall be created, maintained, preserved, stored, transferred, destroyed or disposed of, and otherwise managed in accordance with the provisions of this chapter and AS 45.48.500 - 45.48.530. Records shall be delivered by outgoing officials and employees to their successors, and may not be removed, destroyed or

disposed of, except as provided in this chapter **and AS 45.48.500 - 45.48.530**.

* **Sec. 2.** AS 44.64.030(a) is amended by adding a new paragraph to read:

(40) AS 45.48.080(c) (breach of security involving personal information).

* **Sec. 3.** AS 45 is amended by adding a new chapter to read:

Chapter 48. Personal Information Protection Act.

Article 1. Breach of Security Involving Personal Information.

Sec. 45.48.010. Disclosure of breach of security. (a) If a covered person owns or licenses personal information in any form that includes personal information on a state resident, and a breach of the security of the information system that contains personal information occurs, the covered person shall, after discovering or being notified of the breach, disclose the breach to each state resident whose personal information was subject to the breach.

(b) An information collector shall make the disclosure required by (a) of this section in the most expeditious time possible and without unreasonable delay, except as provided in AS 45.48.020 and as necessary to determine the scope of the breach and restore the reasonable integrity of the information system.

(c) Notwithstanding (a) of this section, disclosure is not required if, after an appropriate investigation or after written notification to the attorney general of this state, the covered person determines that there is not a reasonable likelihood that harm to the consumers whose personal information has been acquired has resulted or will result from the breach. The determination shall be documented in writing and the documentation shall be maintained for five years.

Sec. 45.48.020. Allowable delay in notification. An information collector may delay disclosing the breach under AS 45.48.010 if an appropriate law enforcement agency determines that disclosing the breach will interfere with a criminal investigation. However, the information collector shall disclose the breach to the state resident in the most expeditious time possible and without unreasonable delay after the law enforcement agency informs the information collector in writing that disclosure of the breach will no longer interfere with the investigation.

Sec. 45.48.030. Methods of notice. An information collector shall make the

disclosure required by AS 45.48.010

(1) by a written document sent to the most recent address the information collector has for the state resident;

(2) by electronic means if the information collector's primary method of communication with the state resident is by electronic means, or if making the disclosure by the electronic means is consistent with the provisions regarding electronic records and signatures required for notices legally required to be in writing under 15 U.S.C. 7001 et seq. (Electronic Signatures in Global and National Commerce Act); or

(3) if the information collector demonstrates that the cost of providing notice would exceed $150,000, that the affected class of state residents to be notified exceeds 300,000, or that the information collector does not have sufficient contact information to provide notice, by

(A) electronic mail if the information collector has an electronic mail address for the state resident;

(B) conspicuously posting the disclosure on the Internet website of the information collector if the information collector maintains an Internet site; and

(C) providing a notice to major statewide media.

Sec. 45.48.040. Notification of certain other agencies. (a) If an information collector is required by AS 45.48.010 to notify more than 1,000 state residents of a breach, the information collector shall also notify without unreasonable delay all consumer credit reporting agencies that compile and maintain files on consumers on a nationwide basis and provide the agencies with the timing, distribution, and content of the notices to state residents.

(b) This section may not be construed to require the information collector to provide the consumer reporting agencies identified under (a) of this section with the names or other personal information of the state residents whose personal information was subject to the breach.

(c) This section does not apply to an information collector who is subject to the Gramm-Leach-Bliley Financial Modernization Act.

Amendment 2

Credit

(d) In this section, "consumer reporting agency that compiles and maintains files on consumers on a nationwide basis" has the meaning given in 15 U.S.C. 1681a(p).

Sec. 45.48.050. Exception for employees and agents. In AS 45.48.010 - 45.48.090, the good faith acquisition of personal information by an employee or agent of an information collector for a legitimate purpose of the information collector is not a breach of the security of the information system if the employee or agent does not use the personal information for a purpose unrelated to a legitimate purpose of the information collector and does not make further unauthorized disclosure of the personal information.

Sec. 45.48.060. Waivers. A waiver of AS 45.48.010 - 45.48.090 is void and unenforceable.

Sec. 45.48.070. Treatment of certain breaches. (a) If a breach of the security of the information system containing personal information on a state resident that is maintained by an information recipient occurs, the information recipient is not required to comply with AS 45.48.010 - 45.48.030. However, immediately after the information recipient discovers the breach, the information recipient shall notify the information distributor who owns the personal information or who licensed the use of the personal information to the information recipient about the breach and cooperate with the information distributor as necessary to allow the information distributor to comply with (b) of this section. In this subsection, "cooperate" means sharing with the information distributor information relevant to the breach, except for confidential business information or trade secrets.

(b) If an information recipient notifies an information distributor of a breach under (a) of this section, the information distributor shall comply with AS 45.48.010 - 45.48.030 as if the breach occurred to the information system maintained by the information distributor.

Sec. 45.48.080. Violations. (a) If an information collector who is a governmental agency violates AS 45.48.010 - 45.48.090 with regard to the personal information of a state resident, the information collector

(1) is liable to the state for a civil penalty of up to $500 for each state

resident who was not notified under AS 45.48.010 - 45.48.090, but the total civil penalty may not exceed $50,000; and

(2) may be enjoined from further violations.

(b) If an information collector who is not a governmental agency violates AS 45.48.010 - 45.48.090 with regard to the personal information of a state resident, the violation is an unfair or deceptive act or practice under AS 45.50.471 - 45.50.561. However,

(1) the information collector is not subject to the civil penalties imposed under AS 45.50.551 but is liable to the state for a civil penalty of up to $500 for each state resident who was not notified under AS 45.48.010 - 45.48.090, except that the total civil penalty may not exceed $50,000; and

(2) damages that may be awarded against the information collector under

(A) AS 45.50.531 are limited to actual economic damages that do not exceed $500; and

(B) AS 45.50.537 are limited to actual economic damages.

(c) The Department of Administration may enforce (a) of this section against a governmental agency. The procedure for review of an order or action of the department under this subsection is the same as the procedure provided by AS 44.62 (Administrative Procedure Act), except that the office of administrative hearings (AS 44.64.010) shall conduct the hearings in contested cases and the decision may be appealed under AS 44.64.030(c).

Sec. 45.48.090. Definitions. In AS 45.48.010 - 45.48.090,

(1) "breach of the security" means unauthorized acquisition, or reasonable belief of unauthorized acquisition, of personal information that compromises the security, confidentiality, or integrity of the personal information maintained by the information collector; in this paragraph, "acquisition" includes acquisition by

(A) photocopying, facsimile, or other paper-based method;

(B) a device, including a computer, that can read, write, or store information that is represented in numerical form; or

(C) a method not identified by (A) or (B) of this paragraph;

(2) "covered person" means a

(A) person doing business;

(B) a governmental agency; or

(C) a person with more than 10 employees;

(3) "governmental agency" means a state or local governmental agency, except for an agency of the judicial branch;

(4) "information collector" means a covered person who owns or licenses personal information in any form if the personal information includes personal information on a state resident;

(5) "information distributor" means a person who is an information collector and who owns or licenses personal information to an information recipient;

(6) "information recipient" means a person who is an information collector but who does not own or have the right to license to another information collector the personal information received by the person from an information distributor;

(7) "personal information" means information in any form on an individual that is not encrypted or redacted, or is encrypted and the encryption key has been accessed or acquired, and that consists of a combination of

(A) an individual's name; in this subparagraph, "individual's name" means a combination of an individual's

(i) first name or first initial; and

(ii) last name; and

(B) one or more of the following information elements:

(i) the individual's social security number;

(ii) the individual's driver's license number or state identification card number;

(iii) except as provided in (iv) of this subparagraph, the individual's account number, credit card number, or debit card number;

(iv) if an account can only be accessed with a personal code, the number in (iii) of this subparagraph and the personal code; in

this sub-subparagraph, "personal code" means a security code, an access code, a personal identification number, or a password;

(v) passwords, personal identification numbers, or other access codes for financial accounts.

Article 2. Credit Report and Credit Score Security Freeze.

Sec. 45.48.100. Security freeze authorized. A consumer may prohibit a consumer credit reporting agency from releasing the consumer's credit report or credit score without the express authorization of the consumer by placing a security freeze on the consumer's credit report.

Sec. 45.48.110. Placement of security freeze. (a) To place a security freeze, a consumer shall make the request to the consumer credit reporting agency

(1) by mail to the address designated by the consumer credit reporting agency to receive security freeze requests; or

(2) as allowed by (b) of this section.

(b) A consumer may make a request under (a) of this section by telephone or by fax, the Internet, or other electronic media if the consumer credit reporting agency has developed procedures for using the telephone or an electronic medium to receive and process the request in an expedited manner.

(c) A consumer credit reporting agency shall place a security freeze within five business days after receiving a request under (a) or (b) of this section and proper identification from the consumer.

Sec. 45.48.120. Confirmation of security freeze. (a) Within 10 business days after a consumer makes the request under AS 45.48.110, a consumer credit reporting agency shall send a written confirmation of the placement of the security freeze to the consumer. The confirmation must also inform the consumer that the consumer credit reporting agency may charge, as allowed by AS 45.48.160, a fee for third-party access during the security freeze.

(b) At the same time that the consumer credit reporting agency sends a confirmation under (a) of this section, the consumer credit reporting agency shall provide the consumer with a unique personal identification number, password, or similar device to be used by the consumer when the consumer authorizes the release of

the consumer's credit report or credit score under AS 45.48.130.

Sec. 45.48.130. Access and actions during security freeze. (a) While a security freeze is in place, a consumer credit reporting agency shall allow a third party access to a consumer's credit report or credit score if the consumer requests that the consumer credit reporting agency allow the access.

(b) To make a request under (a) of this section, the consumer shall contact the consumer credit reporting agency by mail at the address designated by the consumer credit reporting agency to receive security freeze requests or as allowed by (c) of this section, authorize the consumer credit reporting agency to allow the access, and provide the consumer credit reporting agency with

(1) proper identification to verify the consumer's identity;

(2) the unique personal identification number, password, or similar device provided under AS 45.48.120(b); and

(3) the proper information necessary to identify the third party to whom the consumer credit reporting agency may allow the access or the time period during which the consumer credit reporting agency may allow the access to third parties who request the access.

(c) In addition to making the request by mail, a consumer may make a request under (a) of this section by telephone or by fax, the Internet, or other electronic media if the consumer credit reporting agency has developed procedures for using the telephone or an electronic medium to receive and process the request in an expedited manner.

(d) Except as provided by (e) of this section, a consumer credit reporting agency that receives a request from a consumer under (b) or (c) of this section shall comply with the request within 15 minutes after receiving the request by telephone or by an electronic medium or within three business days after receiving the request by mail.

(e) A consumer credit reporting agency is not required to comply with a request under (a) of this section within the 15 minutes required by (d) of this section if

(1) the consumer fails to satisfy the requirements of (b) of this section;

(2) one of the following events prevents the consumer credit reporting

agency from removing the security freeze within 15 minutes:

(A) an act of God, including a fire, earthquake, hurricane, storm, or similar natural disaster or phenomenon;

(B) an unauthorized or illegal act by another person, including terrorism, sabotage, riot, vandalism, labor strike, labor dispute disrupting operations, or similar occurrence;

(C) an operational interruption, including an electrical failure, unanticipated delay in equipment or replacement part delivery, computer hardware or software failure inhibiting response time, or similar disruption;

(D) governmental action, including an emergency order or regulation, a judicial law enforcement action, or a similar directive;

(E) regularly scheduled maintenance during other than normal business hours of the consumer credit reporting agency's systems, or updates to the consumer credit reporting agency's systems;

(F) commercially reasonable maintenance of, or repair to, the consumer credit reporting agency's systems that is unexpected or unscheduled; or

(3) the request is received outside of normal business hours.

(f) If a security freeze is in place, a consumer credit reporting agency may not release the credit report or credit score to a third party without the prior express authorization of the consumer.

(g) If a security freeze is in place on a consumer's credit report and credit score and if a third party applies to a consumer credit reporting agency to provide the third party with access to the consumer's credit report or credit score, the consumer credit reporting agency and the third party may treat the third party's application as incomplete unless the consumer authorizes the access under (a) of this section.

(h) If a security freeze is in place, a consumer credit reporting agency may not change the consumer's official information in the consumer's credit report and credit score without sending a written statement of the change to the consumer within 30 days after the change is made. A consumer credit reporting agency is not required to send a written statement if the consumer credit reporting agency makes a technical

change in the consumer's official information. If a consumer credit reporting agency makes a change, other than a technical change, in a consumer's address, the consumer credit reporting agency shall send the written statement to the consumer at both the new address and the former address. In this subsection,

(1) "official information" means name, birth date, social security number, and address;

(2) "technical change" means changing spelling, transposing numbers or letters, abbreviating a word, or spelling out an abbreviation.

(i) This section is not intended to prevent a consumer credit reporting agency from advising a third party that requests access to a consumer's credit report or credit score that a security freeze is in effect.

(j) The procedures used by a consumer credit reporting agency for implementing the provisions of this section may include the use of telephone, facsimile, or electronic means if making the disclosure by the electronic means is consistent with the provisions regarding electronic records and signatures required for notices legally required to be in writing under 15 U.S.C. 7001 et seq. (Electronic Signatures in Global and National Commerce Act).

Sec. 45.48.140. Removal of security freeze. (a) Except as provided by AS 45.48.130, a consumer credit reporting agency may not remove a security freeze unless

(1) the consumer requests that the consumer credit reporting agency remove the security freeze under (b) of this section; or

(2) the consumer made a material misrepresentation of fact to the consumer credit reporting agency when the consumer requested the security freeze under AS 45.48.110; if a consumer credit reporting agency intends to remove a security freeze on a consumer's credit report under this paragraph, the consumer credit reporting agency shall notify the consumer in writing before removing the security freeze.

(b) A consumer credit reporting agency shall remove a security freeze within three business days after receiving a request for removal from the consumer who requested the security freeze.

(c) To make a request under (b) of this section, the consumer shall contact the consumer credit reporting agency by mail or as allowed by (d) of this section, authorize the consumer credit reporting agency to remove the security freeze, and provide the consumer credit reporting agency with

(1) proper identification to verify the consumer's identity; and

(2) the unique personal identification number, password, or similar device provided under AS 45.48.120(b).

(d) In addition to mail, a consumer may make a request under (b) of this section by telephone or by fax, the Internet, or other electronic media if the consumer credit reporting agency has developed procedures for using the telephone or an electronic medium to receive and process the request in an expedited manner.

Sec. 45.48.150. Prohibition. When dealing with a third party, a consumer credit reporting agency may not suggest, state, or imply that a consumer's security freeze reflects a negative credit score, history, report, or rating.

Sec. 45.48.160. Charges. (a) Except as provided by (b), (c), or (d) of this section, a consumer credit reporting agency may not charge a consumer to place or remove a security freeze, to provide access under AS 45.48.130, or to take any other action, including the issuance of a personal identification number, password, or similar device under AS 45.48.120, that is related to the placement of, removal of, or allowing access to a credit report or credit score on which a security freeze has been placed.

(b) A consumer credit reporting agency may charge a consumer $5 for placing a security freeze.

(c) A consumer credit reporting agency may charge the consumer $2 for each access request made by the consumer. In this subsection, "access request" means a request made by the consumer under AS 45.48.130 to allow third-party access to the consumer's credit report or credit score on which a security freeze has been placed.

(d) If a consumer fails to retain a personal identification number, password, or similar device issued under AS 45.48.120, a consumer credit reporting agency may charge the consumer up to $5 for each time after the first time that the consumer credit reporting agency issues the consumer another personal identification number, password, or similar device because the consumer failed to retain the personal

identification number, password, or similar device.

(e) A consumer credit reporting agency may not charge a consumer a fee under (b) or (c) of this section if the consumer has been a victim of identity theft and provides the consumer credit reporting agency with a complaint filed by the consumer with a law enforcement agency.

Sec. 45.48.170. Notice of rights. When a consumer credit reporting agency is required to give a consumer a summary of rights under 15 U.S.C. 1681g of the Fair Credit Reporting Act, a consumer credit reporting agency shall also give the consumer the following notice:

Consumers Have the Right to Obtain a Security Freeze

You may obtain a security freeze on your credit report and credit score for $5 to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may not have to pay the $5 charge if you are a victim of identity theft. You have a right to place a security freeze on your credit report and credit score under state law (AS 45.48.100 - 45.48.290).

The security freeze will prohibit a consumer credit reporting agency from releasing your credit score and any information in your credit report without your express authorization or approval.

The security freeze is designed to prevent credit, loans, and other services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report and credit score may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, a mortgage, a governmental service, a governmental payment, a cellular telephone, a utility, an Internet credit card application, an extension of credit at point of sale, and other items and services.

When you place a security freeze on your credit report and credit score, within 10 business days you will be provided a personal

identification number, password, or similar device to use if you choose to remove the freeze on your credit report and credit score or to temporarily authorize the release of your credit report and credit score to a specific third party or specific third parties or for a specific period of time after the freeze is in place. To provide that authorization, you must contact the consumer credit reporting agency and provide all of the following:

(1) proper identification to verify your identity;

(2) the personal identification number, password, or similar device provided by the consumer credit reporting agency;

(3) proper information necessary to identify the third party or third parties who are authorized to receive the credit report and credit score or the specific period of time for which the credit report and credit score are to be available to third parties.

A consumer credit reporting agency that receives your request to temporarily lift a freeze on a credit report and credit score is required to comply with the request within 15 minutes, except after normal business hours and under certain other conditions, after receiving your request if you make the request by telephone, or an electronic method if the agency provides an electronic method, or within three business days after receiving your request if you make the request by mail. The consumer credit reporting agency may charge you $2 to temporarily lift the freeze.

A security freeze does not apply to circumstances where you have an existing account relationship and a copy of your credit report and credit score are requested by your existing creditor or its agents or affiliates for certain types of account review, collection, fraud control, or similar activities.

If you are actively seeking credit, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either

completely if you are shopping around, or specifically for a certain creditor, days before applying for new credit.

You have a right to bring a civil action against someone who violates your rights under these laws on security freezes. The action can be brought against a consumer credit reporting agency.

Sec. 45.48.180. Notification after violation. If a consumer credit reporting agency violates a security freeze by releasing a consumer's credit report or credit score, the consumer credit reporting agency shall notify the consumer within five business days after discovering or being notified of the release, and the information in the notice must include an identification of the information released and of the third party who received the information.

Sec. 45.48.190. Resellers. A consumer credit reporting agency that acts as a reseller of consumer information shall honor a security freeze placed on a consumer's credit report and credit score by another consumer credit reporting agency.

Sec. 45.48.200. Violations and penalties. (a) A consumer who suffers damages as a result of a person's violation of AS 45.48.100 - 45.48.290 may bring an action in court against the person and recover, in the case of a violation where the person acted

(1) negligently, actual economic damages, court costs allowed by the rules of court, and full reasonable attorney fees;

(2) knowingly,

(A) damages as described in (1) of this subsection;

(B) punitive damages that are not less than $100 nor more than $5,000 for each violation as the court determines to be appropriate; and

(C) other relief that the court determines to be appropriate.

(b) A consumer may bring an action in court against a person for a violation or threatened violation of AS 45.48.100 - 45.48.290 for injunctive relief, whether or not the consumer seeks another remedy under this section.

(c) Notwithstanding (a)(2) of this section, a person who knowingly violates AS 45.48.100 - 45.48.290 is liable in a class action for an amount that the court allows. When determining the amount of an award in a class action under this

subsection, the court shall consider, among the relevant factors, the amount of any actual damages awarded, the frequency of the violations, the resources of the violator, and the number of consumers adversely affected.

(d) In this section, "knowingly" has the meaning given in AS 11.81.900.

Sec. 45.48.210. Exemptions. (a) The provisions of AS 45.48.100 - 45.48.290 do not apply to the use of a credit report by

(1) a person, the person's subsidiary, affiliate, or agent, or the person's assignee with whom a consumer has or, before the assignment, had an account, contract, or debtor-creditor relationship if the purpose of the use is to review the consumer's account or to collect a financial obligation owing on the account, contract, or debt;

(2) a subsidiary, an affiliate, an agent, an assignee, or a prospective assignee of a person to whom access has been granted under AS 45.48.130 if the purpose of the use is to facilitate the extension of credit or another permissible use;

(3) a person acting under a court order, warrant, or subpoena;

(4) an agency of a state or municipality that administers a program for establishing and enforcing child support obligations;

(5) the Department of Health and Social Services, its agents, or its assigns when investigating fraud;

(6) the Department of Revenue, its agents, or its assigns when investigating or collecting delinquent taxes or unpaid court orders or when implementing its other statutory responsibilities;

(7) a person if the purpose of the use is prescreening allowed under 15 U.S.C. 1681b(c) of the Fair Credit Reporting Act;

(8) a person administering a credit file monitoring subscription service to which the consumer has subscribed;

(9) a person providing a consumer with a copy of the consumer's credit report or credit score at the consumer's request;

(10) a person if the data base or file of the consumer credit reporting agency consists entirely of information concerning and used solely for one or more of the following purposes:

(A) criminal record information;

(B) personal loss history information;

(C) fraud prevention or detection;

(D) tenant screening; or

(E) employment screening; or

(11) a person for use for insurance purposes in setting a rate, adjusting a rate, adjusting a claim, or underwriting, except that this paragraph may not be interpreted to authorize an insurance practice that is prohibited by other law; this paragraph may not be interpreted to affect AS 21.36.460 or AS 21.39.035.

(b) Except as provided by AS 45.48.190, the provisions of AS 45.48.100 - 45.48.290 do not apply to a person when acting only as a reseller of consumer information.

Sec. 45.48.290. Definitions. In AS 45.48.100 - 45.48.290,

(1) "account review" means activities related to account maintenance, account monitoring, credit line increases, and account upgrades and enhancements;

(2) "consumer" means an individual who is the subject of a credit report or credit score;

(3) "consumer credit reporting agency" has the meaning given in AS 45.48.990, but does not include a person who issues reports

(A) on incidents of fraud or authorizations for the purpose of approving or processing negotiable instruments, electronic funds transfers, or similar methods of payments; or

(B) regarding account closures because of fraud, substantial overdrafts, automated teller machine abuse, or similar negative information regarding a consumer to inquiring banks or other financial institutions for use only in reviewing consumer requests for deposit accounts at the inquiring banks or financial institutions;

(4) "reseller of consumer information" means a person who assembles and merges information contained in the data bases of consumer credit reporting agencies and does not maintain a permanent data base of consumer information from which new consumer credit reports are produced;

(5) "security freeze" means a prohibition against a consumer credit reporting agency's releasing a consumer's credit report or credit score without the express authorization of the consumer;

(6) "third party" means a person who is not

(A) the consumer who is the subject of the consumer's credit report or credit score; or

(B) the consumer credit reporting agency that is holding the consumer's credit report or credit score.

Article 3. Protection of Social Security Number.

Sec. 45.48.400. Use of social security number. (a) A person may not

(1) intentionally communicate or otherwise make available to the general public an individual's social security number;

(2) print an individual's social security number on a card required for the individual to access products or services provided by the person;

(3) require an individual to transmit the individual's social security number over the Internet unless the Internet connection is secure or the social security number is encrypted;

(4) require an individual to use the individual's social security number to access an Internet site unless a password, a unique personal identification number, or another authentication device is also required to access the site; or

(5) print an individual's social security number on material that is mailed to the individual unless

(A) local, state, or federal law, including a regulation adopted under AS 45.48.470, expressly authorizes placement of the social security number on the material; or

(B) the social security number is included on an application or other form, including a document sent as a part of an application process or an enrollment process, sent by mail to establish, amend, or terminate an account, a contract, or a policy, or to confirm the accuracy of the social security number; however, a social security number allowed to be mailed under this subparagraph may not be printed, in whole or in part, on a postcard or other

mailer that does not require an envelope, or in a manner that makes the social security number visible on the envelope or without the envelope's being opened.

(b) The prohibitions in (a) of this section do not apply if the person is engaging in the business of government and

(1) is authorized by law to communicate or otherwise make available to the general public the individual's social security number; or

(2) the communicating or otherwise making available of the individual's social security number is required for the performance of the person's duties or responsibilities as provided by law.

Sec. 45.48.410. Request and collection. (a) A person who does business in the state, including the business of government, may not request or collect from an individual the individual's social security number. This subsection does not prohibit a person from asking for another form of identification from the individual.

(b) The prohibition in (a) of this section does not apply

(1) if the person is authorized by local, state, or federal law, including a regulation adopted under AS 45.48.470, to demand proof of the individual's social security number, to request or collect the individual's social security number, or to submit the individual's social security number to the local, state, or federal government;

(2) if the person is engaging in the business of government and

(A) is authorized by law to request or collect the individual's social security number; or

(B) the request or collection of the individual's social security number is required for the performance of the person's duties or responsibilities as provided by law;

(3) to a person subject to or a transaction regulated by the Gramm-Leach-Bliley Financial Modernization Act for a purpose authorized by the Gramm-Leach-Bliley Financial Modernization Act;

(4) to a person subject to or a transaction regulated by the Fair Credit Reporting Act for a purpose authorized by the Fair Credit Reporting Act;

(5) if the request or collection is for a background check on the individual, for fraud prevention, for medical treatment, for law enforcement or other government purposes, for the individual's employment, including employment benefits, or for verification of the individual's age;

(6) if the request or collection does not have independent economic value, is incidental to a larger transaction or a larger anticipated transaction, and is necessary to verify the identity of the individual;

(7) to an insurer regulated by AS 21; in this paragraph, "insurer" has the meaning given in AS 21.90.900; or

(8) to a hospital service corporation or a medical service corporation regulated under AS 21.87; in this paragraph, "hospital service corporation" and "medical service corporation" have the meanings given in AS 21.87.330.

Sec. 45.48.420. Sale, lease, loan, trade, or rental. (a) A person may not sell, lease, loan, trade, or rent an individual's social security number to a third party.

(b) The prohibition in (a) of this section does not apply if the sale, lease, loan, trade, or rental is

(1) authorized by local, state, or federal law, including a regulation adopted under AS 45.48.470;

(2) by a person subject to or for a transaction regulated by the Gramm-Leach-Bliley Financial Modernization Act for a purpose authorized by the Gramm-Leach-Bliley Financial Modernization Act;

(3) by a person subject to or for a transaction regulated by the Fair Credit Reporting Act for a purpose authorized by the Fair Credit Reporting Act; or

(4) part of a report prepared by a consumer credit reporting agency in response to a request by a person and the person submits the social security number as part of the request to the consumer credit reporting agency for the preparation of the report.

(c) Nothing in this section prevents a business from transferring social security numbers to another person if the transfer is part of the sale or other transfer of the business to the other person.

(d) A transfer of an individual's social security number for the sole purpose of

identifying a person about whom a report or database check is ordered, received, or provided is not a sale, lease, loan, trade, or rental of a social security number under this section.

(c) A person who knowingly violates (a) of this section is guilty of a class A misdemeanor. In this subsection, "knowingly" has the meaning given in AS 11.81.900.

Sec. 45.48.430. Disclosure. (a) A person doing business, including the business of government, may not disclose an individual's social security number to a third party.

(b) The prohibition in (a) of this section does not apply if

(1) the disclosure is authorized by local, state, or federal law, including a regulation adopted under AS 45.48.470;

(2) the person is engaging in the business of government and

(A) is authorized by law to disclose the individual's social security number; or

(B) the disclosure of the individual's social security number is required for the performance of the person's duties or responsibilities as provided by law;

(3) the disclosure is to a person subject to or for a transaction regulated by the Gramm-Leach-Bliley Financial Modernization Act, and the disclosure is for a purpose authorized by the Gramm-Leach-Bliley Financial Modernization Act or to facilitate a transaction of the individual;

(4) the disclosure is to a person subject to or for a transaction regulated by the Fair Credit Reporting Act, and the disclosure is for a purpose authorized by the Fair Credit Reporting Act;

(5) the disclosure is part of a report prepared by a consumer credit reporting agency in response to a request by a person and the person submits the social security number as part of the request to the consumer credit reporting agency for the preparation of the report; or

(6) the disclosure is for a background check on the individual, identity verification, fraud prevention, medical treatment, law enforcement or other government purposes, or the individual's employment, including employment benefits.

Sec. 45.48.440. Interagency disclosure. Notwithstanding the other provisions of AS 45.48.400 - 45.48.480, a state or local governmental agency may disclose an individual's social security number to another state or local governmental agency or to an agency of the federal government if the disclosure is required in order for the agency to carry out the agency's duties and responsibilities.

Sec. 45.48.450. Exception for employees, agents, and independent contractors. (a) Notwithstanding the other provisions of AS 45.48.400 - 45.48.480, a person may disclose an individual's social security number to an employee or agent of the person for a legitimate purpose established by and as directed by the person, but the employee or agent may not use the social security number for another purpose or make an unauthorized disclosure of the individual's personal information.

(b) Notwithstanding the other provisions of AS 45.48.400 - 45.48.480, and except as provided for an agent under (a) of this section, a person may disclose an individual's social security number to an independent contractor of the person to facilitate the purpose or transaction for which the individual initially provided the social security number to the person, but the independent contractor may not use the social security number for another purpose or make an unauthorized disclosure of the individual's personal information. In this subsection, "independent contractor" includes a debt collector.

Sec. 45.48.460. Employment-related exception. The provisions of AS 45.48.400 - 45.48.480 may not be construed to restrict a person's use or exchange of an individual's social security number

(1) in the course of the administration of a claim, benefit, or procedure related to the individual's employment by the person, including the individual's termination from employment, retirement from employment, and injury suffered during the course of employment; or

(2) to check on an unemployment insurance claim of the individual.

Sec. 45.48.470. Agency regulations. If regulations are necessary in order for a state agency to carry out the state agency's duties and responsibilities, a state agency may adopt regulations under AS 44.62 (Administrative Procedure Act) to establish when the state agency or a person regulated by the state agency may

(1) print an individual's social security number on material that is mailed to the individual;

(2) demand proof from an individual of the individual's social security number, collect from an individual the individual's social security number, or submit an individual's social security number to a local, state, or federal agency;

(3) ask an individual to provide the state agency with the individual's social security number;

(4) disclose an individual's social security number to a third party;

(5) sell, lease, loan, trade, or rent an individual's social security number to a third party.

Sec. 45.48.480. Penalties. (a) A person who knowingly violates AS 45.48.400 - 45.48.430 is liable to the state for a civil penalty not to exceed $3,000.

(b) An individual may bring a civil action in court against a person who knowingly violates AS 45.48.400 - 45.48.430 and may recover actual economic damages, court costs allowed by the rules of court, and full reasonable attorney fees.

(c) In this section, "knowingly" has the meaning given in AS 11.81.900.

Article 4. Disposal of Records.

Sec. 45.48.500. Disposal of records. (a) When disposing of records that contain personal information, a business and a governmental agency shall take all reasonable measures necessary to protect against unauthorized access to or use of the records.

(b) Notwithstanding (a) of this section, if a business or governmental agency has otherwise complied with the provisions of AS 45.48.500 - 45.48.590 in the selection of a third party engaged in the business of record destruction, the business or governmental agency is not liable for the disposal of records under AS 45.48.500 - 45.48.590 after the business or governmental agency has relinquished control of the records to the third party for the destruction of the records.

(c) A business or governmental agency is not liable for the disposal of records under AS 45.48.500 - 45.48.590 after the business or governmental agency has relinquished control of the records to the individual to whom the records pertain.

Sec. 45.48.510. Measures to protect access. The measures that may be taken