HB

65

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

HB 65 "*An Act relating to breaches of security involving personal information, credit report and credit score security freezes, consumer credit monitoring, credit accuracy, protection of social security numbers, care of records, disposal of records, identify theft, furnishing consumer credit header information, credit cards, and debit cards, and to the jurisdiction of the office of administrative hearings; amending Rule 60, Alaska Rules of Civil Procedures; 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 that have access to the use, storage, and disposal of sensitive consumer information be accountable and responsible.

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

(1) **Breach of Security of Personal Information** - requires disclosure of breaches of security involving personal information.
(2) **Credit Report and Credit Score Security Freeze** – allows consumer to freeze and unfreeze access to their credit information at their discretion.
(3) **Consumer Credit Monitoring – Credit Accuracy**
(4) **Protection of Social Security Number** – by restricting sale and distribution.
(5) **Disposal of Records** – requires complete destruction of electronic and paper records that contain personal information.
(6) **Right to File Police Report Regarding Identity Theft** - allowing a person that falls victim to identify theft to make a factual declaration of innocence.
(7) **Consumer Credit Header Information** – restricts distribution of credit header information.
(8) **Truncation of Card Information** – setting up guidelines for use of card numbers on receipts.

FISCAL NOTE

STATE OF ALASKA
2007 LEGISLATIVE SESSION

Fiscal Note Number: HB065-GOV-OMB-3-25-07
Bill Version: HB 65
() Publish Date:

Revision Date/Time (Note if correction):
Dept. Affected: All
Title: Security breaches -- Identity theft
RDU
Component
Sponsor: Rep. Coghill
Requester: House Labor and Commerce Committee
Component No.

Expenditures/Revenues (Thousands of Dollars)

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

OPERATING EXPENDITURES	FY 2008	FY 2009	FY 2010	FY 2011	FY 2012	FY 2013
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 (Specify Type--Do not abbreviate)						
TOTAL	***	***	***	***	***	***

Estimate of any current year (FY2007) cost: 0.0
Check this box (X) if funding for this bill is included in the Governor's FY 2008 budget proposal:

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, could result in the imposition of extremely large financial penalties on the State of Alaska. Article 4 of the bill, relating to social security numbers, would allow individuals to sue the State of Alaska for damages of $5,000 or actual damages, whichever is greater, in the event of a security breach resulting in disclosure of social security numbers.

Although the State is pursuing all prudent and practical security measures to protect (continued)

Prepared by: Jack Kreinheder, Senior Analyst — Phone 465-4676
Division: Office of Management and Budget — Date/Time 3/25/07 10:30 AM

Approved by: Karen J. Rehfeld, Director — Date 3/25/2007
Agency: Office of Management and Budget

ANALYSIS CONTINUATION

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, an attorney could file a class action lawsuit against the State seeking damages of **$2.5 billion** or more (500,000 records multiplied by damages of $5,000 per individual). Even if the State settled such a case for 10 cents on the dollar, the cost to the State would still be $250 million.

A number of 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 would be over $100,000 for postage at bulk rates, plus any overtime and/or contractual assistance required to determine the affected individuals and locate current addresses.

While notification of individuals affected by disclosure of personal information is an appropriate practice, certain requirements of the bill, such as written notice (versus e-mail where possible), may increase the cost of such notification.

FISCAL NOTE

STATE OF ALASKA
2007 LEGISLATIVE SESSION

Fiscal Note Number: HB065-DOA-ETS-3-26-07
Bill Version: HB 65
() Publish Date:

Revision Date/Time (Note if correction):
Dept. Affected: Administration
Title "An Act relating to Breaches of Security Involving...
RDU Enterprise Technology Services
Component Enterprise Technology Services
Sponsor Reps. Coghill, Gara
Requester
Co ponent No. 2082

Expenditures/Revenues (Thousands of Dollars)

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

OPERATING EXPENDITURES	FY 2008	FY 2009	FY 2010	FY 2011	FY 2012	FY 2013
Personal Services	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
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
Equipment	1,765.6	0.0	0.0	0.0	0.0	0.0
Land & Structures	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
Miscellaneous	0.0	0.0	0.0	0.0	0.0	0.0
TOTAL OPERATING	**2,040.6**	**319.0**	**319.0**	**319.0**	**319.0**	**319.0**
CAPITAL EXPENDITURES		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

FUND SOURCE (Thousands of Dollars)						
1002 Federal Receipts	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
1004 GF	2,040.6	319.0	319.0	319.0	319.0	319.0
1005 GF/Program Receipts	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
1156 Reciept Supported Services	0.0	0.0	0.0	0.0	0.0	0.0
TOTAL	**2,040.6**	**319.0**	**319.0**	**319.0**	**319.0**	**319.0**

Estimate of any current year (FY2007) cost: 0.0
Mark this box (X) if funding for this bill is included in the Governor's FY 2008 budget proposal:

POSITIONS

Full-time						
Part-time						
Temporary						

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

HB65 has 2 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 two 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 2008.

Prepared by: Frank Bailey, Special Assistant II
Phone 269-6293
Division Department of Administration
Date/Time 3/26/04 12:00 PM
Approved by: Kevin Brooks, Deputy Commissioner
Date 3/26/2007
Agency Department of Administration

ANALYSIS CONTINUATION

The third 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 this final phase of 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 Request $4,400,000

The amount requested in this fiscal note would have been requested as an FY09 Capital project, but passage of this legislation will require funding now with an anticipated project completion date of June 2008.

SECTIONAL
CS for House Bill 65(JUD)
(25-LS0311\M)

Article 1. Breach of Security Involving Personal Information

Sec. 45.48.010 Disclosure of breach of security

Describes what a person who owns or uses personal information must do in case of a breach of information.

Sec. 45.48.020 Allowable delay in notification

Describes reasons for delaying notification of a breach of information.

Sec. 45.48.030 Methods of notice

Describes the methods to be used to notify a person that there has been a breach of information. Lists exceptions to the methods of notification relating to cost and number of consumers to be notified.

Sec. 45.48.040 Notification of certain other agencies

Describes when it is necessary to notify other consumer reporting agencies about a breach. There are exceptions to these requirements are also set out.

Sec. 45.48.050 Exception of employees and agents

Lists exceptions for acquisition of personal information by an employee or agent of an information collector.

Sec. 45.48.060 Waivers

No waivers of these sections are allowed.

Sec. 45.48.070 Treatment of certain breaches

A breach of information by an information recipient must be reported to the information distributor so they can comply with the notification requirements if the breach occurred to an information system maintained by the information distributor.

Sec. 45.48.080 Violations

Sets out fines for violations of 45.48.010-45.48.090 by a governmental agency that is an information collector, and information collectors who are not governmental agencies. Defines "governmental agency".

Sec. 45.48.090 Definitions

Defines the following terms: breach of the security; information collector; information distributor; information recipient; and personal information.

Article 2. Credit Report and Credit Score Security Freeze

Sec. 45.48.100 Security freeze authorized

Rights of consumers to prohibit release of their personal information.

Sec. 45.48.110 Placement of security freeze

Sets out procedures for a consumer to request a consumer credit reporting agency to freeze their information.

Sec. 45.48.120 Confirmation of security freeze

Describes the responsibility of the consumer credit reporting agency to notify the consumer when a security freeze has been placed.

Sec. 45.48.130 Access and actions during security freeze

Describes how a consumer can allow access to their information by a third party when a security freeze is in place; how an insurer is to treat a consumer's application if a security freeze prevents access to the consumer's information, and what changes are allowed when a security freeze is in place, and notification requirements. Defines "official information" and "technical change".

Sec. 45.48.140 Removal of security freeze

Sets out procedure for removing a security freeze, how the request for the freeze is to be made, how the consumer credit reporting agency shall respond, and what identifiers are necessary to remove the freeze.

Sec. 45.48.150 Prohibition

Sets out guidelines for reporting to third parties when a security freeze is in place.

Sec. 45.48.160 Charges

Charges to a consumer regarding security freezes.

Amendment No. 2 - Page 10, line 20 (b) Insert: a consumer credit reporting agency may charge a consumer $10 for placing a security freeze.

Sec. 45.48.170 Notice of rights

Additional notices to be given when a consumer is provided a summary of rights under the Fair Credit Reporting Act (FCRA).

Amendments No. 2 & 3 - Page 11, line 9 (b) Insert: for $10. Page 12, lines 17-19 Insert: Under some circumstances, the consumer credit reporting agency may charge $2 to temporarily lift the freeze.

Sec. 45.48.180 Notification after violation

Describes the notice required if a consumer credit reporting agency violates a security freeze.

Sec. 45.48.190 Resellers

Requires that a consumer credit reporting agency acting as a reseller honor a security freeze that is placed by another consumer reporting agency.

Sec. 45.48.200 Violations and penalties

Describes the rights of a consumer who suffers damages as a result of a breach of their personal information.

Sec. 45.48.210 Exemptions

Lists exemptions to the use of credit information when a security freeze is in place.

Sec. 45.48.290 Definitions

Defines the following terms: account review; consumer; consumer credit reporting agency; reseller of consumer information; security freeze; third party.

Amendment No. 4 – Delete: [Article 3. Consumer Credit Monitoring; Credit Accuracy – In its entirety.]

Article 3. Protection of Social Security Number

Sec. 45.48.400 Use of social security number

Sets out guidelines for handling a person's social security number.

Sec. 45.48.410 Request and collection

Sets out prohibitions and exemptions for requesting or collecting an individual's social security number.

Amendment No. 9 – Page 17, lines 6 - 11 Insert: new paragraph (2) new language to exempt a person engaged in the business of government from being in violation of this section if they request or collect a SSN.

Amendment No. 12 – Page 17, lines 22 - 24 Insert: new paragraph "(6) if the disclosure does not have independent economic value, is incidental to a larger transaction, and is necessary to verify the identify of the individual."

Sec. 45.48.420 Sale, lease, loan, trade, or rental

Prohibitions and exemptions regarding third party use of social security numbers.

Amendment No. 11 – Page 18, lines 4 - 5 Insert: new subsection (c) that makes it a Class A misdemeanor to knowingly sell, lease, loan, trade, or rent an individuals SSN.

Sec. 45.48.430 Disclosure

Prohibitions and exemptions regarding disclosure of social security numbers to third parties.

Amendment No. 9 – Page 18, lines 12 - 17 Insert: new paragraph (2) new language to exempt a person engaged in the business of government from being in violation of this section if they disclose a SSN.

Sec. 45.48.440 Interagency disclosure

Describes when and to whom disclosure is authorized.

Sec. 45.48.450 Exception for employees, agents, & independent contractors

Describes when and to whom disclosure is authorized.

Sec. 45.48.460 Employment-related exception

Describes when use of a social security number should not be restricted.

Sec. 45.48.470 Agency regulations

Procedures for adopting regulations necessary for a state agency to carry out their duties and responsibilities.

Sec. 45.48.480 Penalties

Rights of the state and individuals against persons that knowingly violate these sections.

Article 4. Disposal of Records

Sec. 45.48.500 Disposal of records

This sets out the measures to be followed when disposing of records which contain personal information.

Sec. 45.48.510 Measures to protect access.

Describes the measures that may be taken to comply with Sec. 45.48.500 (above).

Sec. 45.48.520 Due diligence

Lists procedures that if performed show due diligence.

Sec. 45.48.530 Policy and procedures

A business or governmental agency shall adopt written policies and procedures relating to records disposal.

Sec. 45.48.540 Exemptions

Compliance to these sections is not required if a government agency or business is required by federal law to act in another way, or the business is subject to and in compliance with GLBA, or FCRA.

Sec. 45.48.550 Civil penalty

Liability to the state by an individual, business, or governmental agency for violations of these sections.

Sec. 45.48.560 Court action

An individual damaged by a violation of these sections may file a civil action.

Sec. 45.48.590 Definitions

Defines the following terms: business; conducts business; possesses; dispose; governmental agency; personal information; records.

Amendment No. 5 – Page 23, lines 2 - 10: Inserted new language to define "personal information".

Article 5. Factual Declaration of Innocence after Identify Theft, Right to file Police Report Regarding Identity Theft

Sec. 45.48.600 Factual declaration of innocence after identity theft

Describes the conditions that should exist in order for an individual to petition the superior court for a determination of innocence of a crime involving the theft of their identity.

Sec. 45.48.610 Basis for determination

Lists the type of information that may be made part of the record for the court to make a determination of factual innocence.

Sec. 45.48.620 Criteria for determination; court order

Sets the criteria that the court may use to determine a victim's factual innocence.

Amendment No. 6 – Page 24, line 1 changed shall to may, and Page 24, lines 5 to 13 inserted a new subsection (a) with new language for determining a victim's innocence.

Sec. 45.48.630 Orders regarding records

Describes what the court may order regarding the disposition of incorrect records regarding a victim of identity theft.

Amendment No. 6 – Page 24, line 20 Deleted: "deleted, sealed, or"

Sec. 45.48.640 Vacation of determination

States that a court order may be vacated if there has been a misrepresentation of the material.

Amendment No. 6 – Page 24, line 25 Deleted: "fraudulent material" Inserted: "omission, or false information"

Sec. 45.48.650 Court form

Development of a form to be used under 45.48.620

Sec. 45.48.660 Data base

This section allows the establishment and maintenance of a data base of victims of identity theft, and who has authorization to the information.

Sec. 45.48.670 Toll-free telephone number

Establishes a toll-free number that accesses the information in the data base established in 45.48.660.

Sec. 45.48.680 Right to file police report regarding identity theft

Sets out rights of an individual to file a police report if they suspect they are a victim of identity theft, and the responsibility of a law enforcement agency to make the report even if they do not have jurisdiction.

Sec. 45.48.690 Definitions

Defines the following terms: crime, department, identity theft, perpetrator, and victim.

Amendment No. 7 – Delete Article 7, Consumer Credit Header Information – In its entirety.

Article 6. Truncation of Card Information

Sec. 45.48.750 Truncation of card information

Describes limits on a business regarding the printing of credit or debit card numbers and the exceptions depending on whether the receipt is produced electronically or is handwritten or imprinted.

States that a person may not sell a device that prints more than the last four digits of a credit or debit card on the consumer or merchant copy. Provides for an effective date of January 1, 2009.

Article 7. General Provisions

Sec. 45.48.990 Definitions
Provides definitions of terms.

Sec. 45.48.995 Short Title
Gives Alaska Personal Information Protection Act as the short title of this legislation, amends AS 45.50.471(b) by adding a new paragraph (52), amends the uncodified law of the State of Alaska by adding a new section, and provides for an immediate effective date under AS 01.10.070(c).

INDIRECT COURT RULE AMENDMENTS
Amendment No. 8 – Page 28, line 7 – Insert: new subsection (b) AS 45.48.480(b) added language that changes Rule 82, Alaska Rules of Civil Procedure.

LEGAL SERVICES

DIVISION OF LEGAL AND RESEARCH SERVICES
LEGISLATIVE AFFAIRS AGENCY
STATE OF ALASKA

(907) 465-3867 or 465-2450
FAX (907) 465-2029
Mail Stop 3101

State Capitol
Juneau, Alaska 99801-1182
Deliveries to: 129 6th St., Rm. 329

MEMORANDUM April 23, 2007

SUBJECT: CSHB 65(L&C) relating to personal information
(Work Order No. 25-LS0311\E)

TO: Representative Kurt Olson
Chair of the House Labor and Commerce Committee
Attn: Eleanor Wolfe

FROM: Theresa Bannister
Legislative Counsel

This memo accompanies the bill described above.

1. Technical change. A technical change was made to sec. 45.48.700(a)(1). The name of the referenced federal act was corrected to read "Fair Credit Reporting Act" (the correct name and the name used elsewhere in the bill) instead of "Fair Credit Protection Act."

2. Interstate commerce. Because this bill could apply to out-of-state businesses that operate in the state, including through the Internet, it raises a constitutional interstate commerce issue. Whenever a bill establishes a requirement that may affect persons operating from another state, there is always a question whether the requirement places a burden on interstate commerce that would not satisfy the federal constitutional commerce clause.

3. Federal law preemption. As you are probably aware, certain federal laws may preempt your new provisions in certain areas. If you would like further information on this issue, please advise.

If I may be of further assistance, please advise.

TLB:ljw
07-223.ljw

Enclosure

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, **other than a governmental agency**, 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, **other than a governmental agency**, 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

AKPIRG

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 can to 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.

STATE OF ALASKA

DEPARTMENT OF LAW

OFFICE OF THE ATTORNEY GENERAL

SARAH PALIN, GOVERNOR

1031 WEST 4TH AVENUE, SUITE 200
ANCHORAGE, ALASKA 99501-5903
PHONE: (907)269-5100
FAX: (907)276-8554

January 15, 2007

Honorable Jay Ramras
House of Representatives
State Capitol
MS 3100, Room 118
Juneau, Alaska 99801-1182

Re: HB 31, HB 65; Identity Theft Legislation

Dear Representative Ramras:

As sponsors of Identity Theft legislation, the Department of Law would like to share with you its letter to Senator Gene Therriault, attached, that explains the Department's concerns with SB 21. HB 31 and HB 65 appear to be identical copies of SB 21. Please share this with you committee members.

Please let me know if you have any questions.

Sincerely,

TALIS J. COLBERG
ATTORNEY GENERAL

By: Clyde E. Sniffen, Jr.
Assistant Attorney General

CES/mdz
Enclosure

cc: Craig Tillery
Gail Voightlander
Deborah Behr

STATE OF ALASKA

DEPARTMENT OF LAW

OFFICE OF THE ATTORNEY GENERAL

SARAH PALIN, GOVERNOR

1031 WEST 4TH AVENUE, SUITE 200
ANCHORAGE, ALASKA 99501-5903
PHONE: (907)269-5100
FAX: (907)276-8554

December 19, 2006

The Honorable Gene Therriault
State Capitol
MS 3100
Room 119
Juneau, AK 99801-1182

Re: HCS for CS for SB 169(FIN) am H; Identity Theft Legislation

Dear Senator Therriault:

Thank you again for sponsoring, legislation that we hope will make a difference in the fight against identity theft. The Department of Law continues to offer its support for this legislation, although we hope to work with you to resolve some concerns we continue to have. This bill adds comprehensive requirements on individuals, business, and state agencies to safeguard personal information, including social security numbers (SSN's) and the disposal of records containing personal information. The Department of Law has testified in support of the intent of this bill, but has concerns about how this bill may expose the state to substantial liability for inadvertent disclosure of personal information, including SSN's, or the improper disposal of records. As you know, numerous state agencies must collect, disclose, and use personal information for a variety of important state governmental functions.

The state is not suggesting that its agencies should not comply with the requirements of this bill. It should be subject to the same compliance as anyone who handles personal information. The only concern is the potential liability of the state for inadvertent mistakes that will surely be capitalized on by creative class action attorneys. Because the state does not operate like private business, it should not be exposed to the same liability. Unlike private business, the state does not have the choice of simply not engaging in activity that involves the collection of personal information as an option to avoid liability under the bill. The state is required by law to administer a variety of programs. The state does not make money by collecting and selling personal information.

It is also noteworthy that the majority of states with security breach and credit freeze laws do not impose liability on governmental entities. The laws we have reviewed consistently apply to only private business entities and individuals, not state government. Most of these laws also provide enforcement by the attorney general of the state, penalizing violations under the state's consumer protection laws. This is consistent with the principles of sovereign immunity, which recognizes that states should not be held liable for performing the functions of state government.

The Department appreciates the change in Sec. 45.48.080 that limits state penalty exposure to $50,000. The bill contains two other provisions, however, that allow individuals to sue the state for actual damages (unlimited) or $3,000, whichever is greater. The first is Sec. 45.48.480, relating to the illegal disclosure of SSN's. The second is Sec. 45.48.550, relating to disposal of records.

The scope of potential liability of the state under these two provisions is much higher than nearly every business subject to the bill because the state is required to engage in transactions involving hundreds of thousands of individuals (i.e., driver's licenses, fishing licenses, PFD applications, etc.). Each of these transactions could involve the use of SSN's. And nearly every transaction will result in records that may contain personal information. Where the actual damage is less than $3,000, the penalty is punitive. The state is not required to ever pay punitive damages.

These seemingly low amounts of damages imposed for liability under the act grow to huge numbers when multiplied by the potential number of affected consumers. A class action claim for 300,000 drivers or PFD recipients creates a penalty exposure to the state of $1.5 billion, regardless of whether a consumer has suffered any damages. The potential for a class action lawsuit and the recovery of huge damages will encourage plaintiffs' attorneys probing the law for a loophole and could result in potential liability not intended by the legislature. Even if ultimately successful in defending these lawsuits, the cost of litigation will be substantial.

Sec. 45.48.480 and .550 both contain a requirement that before liability can be found, a person must act "knowingly." This standard does not protect the state from liability for several reasons. The standard is actually fairly low when the definition under AS 11.81.900 is considered. A state employee can act "knowingly" if he or she has a "substantial probability" of knowledge that the conduct is prohibited. Additionally, some state employment contracts may require the state to both indemnify and defend individual employees for a "knowingly" type of act or failure to act.

The Department proposes the addition of the following language to both Sec's. 45.48.480 and .550:

( ) No claim may be made under this subsection against a governmental entity or its employees.

We believe this language resolves the state's concerns, while still preserving the intent of the bill.

While the Department supports the concepts embodied in this legislation, exposing the state to the potential liability created by this bill is unnecessary. The target of this bill should remain on private industry. Thank you again for your efforts on this legislation. We are available at your convenience to discuss any issues related to the state's concerns.

Sincerely,

TALIS J. COLBERG
ATTORNEY GENERAL

By: Clyde E. Sniffen, Jr.
Clyde E. Sniffen, Jr.
Senior Assistant Attorney General

cc: Craig Tillery, Deputy Attorney General
Kevin Jardell
Gail Voightlander
Randy Ruaro

CES/sjm

SARAH PALIN, GOVERNOR

DEPARTMENT OF LAW

OFFICE OF THE ATTORNEY GENERAL

1031 WEST 4TH AVENUE, SUITE 200
ANCHORAGE, ALASKA 99501-5903
PHONE: (907)269-5100
FAX: (907)276-8554

COMMENTS FOR THE HOUSE JUDICIARY COMMITTEE CONCERING LIABILITY ISSUES CS FOR HOUSE BILL NO. 65(L&C) (VERSION \E)

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 Department cannot support this bill until these liability provisions are addressed.

The section that causes the Department the most concern is found in Article 4 (protection of social security numbers) at Sec. 45.48.480 (penalties) beginning on page 22 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. Thus, ***even with no damages,*** a consumer could collect $5,000 from the state for a simple mistake. When multiplied by the potential number of disclosures, the state's monetary exposure under this section could be enormous while consumers have suffered ***NO DAMAGES***. The Department believes this exposure is completely unnecessary, does nothing to further the goals of the bill, and should be amended. The Department has prepared a proposed amendment that is attached.

The following are some common misconceptions about the effect of this amendment:

1. Shouldn't the State be accountable for disclosing a social security number just like everyone else?

YES. But the penalty provision in this bill 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, maintain and disclose, and has spent millions of dollars upgrading its systems. This effort will continue regardless of whether the state is exposed to liability. THE STATE WILL STILL BE SUBJECT TO ALL THE REQUIREMENTS OF THIS BILL.

//
//
//
//
//

2. Why should the state be treated differently than private business under this bill?

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

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

* **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.**

* **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.**

* **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 discretionary duties required by statute. The state is also exempt from punitive damage awards. The policy behind treating the state differently is clear, and does not create a "double standard." Payment of penalties by the state simply makes these funds unavailable for public purposes.**

3. Don't other states hold government responsible for these kinds of disclosures?

NO. 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. 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. Only two states (that we know of), out of over 20 that have these laws, even allow the government to be sued; Nevada and Louisiana. In Nevada only the AG can bring a suit against a

government agency. In Louisiana, a private right of action against the government exists, but only for actual damages.

4. If the state is not liable, how can consumers recover damages if the state discloses a SSN in violation of this law?

Individual consumers who are harmed by the state's conduct in releasing a SSN can bring a civil action against the state for negligence or any other claim the consumer has. This right exists regardless of this statute. The state gets sued regularly by individuals who believe the state has violated the law. Individuals can do the same for violations of this statute.

5. Doesn't the requirement that the state act "knowingly" protect the state from negligent or inadvertent mistakes?

NO. 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.

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.

May 2, 2007

Good afternoon Chairman Ramras 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. I am here today representing the Alaska Bankers Association in reference to HB 65.

You should have all received a copy of a letter written to Representative Coghill by David Lawer, who is the current President of the Alaska Bankers Association and my purpose here today is 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 laws and statutes 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**

I have brought along this binder to show you one of our desk references for "Safeguarding Customer Information", a copy of which was given to Representative Coghill at the beginning of this session.

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 National Credit Union 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 national uniformity provisions
- Added two national uniformity provisions for identity theft prevention measures
- Established permanent preemption of state law related to these nine uniformity provisions:
    - 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 & third amendments as described in our letter are being partially taken care of with amendments submitted by Representative Coghill and we urge the committee to accept these amendments as presented.

Again, the Alaska Bankers Association's primary focus is to try to keep HB65 in line with federal regulations as much as possible. Nonetheless, we also want the committee to know that we support the bill and will not oppose it.

We also want to thank Representative Coghill for working with us on this bill.

Thank you for listening.

Craig E. Dahl, President & CEO
Alaska Pacific Bank
2094 Jordan Ave

(907 790-5101)

Jane Pierson

From: Ed Sniffen [Ed_Sniffen@law.state.ak.us]
Sent: Thursday, May 03, 2007 4:20 PM
To: Jane Pierson
Cc: Karen Lidster
Subject: HB 65 questions

Hi Jane! Great to meet you on Wednesday.

I see HB 65 is up on Saturday at 8:00 am. I wanted to make sure I had all of Rep. Ramras' questions about employer/employee liability answered before the hearing. He made some reference to the Holiday case, and questioned whether a business owner can be held liable for the actions of an employee. The Holiday case is very specific to a tobacco seller, and has no application to the liability imposed on businesses in HB 65. In Holiday, the court found that the automatic penalty and suspension provisions of AS 43.70.075(d) did not provide a business with sufficient "due process" to challenge the penalty. Under that statute, a tobacco seller is presumed to be responsible for an employee who is convicted of selling tobacco products to a minor, and is automatically issued a license suspension and a penalty.

HB 65 has no provisions like AS 43.70.075. Instead, "regular" principles of employment law will apply. Those laws say that an employer is responsible for the conduct of an employee while the employee is acting in the course and scope of his/her employment. The Alaska Supreme court in a recent case spelled out this liability in Laidlaw Transit v. Crouse, 53 P.3d 1093 (Alaska 2002). There, the Supreme Court held an employer can be responsible for the conduct of its employees, even when the employee does illegal things (in that case, the employee, a bus driver, was smoking marijuana and got in an accident).

In the context of HB 65, all employers will be responsible for the conduct of its employees that are acting in the course and scope of employment. Otherwise, the law would have no teeth. Every information collector, for example, could not be cited because all their activity is handled through employees. We would be left with going after only individual employees, and never be able to get at the business they work for. This would defeat the entire purpose of the bill. An employer can always argue that its employee was not acting in the course and scope of employment to avoid liability, but the Supreme Court has made that argument a tough one.

Let me know if the Representative has any further questions I can answer before Saturday's hearing.

Thanks!

Clyde "Ed" Sniffen, Jr.
Senior Assistant Attorney General
Commercial and Fair Business Section
Department of Law
1031 W. 4th Ave. #200
Anchorage, AK 99501
(907) 269-5100
(907) 276-8554 (fax)
Ed_Sniffen@law.state.ak.us

Amend #10
Remove 51C

Emily Stancliff

From: KRISTOPHER KNAUSS [knauss@gci.net]
Sent: Wednesday, May 02, 2007 9:53 PM
To: Rep. Jay Ramras
Subject: HB 65 Language

Attachments: ATT1081381.htm; AK HB 65 pci amd summary.doc


ATT1081381.htm (274 B)


AK HB 65 pci amd summary.doc (...

Jay,

Please consider amendments to HB 65 this Saturday.

Thanks,

Kris Knauss

ChoicePoint

Office of Government Affairs

May 2, 2007

The Honorable Jay Ramras, Chairman
House Judiciary Committee
State Capitol, Room 118
Juneau, AK 99801-1182

Re: Alaska House Bill 65

Dear Chairman Ramras:

It is my understanding that House Bill 65 will be considered by the House Judiciary Committee, and I am writing on behalf of ChoicePoint Inc. to offer comment. ChoicePoint provides information, identification, verification, and fraud prevention tools to insurance companies, employers, local, state and federal law enforcement agencies, and local, state, and federal government agencies.

Article 2. Credit Report and Credit Score Security Freeze

Article 9. General Provisions

Our comments relating to **Article 2** are directed at definitions used in the bill that would significantly and negatively alter the application and scope of the bill resulting in unintended consequence.

Specifically, our concerns are in **Article 9, Section 45.48.990**, and the definitional language used for "consumer credit reporting agency," "credit report" and "security freeze."

The provisions of Article 2 relating to credit report security freeze correctly apply to a "credit report" and a "consumer credit reporting agency." However, the actual definitional language used in Article 9, Section 45.48.990 for "credit report" and "consumer credit reporting agency" is overly broad. The result is the bill would capture non-credit information and databases that are used for fraud prevention and public safety purposes.

The current definitional language for the terms "credit report" and "consumer credit reporting agency" are identical to the definitions for a "consumer report" and a "consumer reporting agency" as defined in the federal Fair Credit Reporting Act. The two terms are not synonymous. The definitions for "consumer report" and "consumer reporting agency" in the federal FCRA are umbrella terms used to define all "consumer reports" regulated by the Federal Trade Commission, including data other than credit. In short, a credit report is a consumer report under the federal Fair Credit Reporting Act, but not all consumer reports involve credit data.

As you are undoubtedly aware, the public policy and legislative intent of "credit security freeze" legislation, dating back to its first passage in California, is to allow a consumer to "freeze" access to their credit report by third parties for credit transactions as an identity theft prevention tool.

1000 Alderman Drive Alpharetta, Georgia 30005 • (Tel) 770.752.6000 • (Fax) 770.619.8411

The early laws – California, Vermont, Louisiana - all reflect this public policy and legislative intent, providing for a "freeze" on a consumer's credit report, as do subsequent laws passed in states such as Washington, Pennsylvania, Connecticut, New York, and Illinois.

While this distinction may appear insignificant or technical in nature, the use of the definition of "consumer reporting agency" and "consumer report" as found in the federal FCRA would legislate requirements on consumer reports which have no credit data and are not used for credit-granting purposes, and on companies who are not credit reporting agencies and who do not maintain, collect, or house consumer credit data.

ChoicePoint provides employment, residential, and volunteer background screening services, which includes criminal and other non-credit information, that are regulated as consumer reports. In Alaska alone, numerous nonprofits benefit from background screening from ChoicePoint through our Volunteer*Select* program. The organizations we serve in Alaska include numerous churches and other religious organizations; Boys & Girls Clubs of Alaska, Big Brothers Big Sisters, and related youth support organizations; the Alaska State Hockey Association, Pop Warner Football, and other youth sports organizations.

Additionally, ChoicePoint provides various underwriting tools and information to insurers that are also regulated as "consumer reports" by the federal Fair Credit Reporting Act. Most notable is our C.L.U.E. report, a claims loss history report. A C.L.U.E. report does not contain consumer credit information nor is it used for credit-granting purposes.

However, ChoicePoint is not a "credit reporting agency." ChoicePoint does not maintain or house credit files or credit data on individual consumers. Further, ChoicePoint does not sell or produce credit reports that are utilized by third parties in consumer applications for credit cards, loans, or any retail consumer credit purchase.

For ChoicePoint and other consumer reporting agencies who are not credit reporting agencies, using the definitions for "consumer reporting agency" and "consumer report" would extend the "freeze" to reports which have no credit data, are not used for credit-granting purposes, and many of which are used for fraud prevention and public safety purposes. Thus, to legislate a freeze capability would allow the fraud prevention tool to become a fraud enabling tool.

The only reason a consumer would want or need to "freeze" a C.L.U.E. report or their criminal history is to commit insurance fraud, or to hide nefarious information. Otherwise, these reports have no value to identity thieves for credit or financial information.

Other states have reconciled the "consumer report" versus "credit report" issue with appropriate definitional and other language clarifying the scope and purpose of a "security freeze." I am including relevant examples of those definitions and provisions for your review and consideration.

Suggested Definitions

Article 2, Section 45.48.290

(4) "Security freeze" means a restriction placed on a consumer credit report at the request of the consumer that prohibits a consumer credit reporting agency from releasing all or any part of the consumer's credit report or any information derived from the consumer's credit report relating to the extension of credit without the express authorization of the consumer.

(Texas, South Dakota, Utah, Wisconsin, Kansas, Kentucky, Hawaii, Illinois, Minnesota, Oklahoma, Rhode Island, Wyoming, Arkansas, West Virginia, Mississippi laws; AZ, GA, OR, WA, NE, NM, MI bills)

Article 2, Sec. 45.48.200

(12) Any person or entity for use in setting or adjusting a rate, adjusting a claim, or underwriting for insurance purposes.

(Colorado, North Carolina, South Dakota, North Dakota, Wisconsin, Kansas, Kentucky, Vermont, Illinois, Florida, New Hampshire, Hawaii, Oklahoma, District of Columbia, Pennsylvania, Delaware, Mississippi, West Virginia, Arkansas laws; AZ, GA, MD, MI, MT, NE, VA bills)

Article 9, Sec. 45.48.990

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

(3) "Credit report" means any written, oral or other communication of any credit information by a credit reporting agency which operates or maintains a database of consumer credit information bearing on a consumer's credit worthiness, credit standing, or credit capacity."

Article 4. Protection of Social Security Numbers

ChoicePoint supports efforts to regulate the public display of a Social Security number to the general public by a business or commercial user. In addition, we support strong penalties for those who use SSNs to misappropriate the identities of others for fraud or to harm the individual.

However, Sections **45.48.410**, **45,48.420**, and **45.48.430** all establish over-reaching restrictions on beneficial and necessary law enforcement, government, business, and commercial use of SSN data, notwithstanding the limited exemptions provided.

Notwithstanding the current exemptions, the regulated uses that would currently be negatively impacted include those that occur under the federal Fair Credit Reporting Act, federal Gramm-Leach-Bliley Act, the federal Driver's Privacy Protection Act, verification and administration purposes, national and homeland security purposes, and fraud prevention.

Article 7. Consumer Credit Header Information

ChoicePoint opposes **Article 7** in its entirety. However, ChoicePoint does not oppose regulation of this data, which all ready occurs under existing stringent federal regulatory structure.

ChoicePoint provides information and verification products and services that rely on identifying information from credit headers. These products and services are used by law enforcement, government, private and charitable organizations, and business entities to detect and prevent fraud, and to locate, verify or authenticate a person's identity. Prohibiting or restricting access to header information would be a significant blow to the many important business and societal needs, including law enforcement, child support enforcement, homeland security, and more.

No state has a law regulating credit header information, and there are ample federal protections. Information commonly referred to as credit header information is strictly regulated by two federal laws: the federal Fair Credit Reporting Act (FCRA), 15 U.S.C. 1681 et seq. and the federal Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. 6801 et seq.

When the information is attached to a credit report, the information is governed by the FCRA. The permissible purposes sections of these laws are very narrowly tailored and designed to specifically limit who can obtain access to credit reports, including the "credit header" information in those reports, and under what circumstances.

When the information is not attached to a credit report, the information is regulated by GLBA. The GLBA limits the ability to transmit "credit header" information and allows for certain specific and societal beneficial uses. 15 U.S.C. 6802(e). This information can only be shared with known entities for specific uses permitted under the exemptions. Typically these uses are authentication and verification of identities, the prevention and detection of fraud, assessing institutional risk, and law enforcement investigations.

By restricting the access and use of this data, Alaska would be uniquely positioned as an outpo for fraudsters, criminals, and terrorists to avoid detection and location.

Alaska government, domestic Alaska businesses, and national and international companies that do business in Alaska utilize this data daily to combat fraud and crime:

- *Law enforcement*. Credit header information provides the most current contact information enabling law enforcement to locate witnesses and suspects, make arrests, thwart unlawful activities, and collect criminal fines.

- *Homeland Security*. The federal government relies heavily on credit header information to verify identity, thwart terrorist activity, and locate witnesses and suspects in connection with threats against our homeland.

- *Child Support Enforcement*. Credit header information is widely used by state government law enforcement agencies to locate deadbeat parents and enforce outstanding child support debts.

- *Financial Institutions*. Financial institutions use credit header information to comply with the US Patriot Act. This provision requires financial institutions to verify the identity of customers opening up new accounts.

- *Retailer fraud*. Credit header is used in the on-line and off-line environment to validate and authenticate a consumer's identity, so that fraudsters and criminals cannot impersonate legitimate buyers.

- *Insurance fraud*. Credit header data is critical in helping insurance companies prevent fraudulent insurance claims and are used widely to verify identity to ensure that insurance claims are not paid to undeserving individuals.

Thank you for your consideration of these issues. I would be happy to meet or speak with you at your convenience. I can be reached at 770-752-3383 during the day, and by email at Jon.Burton@ChoicePoint.com.

Sincerely,

Jon Burton, Vice President
State Government Relations

Consumers Union

136

To: Senator Gene Therriault, c/o Heather Brakes
From: Gail Hillebrand
Date: March 22, 2007
Re: Responses to ChoicePoint letter of March 14, 2007

Ms. Brakes asked me to provide information in response to the issues raised by ChoicePoint about SB 21 in their letter of March 14, focusing on Consumers Union's views on the implications of the changes sought by ChoicePoint, what other states have done, and any recommended compromise language.

Summary of recommendations:

- The defintional changes to consumer report, credit report, and security freeze sought by ChoicePoint would have adverse effects. SB 21 already uses an approach adopted elsewhere of exempting consumer reports that are of a specialty, non-account opening nature. SB 21 already exempts the types of screening reports that ChoicePoint offers as the reason for seeking definitional changes. No change in these definitions is recommended.

- The insurance exemption is found in some states and not others, but in some states it is narrower than what ChoicePoint has proposed. We offer language below.

- The restrictions related to sale, posting, and mailing of the Social Security numbers are similar to what many other states have done. Some states also restrict the collection of SSNs. We recommend no change in Article 4.

- In the spirit of compromise, the complex provisions of Article 7 could be deleted without undermining the remainder of the measure.

- Two technical changes in Article 2 on the security freeze would be valuable. The first is to delete the certified mail requirement for lifting the freeze, which is not commonly required in other states. The second is to require that resellers be obligated to honor a freeze already found on a consumer report which they purchase, so that the reseller exemption does not become a loophole. Other states take this approach.

1. ChoicePoint's proposals to change three basic definitions would create problems. SB 21 already contains an exemption to exclude screening for employees, tenants, criminal records, fraud prevention, and personal loss history. No other change is needed or desirable.

ChoicePoint's proposed narrowing of the definitions of consumer reporting agency, consumer report, and security freeze would reduce the security freeze solely to credit purposes. However, to be most effective in preventing the new account form of identity theft, the freeze should cover not only credit reports for credit purposes, but also any consumer report consulted for the purpose of opening a new account for the provision of goods or services for later payment. When an identity thief opens a new account for utilities or a phone and runs up an unpaid bill, this will reflect poorly on the consumer's credit record whether or not the account is technically a credit account. According to the Federal Trade Commission's January 2007 ID theft complaint

West Coast Office
1535 Mission Street • San Francisco, CA 94103
415.431.6747 Tel • 415.431.0906 Fax

report, more consumers complained in 2006 about the identity thieves opening fraudulent new accounts for cell phone, regular phone, and utility accounts than the number of consumers who complained about the opening of false new credit card accounts. In 2006, complaints about opening false new accounts for cell phone, regular phone, and utility accounts totaled 17.4% of ID theft complaints, while complaints about new credit card accounts comprised 15.2% of the total.

The issue raised by ChoicePoint about criminal, tenant, and employment screening plus fraud prevention has already been fully addressed in SB 21. Section 45.48.200(10) already exempts:

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

1. criminal record information;
2. personal loss history information;
3. fraud prevention or detection;
4. tenant screening; or
5. employment screening; or [Section 11 follows].

SB 21's approach is the same as Florida law. The Florida law, HB 37, section 501.005(12)(j), uses the same exempting language, for databases which are composed "entirely" of screening information and are used "solely" for one or more of the stated screening purposes. It also includes the same list of exempt purposes.

Florida's law states in relevant part:

(12) The provisions of this section do not apply to the use of a consumer report by the following persons or for the following reasons:

(j) A consumer reporting agency's database or file which consists entirely of information concerning, and is used solely for, one or more of the following:

1. criminal record information.
2. personal loss history information.
3. fraud prevention or detection.
4. tenant screening.
5. employment screening.

The full text of the Florida law can be found at:
http://www.myfloridahouse.gov/Sections/Documents/loaddoc.aspx?FileName=_h0037er.doc&DocumentType=Bill&BillNumber=0037&Session=2006

The Montana security freeze bill, which has cleared policy committees in both houses, uses the exact language as the Florida law, but with the exempted categories listed in a different order. The New Mexico legislature recently adopted similar language in a bill which has passed both houses and awaits the Governor's signature. The New Mexico bill applies to releases "from a consumer reporting agency's database or file that consists only of and is used solely for one or more of the following:" and then includes a similar list to the Florida list, although the New Mexico list omits "personal loss history."

Recommendation One: SB 21, Section 45.48.200 already exempts the use of identified types of specialty databases. The proposed changes to the definitions of consumer reporting agency, credit report, and security freeze should be rejected.

2. Adding an insurance exclusion raises two policy choices: should any exclusion be limited to underwriting rather than also covering claims adjusting, and should any exclusion expressly leave to other law questions of the appropriateness of using consumer credit information in making insurance decisions?

ChoicePoint also proposes exempting insurance uses from the freeze. States are going both ways on this issue, some are exempting some or all insurance uses, while others are including insurance uses consistent with the goal of giving consumers more ability to require consent before information from their consumer reporting files is made available to others.

ChoicePoint offers language that would exempt not only underwriting (pricing) but also "adjusting a claim." There are policy questions, quite apart from the freeze issues, about the appropriateness of using some types of consumer reporting information, such as bill payment patterns and credit usage patterns, to price insurance and to decide whether or how much to pay on insurance claims (claims adjusting).

Of the 28 security freeze laws enacted to date (27 states plus DC), ChoicePoint cites 15 as having an insurance exclusion. However, some of the states it cites have worded the exclusion more narrowly than the language ChoicePoint offers for Alaska.

ChoicePoint cites Oklahoma and Illinois, among other state laws, in support of its proposed language, but both of those states have a narrower exemption, reaching only: "Any person using the information in connection with the underwriting of insurance." (Omitting the "adjusting a claim" language.) North Carolina narrows the language in a different way with its exemption limited to property and casualty insurers.

ChoicePoint also cites a freeze bill in West Virginia. That bill contains an important addition to the exemption not included in the language proposed by ChoicePoint's March 14 letter. The West Virginia bill, SB 428, p. 8, section (j)(10) as enrolled, exempts insurance purposes "to the extent not otherwise prohibited by law." This clarifies that the freeze exemption is not independently authorizing these uses. The posted version of North Dakota's HB 1417 uses similar language, adding to its insurance exemption a statement that: "This exemption does not determine or affect whether these uses are permitted under other law."

The value of adding this type of language is that it makes it clear that any exclusion from the freeze does not decide the controversial issue of whether credit information is a proper source of information to use in setting insurance pricing.

Recommendation Two: If a decision is made to exclude insurance, the narrower way to do so is the Wyoming/Illinois approach which is limited to underwriting and not to claims. There should also be language to clarify that the exemption doesn't endorse this use of consumer report information. To do this, Article 2, Sec. 45.48.200 would be amended to add:

(12) a person using the information in connection with the underwriting of insurance. This exemption does not determine or affect whether such use is permitted under other law.

3. The Social Security number restrictions are important and should be retained in the bill

A number of states have provided their consumers with protection for their Social Security numbers which are similar to most of the protections found in SB 21.

Collection of SSNs restricted: Section 45.48.400 restricts the request and collection of individual SSNs. Other forms of identification may be sought. The closest state law is New Mexico, which prohibits businesses from requiring an SSN unless it will be used in a manner consistent with state or federal law or as part of an application for credit or in connection with an annuity or insurance. N.M. Stat. Ann. § 57-12-3. For obligations on government agencies not to collect SSNs, see North Carolina law, which says that no government agency shall "collect social security number from an individual unless authorized by law to do so or unless the collection of the social security number is otherwise imperative for the performance of that agency's duties and responsibilities as prescribed by law. Social security numbers collected an agency must be relevant to the purpose for which collected and shall not be collected unt and unless the need for social security numbers has been clearly documented." N.C. Gen. Stats. Sec. 132-1.8(b)(1).

Posting, display, use on cards, and mailing of SSNs restricted: Section 45.48.400 restricts making available to the public an SSN, printing the SSN on a card required for access to products or services, requiring internet transmission of non-encrypted SSNs, requiring the us to access an Internet site unless another PIN or password is also used, and printing an SSN on certain mailed materials, with exceptions for some types of mailings. This is a very standard list of restrictions, found in many other state laws. Some states adopt the full list, such as Colorado, North Carolina, Rhode Island, Illinois, Pennsylvania, Arizona, New Mexico, Minnesota and California, in statutes similar to Section 45.48.400 with some variations in the wording of the mailing section. New Jersey and Hawaii also prohibit all of these uses, with slight variations in the statutory wording. Additional states such as Connecticut and Virginia have a similar list but omit the restriction on the mailing of SSNs.

Sale of SSNs: Section 45.48.420 restricts sale, lease, loan and rental of SSNs, with exceptions for express authorization by law and for requests to consumer reporting agencies for reports. This section is stronger than that found in the current laws of other states. North Carolina law does require an individual's written consent before the intentional sale, lease, loan, rent or trade of an SSN, but only where the party making the disclosure "knows or in the exercise of reasonable diligence would have reason to believe that the third party lacks a legitimate purpose for obtaining the individual's social security number." N.C. Gen. Stats. § 75-62(a)(6).

Other disclosure: Section 45.48.430 prevents the disclosure of SSNs, with exceptions. There are exceptions where authorized by law, the disclosure is to a financial institution to facilitate a transaction of the individual, the disclosure is part of a request to a consumer reporting agency for a report or the disclosure is for a background check or law enforcement purposes. In general, the SSN should not be needed outside of the contexts of credit, employment, taxes, and investment. All of those uses should fall under one of the exemptions already found in section 45.48.430.

Recommendation Three: Consumers Union recommends that no change be made in the Social Security number sections of the bill.

4. Article 7 on consumer credit header information addresses a real issue but could be eliminated without damage to the rest of the bill.

The restriction on the provision of credit header information was included in the Consumers Union/US PIRG model anti-ID theft law at the request of our partner in the effort, US PIRG. The section addresses a real problem – that consumer reporting agencies offer access to individual's Social Security numbers which they maintain in databases containing Social Security numbers that were pulled from credit reports before the federal Gramm Leach Bliley Act went into effect, or which have been added later after a consent from the consumer to the sharing of personal information. The information in the credit header database then can be sold free of the restrictions which apply to the sale of consumer reports. Article 7 is designed to change that result.

Recommendation Four: While we believe that the sale of SSNs pulled from credit headers is an important issue, it is one that Alaska might choose not to be the pioneering state in addressing. If you are looking for areas in which to respond to the ChoicePoint proposals in a spirit of compromise, Article 7 could be removed from the bill without doing damage to the remainder of the measure.

5. Two technical changes in the security freeze section are needed. HB 65 Page 7 line 15

SB 21, page 9, line 30, requires the use of certified mail to lift or remove a security freeze when mail is the method by which removal is requested. While many states require certified mail to place the freeze, they do not require it to lift the freeze, but instead permit regular mail as the form of mail to be used, along with the unique PIN, to lift or remove the freeze.

Consumers Union believes that certified mail is an unnecessary hurdle to the use of a freeze even with respect to placement of the freeze. Whatever choice is made about requiring certified mail for placing the freeze, consumers should be able to lift and remove the freeze using regular mail.

Recommendation Five: Delete "certified" in SB 21 at page 9, line 30.

The other technical change is to add a requirement commonly found in other state freeze laws that exempt resellers must honor a freeze already in place on a consumer reporting file. SB 21 exempts resellers from an obligation to place, lift or remove a security freeze. However, it omits the commonly found requirement that a reseller honor a freeze placed at the CRA from whom the reseller acquires the report. Other state laws generally require that resellers honor a security freeze. For example, California law exempts resellers but adds: "However, a consumer credit reporting agency acting pursuant to [the reseller section] shall honor any security freeze placed on a consumer credit report by another consumer credit reporting agency. Cal Civil Code §1785.11.4. Minnesota law is similar. It exempts resellers and then states: However, a consumer reporting agency must honor any security freeze placed on a consumer report by another consumer reporting agency." Minn. Stats 13C.018.

Recommendation Six: In SB 21, page 14, line 21, add: "However, a consumer reporting agency must honor any security freeze placed on a consumer report by another consumer reporting agency."

Thank you for soliciting comments from Consumers Union. If we can provide any further information, please contact Gail Hillebrand or Michelle Jun at (415) 431-6747, or hillga@consumer.org and junmich@consumer.org.

415-431-0906 Fax

AARP Alaska

May 1, 2007

The Honorable Jay Ramras, Chair
House Judiciary Committee
Alaska State Capitol, Room 118
Juneau, Alaska 99801-1182

HB 65 (Coghill and Gara)—Support

Dear Chair Ramras:

On behalf of the members of AARP in Alaska, we urge you and your colleagues on the House Judiciary Committee to support HB 65, authored by your Committee colleague Representative John Coghill and Representative Les Gara and co-sponsored by you and your Committee members Representatives Bob Lynn and Ralph Samuels as well as Representatives Fairclough, Kawasaki, Kerttula, Gatto, Neuman and Olson. This bill builds on much of the excellent work done last year 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 Nancy Dahlstrom
Representative John Coghill
Representative Ralph Samuels
Representative Max Gruenberg
Representative Lindsey Holmes
Representative Bob Lynn
Representative Les Gara
Senator Gene Therriault

Sec. 28.10.505. Disclosure of personal information contained in motor vehicle records.

(a) Notwithstanding AS 40.25.300 and except as provided in this section, the department may not disclose personal information contained in motor vehicle records maintained by the department under this chapter.

(b) Personal information shall be disclosed for use in connection with matters of motor vehicle or driver safety or theft; motor vehicle emissions; motor vehicle product alterations, recalls, or advisories; performance monitoring of motor vehicles and dealers by motor vehicle manufacturers; and removal of nonowner records from the original owner records of motor vehicle manufacturers as required by federal law.

(c) Personal information may be disclosed if the requesting person demonstrates, in a form and manner the department prescribes, that the requesting person has obtained the written consent of the person who is the subject of the information.

(d) Personal information may be disclosed by the department upon proof of the identity of the person requesting a record and representation by the requesting person that the use of the personal information is strictly limited to one or more of the following uses:

(1) for use by a government agency, including a court or law enforcement agency, in carrying out its functions, or a private person or entity acting on behalf of a government agency in carrying out its functions;

(2) for use in the normal course of business by a legitimate business or an agent, employee, or contractor of the business, but only

(A) to verify the accuracy of personal information submitted by an individual to the business or an agent, employee, or contractor of the business; and

(B) if the information submitted is not correct, to obtain the correct information, but only for the purposes of preventing fraud by pursuing legal remedies against, or recovering on a debt or security interest against, an individual;

(3) for use in connection with a civil, criminal, administrative, or arbitration proceeding in a court or government agency or before a self-regulatory body, including service of process and the execution or enforcement of a judgment or court order;

(4) for use in research activities, or in producing statistical reports, if the personal information is not published, redisclosed, or used to contact an individual;

(5) for use by an insurer or insurance support organization, or by a self-insured entity, or an agent, employee, or contractor of an insurer, in connection with claims investigation activities, anti-fraud activities, rating, or underwriting;

(6) for use in providing notice to the owners of towed or impounded vehicles;

(7) for use by an employer or an agent or insurer of an employer to obtain or verify information relating to a holder of a commercial driver's license that is required under 49 U.S.C. 31101 - 31162 (Commercial Motor Vehicle Safety Act);

(8) for use in connection with the operation of private toll transportation facilities;

(9) for use in connection with a legitimate business operating under a contract with the department;

(10) for bulk distribution for surveys, marketing, or solicitations if the person who is the subject of the information has provided written consent to the release; and

(11) for any other purpose specifically authorized by law that is related to the operation of a motor vehicle or related to public safety.

(e) Personal information contained in an individual record may be disclosed, without regard to the intended use of the personal information, if the person who is the subject of the information has provided written consent to the release.

(f) In this section,

(1) "disclose" means to engage in a practice or conduct that makes available or makes known personal information contained in records of the department about a person to another person, organization, or entity by any means of communication;

(2) "individual record" means a record containing personal information about a designated person who is the subject of the record, as identified in a request for information;

(3) "personal information" means information that identifies a person, including a name, address, telephone number, and medical or disability information, but does not include information on vehicular accidents, driving- or equipment-related violations, driver's license or registration status, or a zip code.

Sec. 28.10.510. - 28.10.540l Liens; nonresident owners. [Repealed, Sec. 7 ch 178 SLA 1978].

Repealed or Renumbered

Article 2
Disclosure Requirements

Section
200. Public information principles.
210. Access to records; rights; requirements; format.
220. Requestor's justification or need for records.
230. Nondiscrimination.
240. Reasonable fees required.

2 AAC 96.200. Public information principles

Statute text
(a) It is the policy of the executive branch of government to disclose public records and to provide copies of those records in an expeditious manner. Disclosing public records and making copies of them upon payment of the required fees, if any, is a public agency obligation.

(b) It is the policy of the executive branch of government to limit the collection of personal information only to that data necessary for the efficient administration of a public agency.

(c) To ensure that public information is widely available to the public, public agencies are to comply with AS 40.25.115(e) regarding submission of information to the Alaska State Library about

(1) public information that a public agency collects, compiles, or publishes, including information regarding databases used by the agency to maintain public records; and

(2) information about the electronic services and products routinely provided to the public, the public agency shall provide information to the Alaska State Library when electronic services and products are made available to the public and when electronic services or products of that public agency are substantially modified.

2 AAC 96.210. Access to records; rights; requirements; format

Statute text
(a) Subject to the provisions of AS 40.25.110 - 40.25.220, a public record maintained by a public agency is available for inspection and copying in the format in which that agency maintains or disseminates the record. A public agency shall duplicate and provide copies

of a public record upon request and upon payment of the applicable fee as described by this chapter.

(b) A public agency is not required to compile or summarize its public records in response to a request for public records.

(c) A public agency is not required to manipulate its data to create new records in response to a request for public records. A public agency may manipulate its data to create electronic services and products if

(1) the public agency can do so without impairing its functioning;

(2) the data is protected from intentional or accidental modification or destruction; and

(3) the requestor pays for the cost of developing the requested electronic service or product, based on fees established by the public agency under 2 AAC 96.460.

(d) When providing public records or electronic services or products, a public agency shall ensure that access to confidential information and proprietary software is protected. Except as provided by law, if the request is for a public record that contains confidential information, the public agency shall delete or mask the nondisclosable confidential information and provide the requested public records upon payment of the applicable fee as described in 2 AAC 96.360.

2 AAC 96.220. Requestor's justification or need for records

Statute text
All disclosable public records must be made available upon request and upon compliance with the requirements of AS 40.25.110 - AS 40.25.125 and this chapter. A public agency may not request a justification or explanation of need or intended use, but a public agency may inquire whether the person making the request is a party, or represents a party, involved in litigation with the state or a public agency to which the requested record is relevant. If so, the requestor shall be informed to make the request in accordance with applicable court rules.

2 AAC 96.230. Nondiscrimination

Statute text

When providing public records or electronic services and products, a public agency may not discriminate among requestors or classes of requestors, such as academic researchers, state and federal agencies, members of the public, news organizations, genealogists, or nonprofit groups.

2 AAC 96.240. Reasonable fees required

Statute text

(a) A public agency may establish a fee schedule for duplicating public records, and shall establish a fee schedule for providing electronic services and products. Fees shall be consistent with AS 40.25.110, AS 40.25.115, and this chapter.

(b) The fees developed by a public agency to provide electronic services and products may not be set at a level necessary to recover all development and operational costs of the public agency's information system, unless the system exists solely for responding to requests for public records.

(c) Fees may not be assessed as a condition of inspecting public records if the public agency receiving the request does not incur costs to search for the requested public record.

HOUSE COMMITTEE REPO[redacted]

(7)
Date Referred to Committee: April 24, 2007 **FURTHER REFERRALS: Finance**

Date of Committee Action: May 5 2007

The JUDICIARY Committee considered: **HB 65**

HOUSE BILL NO. 65 **PERSONAL INFORMATION & CONSUMER CREDIT**

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

Recommends it be replaced with | | HCS *or* | ✓ | CS *for* HB65 (JUD)
***For Senate Bills with new title:* | | *Technical Title* | | *New Title: HCR*_____ | | Same Title | ✓ | New Title**

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

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

NEW **FISCAL NOTES** *Assigned by Chief Clerk's Office				
List by Dept(s):	*FN#	Fiscal	Indet.	Zero

PREVIOUS **FISCAL NOTES**				
List by Dept(s):	FN#	Fiscal	Indet.	Zero
ADM	2	✓		
[redacted]	1		✓	

Signing with recommendations	Printed Last Name	DP	DNP	NR	AM
	Holmes	X			
	Cynthia	X			
	Coghill	✓			
	[redacted]				X
	SAMUELS				X
Chair:	RAMRAS	X			
Chair:					

ALASKA STATE LEGISLATURE
HOUSE JUDICIARY COMMITTEE

Representative Jay Ramras
Chairman
(907) 465-3004
Fax: (907) 465-2070
Representative_Jay_Ramras@legis.state.ak.us

1292 Sadler Way, Suite 324
Fairbanks, AK 99701

Committee Members:
Representative Nancy Dahlstrom,
Vice-Chairman
Representative John Coghill
Representative Bob Lynn
Representative Ralph Samuels
Representative Max Gruenberg
Representative Lindsey Holmes

State Capitol Room 120
Juneau, Alaska 99801-1182

Fax

To: Leg. Legal

Fax #: 2029 Number of pages including cover:

From: Jane Pierson

Date: May 2, 2007

Re: HB65 version \E

Please draft a HJUD CS for the above-referenced bill with attached amendments. We will be taking the bill up again on Saturday, May 5, 2007.

Thank you.

25-LS0311\E.6
Bannister
4/30/07

AMENDMENT #2 ADOPT.

OFFERED IN THE HOUSE

TO: CSHB 65(L&C)

Page 7, line 5:

Delete "AS 45.48.160(b)"

Insert "AS 45.48.160(c)"

Page 10, line 15:

Delete "(b) or (c)"

Insert "(b), (c), or (d)"

Page 10, following line 20:

Insert a new subsection to read:

"(b) A consumer credit reporting agency may charge a consumer $2 for placing a security freeze."

Page 10, line 21:

Delete "(b)"

Insert "(c)"

Page 10, line 27:

Delete "(c)"

Insert "(d)"

Page 11, line 8:

Delete "at no charge"

Insert "for $10"

25-LS0311\E.9
Bannister
4/30/07

AMENDMENT #3 ADOPT

OFFERED IN THE HOUSE

TO: CSHB 65(L&C)

Page 10, line 2:

Delete "certified"

Page 10, line 8:

Delete "certified"

Page 12, line 16, following "mail.":

Insert "Under some circumstances, the consumer credit reporting agency may charge you $2 to temporarily lift the freeze."

AK BANKERS.

25-LS0311\E.3
Bannister
5/1/07

AMENDMENT #4

Delete ART 3.
ADOPT

OFFERED IN THE HOUSE

TO: CSHB 65(L&C)

Page 1, line 2:

Delete "**consumer credit monitoring, credit accuracy,**"

Page 15, line 29, through page 18, line 23:

Delete all material.

Page 18, line 24:

Delete "**Article 4**"

Insert "**Article 3**"

Page 22, line 21.

Delete "**Article 5**"

Insert "**Article 4**"

Page 25, line 22:

Delete "**Article 6**"

Insert "**Article 5**"

Page 27, line 31:

Delete "**Article 7**"

Insert "**Article 6**"

Page 28, line 16:

Delete "**Article 8**"

Insert "**Article 7**"

Page 29, line 13:

Delete "**Article 9**"

Insert "**Article 8**"

25-LS0311\E.2
Bannister
5/2/07

#5 ADOPT

AMENDMENT

OFFERED IN THE HOUSE

TO: CSHB 65(L&C)

Page 25, lines 10 - 16:

Delete all material and insert:

"(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, address, or telephone number; and

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

MUST BE SAME AS EXPLICIT

ADOPT

25-LS0311\E.13
Bannister
5/2/07

#6

AMENDMENT

OFFERED IN THE HOUSE

TO: CSHB 65(L&C)

Page 25, line 30, following "theft":

Delete ";"

Insert "by the victim; and"

Page 26, line 10:

Delete "shall"

Insert "may"

Page 26, lines 11 - 18:

Delete all material.

Insert "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."

Page 26, line 25:

Delete "deleted, sealed, or"

Page 26, line 30:

Delete "or fraudulent material"

Insert ", omission, or false information"

ADOPT

25-LS0311\E.14
Bannister
5/2/07

#7

AMENDMENT

OFFERED IN THE HOUSE

TO: CSHB 65(L&C)

Page 1, line 4:

Delete "**furnishing consumer credit header information,**"

Page 27, line 31, through page 28, line 15:

Delete all material.

Page 28, line 16:

Delete "**Article 8**"

Insert "**Article 7**"

Page 29, line 13:

Delete "**Article 9**"

Insert "**Article 8**"

(b) The department shall disclose applicant information to a business under a contract with the department that requests the applicant information if the business has a license under AS 43.70.020, the business, or an agent, an employee, or a contractor of the business, indicates that the business will use the applicant information only in the normal course of business, the person making the request provides proof of the person's identity, and the person making the request states that the business will use the applicant information only

(1) to obtain information for law enforcement agencies or for an investigation, if the business is the practice of law or includes the service of process;

(2) in connection with a civil, a criminal, an administrative, or an arbitration proceeding, including the service of process, investigation in anticipation of litigation, executing on a judgment, enforcing a judgment, or complying with a court order;

(3) for a legal or beneficial interest relating to the applicant, if the business holds the legal or beneficial interest;

(4) on behalf of the applicant, if the business is acting in a fiduciary capacity on behalf of the applicant;

(5) in connection with insurance claims, insurance investigations, or insurance anti-fraud activities, if the business is an insurer or a person who provides support services to an insurer;

(6) to comply with federal, state, or municipal laws, regulations, ordinances, or other legal requirements; or

(7) for bulk distribution to political candidates, nonprofit organizations, or persons taking polls.

(c) In this section,

(1) "applicant" means an applicant for a permanent fund dividend;

(2) "applicant information" means name, mailing address, and birth year of an applicant;

(3) "business" means a person engaging in business."

Renumber the following bill sections accordingly.

Page 27, line 23:

Delete "sec. 3"

Insert "sec. 5"

Page 27, line 27:

Delete "sec. 3"

Insert "sec. 5"

Page 27, line 30:

Delete "sec. 3"

Insert "sec. 5"

Page 28, line 1:

Delete "sec. 4"

Insert "sec. 6"

ADOPT

25-LS0311\E.4
Bannister
5/1/07

#8

AMENDMENT

OFFERED IN THE HOUSE

TO: CSHB 65(L&C)

Page 1, line 5:

Delete "**Rule 60**"

Insert "**Rules 60 and 82**"

Page 22, line 16:

Delete "and court costs and attorney fees"

Insert "court costs"

Page 22, line 17, following "court":

Insert ", and full reasonable attorney fees"

Page 30, line 24:

Delete "AMENDMENT."

Insert "AMENDMENTS. (a)"

Page 30, following line 27:

Insert a new subsection to read:

"(b) AS 45.48.480(b), enacted by sec. 3 of this Act, has 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 45.48.480(b)."

ADOPT

25-LS0311\E.5
Bannister
5/1/07

#9

AMENDMENT

OFFERED IN THE HOUSE

TO: CSHB 65(L&C)

Page 19, following line 28:

Insert a new paragraph to read:

"(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;"

Renumber the following paragraphs accordingly.

Page 20, following line 23:

Insert a new paragraph to read:

"(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;"

Renumber the following paragraphs accordingly.

ADOPT

25-LS0311\E.7
Bannister
5/1/07

AMENDMENT #11

OFFERED IN THE HOUSE

TO: CSHB 65(L&C)

Page 20, following line 17:

Insert a new subsection to read:

"(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."

Page 22, lines 18 - 20:

Delete all material.

Reletter the following subsection accordingly.

ADOPT

25-LS0311\E.8
Bannister
4/30/07

AMENDMENT #12

OFFERED IN THE HOUSE

TO: CSHB 65(L&C)

Page 20, line 4:

Delete "or"

Page 20, line 7, following "benefits":

Insert "; or

(5) if the disclosure does not have independent economic value, is incidental to a larger transaction, and is necessary to verify the identity of the individual"

HELD

25-LS0311\E.12
Bannister
5/1/07

AMENDMENT #1

Rep. Kawasaki

OFFERED IN THE HOUSE

TO: CSHB 65(L&C)

M6
BL
JC
JR
ND
RS
LH

Page 1, line 1, following "**to**":

Insert "**the disclosure of permanent fund dividend applicant records,**"

Page 2, following line 3:

Insert new bill sections to read:

"*** Sec. 2.** AS 43.23.017 is amended to read:

Sec. 43.23.017. Applicant information confidential. Information on each permanent fund dividend application, except the applicant's name, is confidential. The department may only release information that is confidential under this section

(1) to a local, state, or federal government agency;

(2) in compliance with a court order;

(3) to the individual who or agency that files an application on behalf of another;

(4) to a banking institution to verify the direct deposit of a permanent fund dividend or correct an error in that deposit;

(5) as directed to do so by the applicant; [AND]

(6) to a contractor who has a contract with a person entitled to obtain the information under (1) - (5) of this section to receive, store, or manage the information on that person's behalf; a contractor receiving data under this paragraph may only use the data as directed by and for the purposes of the person entitled to obtain the information**; and**

(7) as provided under (b) of this section.

*** Sec. 3.** AS 43.23.017 is amended by adding new subsections to read:

(b) The department shall disclose applicant information to a business that requests the applicant information if the business has a license under AS 43.70.020, the business, or an agent, an employee, or a contractor of the business, indicates that the business will use the applicant information only in the normal course of business, the person making the request provides proof of the person's identity, and the person making the request states that the business will use the applicant information only

(1) as necessary to implement or enforce a transaction authorized by the applicant;

(2) to obtain information from law enforcement agencies or self-regulatory organizations or for an investigation, if the business is the practice of law or includes the service of process;

(3) in connection with a civil, a criminal, an administrative, or an arbitration proceeding, including the service of process, investigation in anticipation of litigation, executing on a judgment, enforcing a judgment, or complying with a court order;

(4) for a legal or beneficial interest relating to the applicant, if the business holds the legal or beneficial interest;

(5) on behalf of the applicant, if the business is acting in a fiduciary capacity on behalf of the applicant;

(6) to verify the accuracy of information provided by the applicant, to prevent fraud by the applicant, or to pursue legal remedies against the applicant;

(7) in connection with insurance claims, insurance investigations, or insurance anti-fraud activities, if the business is an insurer or a person who provides support services to an insurer;

(8) to comply with federal, state, or municipal laws, regulations, ordinances, or other legal requirements; or

(9) for bulk distribution to political candidates, nonprofit organizations, or persons taking polls.

(c) In this section,

(1) "applicant" means an applicant for a permanent fund dividend;

(2) "applicant information" means name, mailing address, and birth

year of an applicant;

(3) "business" means a person engaging in business."

Renumber the following bill sections accordingly.

Page 30, line 24:

Delete "sec. 3"

Insert "sec. 5"

Page 30, line 28:

Delete "sec. 3"

Insert "sec. 5"

Page 30, line 30:

Delete "sec. 4"

Insert "sec. 6"

Bill contains 3 sections
Sec. 1 – Care of Records

Sec. 2 – Adds a new paragraph to AS 44.64.030 – *Breach of Security involving personal information*

Sec. 3 – Amends AS 45 adding a new chapter -
Chapter 48 – *Personal Information Protection Act*

Within new Chapter 48 – are 9 Articles

Article 1. Breach of Security Involving Personal Information

Article 2. Credit Report and Credit Score Security Freeze

~~**Article 3. Consumer Credit Monitoring; Credit Accuracy**~~

Article 4.3 Protection of Social Security Number

Article 5.4 Disposal of Records

Article 6.5 Factual Declaration of Innocence after Identify Theft, Right to file Police Report Regarding Identity Theft

Article 7.6 Consumer Credit Header Information

Article 8.7 Truncation of Card Information

Article 9.8 General Provisions

ADOPT

M

25-LS0311\E.15
Bannister
5/2/07

AMENDMENT #10

OFFERED IN THE HOUSE

TO: CSHB 65(L&C)

20 9-10

Page ~~22~~, lines ~~15-16~~:

Delete "or $5,000, whichever amount is greater,"

Amend #13

p. 23, L 24 - Delete "by the victim"

25-LS0311\M.4
Bannister
5/4/07

#1

AMENDMENT

N - N
C - Y
S - Y
L - Y
H - N
G - N
R - Y

4-3 ADOPTED

OFFERED IN THE HOUSE

TO: CSHB 65(JUD), Draft Version "M"

Page 1, line 1, following "to":

Insert "**the disclosure of permanent fund dividend applicant records,**"

Page 2, following line 2:

Insert new bill sections to read:

"* **Sec. 2.** AS 43.23.017 is amended to read:

Sec. 43.23.017. Applicant information confidential. Information on each permanent fund dividend application, except the applicant's name, is confidential. The department may only release information that is confidential under this section

(1) to a local, state, or federal government agency;

(2) in compliance with a court order;

(3) to the individual who or agency that files an application on behalf of another;

(4) to a banking institution to verify the direct deposit of a permanent fund dividend or correct an error in that deposit;

(5) as directed to do so by the applicant; [AND]

(6) to a contractor who has a contract with a person entitled to obtain the information under (1) - (5) of this section to receive, store, or manage the information on that person's behalf; a contractor receiving data under this paragraph may only use the data as directed by and for the purposes of the person entitled to obtain the information; **and**

(7) as provided under (b) of this section.

* **Sec. 3.** AS 43.23.017 is amended by adding new subsections to read:

(b) The department shall disclose applicant information to a business under a contract with the department that requests the applicant information if the business has a license under AS 43.70.020, the business, or an agent, an employee, or a contractor of the business, indicates that the business will use the applicant information only in the normal course of business, the person making the request provides proof of the person's identity, and the person making the request states that the business will use the applicant information only

(1) to obtain information for law enforcement agencies or for an investigation, if the business is the practice of law or includes the service of process;

(2) in connection with a civil, a criminal, an administrative, or an arbitration proceeding, including the service of process, investigation in anticipation of litigation, executing on a judgment, enforcing a judgment, or complying with a court order;

(3) for a legal or beneficial interest relating to the applicant, if the business holds the legal or beneficial interest;

(4) on behalf of the applicant, if the business is acting in a fiduciary capacity on behalf of the applicant;

(5) in connection with insurance claims, insurance investigations, or insurance anti-fraud activities, if the business is an insurer or a person who provides support services to an insurer;

(6) to comply with federal, state, or municipal laws, regulations, ordinances, or other legal requirements; or

(7) for bulk distribution to political candidates, nonprofit organizations, or persons taking polls.

(c) In this section,

(1) "applicant" means an applicant for a permanent fund dividend;

(2) "applicant information" means name, mailing address, and birth year of an applicant;

(3) "business" means a person engaging in business."

Renumber the following bill sections accordingly.

Page 27, line 23:
Delete "sec. 3"
Insert "sec. 5"

Page 27, line 27:
Delete "sec. 3"
Insert "sec. 5"

Page 27, line 30:
Delete "sec. 3"
Insert "sec. 5"

Page 28, line 1:
Delete "sec. 4"
Insert "sec. 6"

New #2 to Amend #1 FAILED

By: Lynn + Gruenberg

Amendment to Amendment ___ to CSHB 65 (JUD)
(#25-LS0311\M.4")

page 2 line 24

Party or candidate

Add:

"Applicant information for bulk distribution to political candidates in an election shall also be disclosed directly to a candidate who has filed a party ~~directly~~ a declaration of candidacy or letter of intent or a recognized political to run in that ~~race~~ election."

2-5 FAILED

New Amendment 2 to Amendment 1 to CSHB 65 (JUD) By: Lynn + Gruenberg
(#25-LS0311\M.4")

page 2 line 24

Add:

"Applicant information for bulk distribution to political candidates in an election shall also be disclosed directly to a candidate who has filed a ~~directly~~ a declaration of candidacy a letter of intent to run in that ~~race~~ election." or to a recognized political party

Conform the rest of the amendment accordingly

W/D

25-LS0311\M.2
Bannister
5/4/07

11

AMENDMENT

OFFERED IN THE HOUSE BY REPRESENTATIVE RAMRAS

TO: CSHB 65(JUD), Draft Version "M"

Page 26, lines 29 - 30:

Delete "assembling or evaluating consumer credit information or other information on consumers"

Insert "maintaining consumer credit information"

to any person related by common ownership or affiliated by corporate control, if the information is--

(A) medical information;

(B) an individualized list or description based on the payment transactions of the consumer for medical products or services; or

(C) an aggregate list of identified consumers based on payment transactions for medical products or services.

(e) The term "investigative consumer report" means a consumer report or portion thereof in which information on a consumer's character, general reputation, personal characteristics, or mode of living is obtained through personal interviews with neighbors, friends, or associates of the consumer reported on or with others with whom he is acquainted or who may have knowledge concerning any such items of information. However, such information shall not include specific factual information on a consumer's credit record obtained directly from a creditor of the consumer or from a consumer reporting agency when such information was obtained directly from a creditor of the consumer or from the consumer.

(f) The term "consumer reporting agency" means any person which, 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 consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports.

(g) The term "file," when used in connection with information on any consumer, means all of the information on that consumer recorded and retained by a consumer reporting agency regardless of how the information is stored.

(h) The term "employment purposes" when used in connection with a consumer report means a report used for the purpose of evaluating a consumer for employment, promotion, reassignment or retention as an employee.

(i) The term "medical information" --

(1) means information or data, whether oral or recorded, in any form or medium, created by or derived from a health care provider or the consumer, that relates to--

(A) the past, present, or future physical, mental, or behavioral health or condition of an individual;

(B) the provision of health care to an individual; or

(C) the payment for the provision of health care to an individual.

Norman Cohen

From: Everett Robbins [president@apdea.org]
Sent: Monday, February 05, 2007 1:54 PM
To: Norman Cohen
Subject: RE: HB 67 - Municipal Property Tax Exemption for Law Enforcement Officers

Rep. Max Gruenberg
State Capitol, Room 110
Juneau, AK 99801

Dear Representative Gruenberg:

I am writing in support of the municipal tax exemption for law enforcement officers (House Bill 67). This legislation would allow a municipality to enact an ordinance designating eligible parcels of property exempt from taxation up to $150,000 of the assessed value of the property. Eligible parcels of property are those (1) that are owned by and constitute the primary residence of a law enforcement officer; (2) that meet the eligibility requirements under a federal program of special assistance; and (3) that have a statistically higher occurrence of crime that the municipality as a whole.

We believe this bill would be instrumental in helping to reduce crime throughout Anchorage while also recognizing the contributions that law enforcement officers make in our communities. This bill would help to foster the concept of community policing by providing an incentive for law enforcement officers to work and live in neighborhoods most in need of police interaction and intervention. This bill may well help to relieve the economic costs to the municipalities, as well as private employers and individuals, that are generally associated with high-crime neighborhoods by encouraging law enforcement officers to insert themselves into their communities and assume a personal stake in the future of the neighborhood. The bill is also an important recognition of the services provided by individual law enforcement officers. In short, we believe this bill would be beneficial from both the public's perspective and any individual law enforcement officer who participates in the program.

Thank you for introducing this bill into the Alaska legislature. If it passes, Alaska will lead the way in recognizing the contributions that law enforcement officers make in our communities and the benefit that can be derived from permitting a property exemption for those officers who demonstrate their commitment to community policing. Please convey my wholehearted support for its passage to the relevant legislative committees and leaders of each chamber.

Sincerely,

Everett Robbins
President
Anchorage Police Department Employee's Association

25-LS0311\M.3
Bannister
5/4/07

#12 JUD

AMENDMENT

OFFERED IN THE HOUSE BY REPRESENTATIVE RAMRAS

TO: CSHB 65(JUD), Draft Version "M"

Page 27, lines 1 - 11:

Delete all material and insert:

"(3) "credit report" means a written, oral, or other communication of credit information by a consumer credit reporting agency bearing on a consumer's credit worthiness, credit standing, or credit capacity;"

enforcement agency about unlawful use of his or her personal information by another person.

(o) If a security freeze is in place, a consumer reporting agency shall not change any of the following official information in a credit report without sending a written confirmation of the change to the consumer within 30 days of the change being posted to the consumer's file: (i) name, (ii) date of birth, (iii) Social Security number, and (iv) address. Written confirmation is not required for technical modifications of a consumer's official information, including name and street abbreviations, complete spellings, or transposition of numbers or letters. In the case of an address change, the written confirmation shall be sent to both the new address and to the former address.

(p) The following entities are not required to place a security freeze in a consumer report, however, pursuant to paragraph (3) of this subsection, a consumer reporting agency acting as a reseller shall honor any security freeze placed on a consumer credit report by another consumer reporting agency:

(1) A check services or fraud prevention services company, which issues reports on incidents of fraud or authorizations for the purpose of approving or processing negotiable instruments, electronic funds transfers, or similar methods of payment.

(2) A deposit account information service company, which issues reports regarding account closures due to fraud, substantial overdrafts, ATM abuse, or similar negative information regarding a consumer to inquiring banks or other financial institutions for use only in reviewing a consumer request for a deposit account at the inquiring bank or financial institution.

(3) A consumer reporting agency that:

(A) acts only to resell credit information by assembling and merging information contained in a database of one or more consumer reporting agencies; and

(B) does not maintain a permanent database of credit information from which new credit reports are produced.

(q) For purposes of this Section:

"Credit report" has the same meaning as "consumer report", as ascribed to it in 15 U.S.C. § 1681a(d).

"Consumer reporting agency" has the meaning ascribed to it in 15 U.S.C. § 1681a(f).

"Security freeze" means a notice placed in a consumer's credit report, at the request of the consumer and subject to certain exceptions, that prohibits the consumer reporting agency from releasing the consumer's credit report or score relating to an extension of credit, without the express authorization of the consumer.

"Extension of credit" does not include an increase in an existing open-end credit plan, as defined in Regulation Z of the Federal Reserve System (12 C.F.R. 226.2), or any change to or review of an existing credit account.

"Proper identification" means information generally deemed sufficient to identify a person. Only if the consumer is unable to reasonably identify himself or herself with the information described above, may a consumer reporting agency require additional information concerning the consumer's employment and personal or family history in order to verify his or her identity.

(r) Any person who violates this Section commits an unlawful practice within the meaning of this Act.

CREDIT(S)

25-LS0311\M
Bannister
5/3/07

CS FOR HOUSE BILL NO. 65(JUD)

IN THE LEGISLATURE OF THE STATE OF ALASKA

TWENTY-FIFTH LEGISLATURE - FIRST SESSION

BY THE HOUSE JUDICIARY COMMITTEE

Offered:
Referred:

Sponsor(s): REPRESENTATIVES COGHILL AND GARA, Hawker, Lynn, Samuels, Fairclough, Ramras, Kawasaki, Kerttula, Gatto, Neuman, Olson

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:

(35) 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 person owns or uses personal information that includes personal information on a state resident, and a breach of the security of the information system containing the personal information occurs, the 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.

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 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 sufficien. 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.

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

(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, 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.

(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).

(d) In this section, "governmental agency" means a state or local governmental agency, except for an agency of the judicial branch.

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

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

(4) "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;

(5) "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, address, or telephone number; 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) the individual's account number, credit card account number, or debit card account number;

(iv) account passwords or personal identification numbers or other access codes.

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 all or a part of 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 certified 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(c), 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) A consumer credit reporting agency that receives a request from a consumer under (b) or (c) of this section shall comply with the request immediately after receiving the request by telephone or by an electronic medium or within three business days after receiving the request by mail.

(e) 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.

(f) 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, except as provided for insurers under (g) of this section, the third party may treat the third party's application as incomplete unless the consumer authorizes the access under (a) of this section.

(g) If an insurer requests access to a consumer's credit report and credit score on which a security freeze is in place, unless the consumer authorizes access under (a) of this section, the insurer may, notwithstanding AS 21.36.460,

(1) treat the consumer's application as incomplete;

(2) decline the consumer's application if the consumer does not lift the security freeze for the insurer after a request by the insurer or the insurer's agent;

(3) treat the consumer as if the consumer has a neutral credit rating;

(4) exclude the use of credit information as a factor and use only underwriting criteria; or

(5) treat the consumer in a manner that is otherwise approved by the division of insurance.

(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 co umer 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 immediately 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 $10 for placing a security freeze.

(c) If a consumer makes more than two access requests during a calendar year, a consumer credit reporting agency may charge the consumer $2 for each additional access request made by the consumer during that calendar year. 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.

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 (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 $10 to protect your privacy and ensure that credit is not granted in your name without your knowledge. 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, rental housing, employment, an investment, a license, a cellular telephone, a utility, a digital signature, an Internet credit card transaction, 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 immediately 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. Under some circumstances, 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 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 damages, including loss of wages, and, when applicable, damages for pain and suffering;

(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) (Fair Credit Reporting Act);

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

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

(10) a consumer credit reporting agency 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.

(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 who acts 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 from releasing all or a part of 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 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.

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 an 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 expressly 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 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 financial institution that is regulated by 15 U.S.C. 6801 - 6827 (Gramm-Leach-Bliley Financial Modernization Act) if the financial institution requests or collects the individual's social security number to facilitate a transaction of the individual;

(4) to a communication to or from a consumer reporting agency; in this paragraph, "consumer reporting agency" has the meaning given in 15 U.S.C. 1681a (Fair Credit Reporting Act);

(5) if the request or collection is for a background check on the individual, law enforcement purposes, or the individual's employment, including employment benefits; or

(6) if the disclosure does not have independent economic value, is incidental to a larger transaction, and is necessary to verify the identity of the individual.

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

(2) 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) 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 expressly 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 third party is a financial institution that is regulated by 15 U.S.C. 6801 - 6827 (Gramm-Leach-Bliley Financial Modernization Act), and the disclosure is to facilitate a transaction of the individual;

(4) 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

(5) the disclosure is for a background check on the individual, law enforcement 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.

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 damages or $5,000, whichever amount is greater, 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 15 U.S.C. 6801 - 6827 (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 (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 damages for the violation and court costs and attorney fees allowed by the rules of court.

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, address, or telephone number; 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 by the victim; 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 a 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) "identity theft" means the theft of the identity of an individual;

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

(5) "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) An individual may bring a civil action in court against a person who knowingly violates this section and may recover actual damages or $5,000, whichever is greater, and court costs and attorney fees allowed by the rules of court.

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

(e) 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 written, oral, or other communication of information by a consumer credit reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living if the communication is used or expected to be used or collected in whole or in part to serve as a factor in establishing the consumer's eligibility for

(A) credit or insurance to be used primarily for personal, family, or household purposes;

(B) employment purposes; or

(C) any other permissible purpose authorized under section 15 U.S.C. 1681b;

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

(5) "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;

(6) "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 45.48.750 is amended by adding a new subsection to read:

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

*** Sec. 5.** AS 45.50.471(b) is amended by adding a new paragraph to read:

(52) 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 45.48.080;

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

*** Sec. 6.** 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 45.48.480(b), enacted by sec. 3 of this Act, has 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 45.48.480(b).

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

*** Sec. 8.** AS 45.48.750(f), enacted by sec. 4 of this Act, takes effect January 1, 2009.

Summary of proposed PCI amendments to HB 65 (credit freeze provisions)

PCI has proposed a series of amendments to HB 65 that are designed to do two things:

1. Allow access to "frozen" consumer files for non-lending purposes (including insurance rating).
   a. Identity thieves do not steal consumer information to buy home or auto insurance.
   b. Insurers can more quickly, accurately and conveniently provide rate quotes to consumers with access to their consumer files.

2. Remove language added that was intended to help insurers, but in fact limits our ability to fairly provide accurate rate quotes to individuals with frozen credit files.
   a. This language was suggested in 2006 as an alternative an insurer exemption, but regardless of whether an exemption is allowed or not; PCI supports removal of the language as noted below in **Sec. 45.48.110**.

Proposed amendments and their effect:

Article 2. Credit Report and Credit Score Security Freeze.

Sec. 45.48.100. Security freeze authorized. A consumer may place a "security freeze" notice on a their consumer file that prohibits a consumer reporting agency from releasing a consumer report relating to the extension of credit involving that consumer file without the express authorization of the consumer." ~~prohibit a consumer credit reporting agency from releasing all or a part of 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.~~

EFFECT: specifies that a consumer may place a security freeze on their consumer file (we use the term "consumer file" and "consumer report" to include non-credit consumer files, including driver records) which prevents the unauthorized release of consumer reports relating to the extension of credit. By omission, non-lending related access to "frozen" consumer reports is allowed.

Sec. 45.48.110. Placement of security freeze.

(e) 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 that intends to use the information to determine a consumer's eligibility for credit or for the opening of a new account without the prior express authorization of the consumer.

(f) 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, except as provided for insurers under (g) of this section,~~ the third party may treat the third party's application as incomplete unless the consumer authorizes the access under (a) of this section.

~~(g) If an insurer requests access to a consumer report on which a security freeze is in place, unless the consumer authorizes access under (a) of this section, the insurer may, notwithstanding AS 21.36.460,~~

~~(1) treat the consumer's application as incomplete;~~

~~(2) decline the consumer's application if the consumer does not lift the security freeze for the insurer after a request by the insurer or the insurer's agent;~~

~~(3) treat the consumer as if the consumer has a neutral credit rating;~~

~~(4) exclude the use of credit information as a factor and use only underwriting criteria; or~~

~~(5) treat the consumer in a manner that is otherwise approved by the division of insurance.~~

~~(h)~~ (g)If a security freeze is in place, a consumer credit reporting agency may not…

EFFECT: Deletes language added to the bill at the request of insurers in 2006 that specifies how an insurer may deal with a consumer seeking rate information on an insurance policy if they have placed a "freeze" on their consumer file and cannot or will not lift the freeze in order to obtain the rate quote. With this change, all entities (absent a specific exemption or the "narrow consumer file definition" proposed above) will be required to treat a consumer with a "frozen" file in the same way. Even if the other amendments proposed here are not accepted, we support removing the language in the above section.

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

(5) "security freeze" means a notice placed on a consumer file that prohibits a consumer reporting agency from releasing a consumer report relating to the extension of credit involving that consumer file ~~prohibition against a consumer credit reporting agency from releasing all or a part of a consumer's credit report or credit score~~ without the express authorization of the consumer. ;

EFFECT: Specifies in the definition section that a "security freeze" means a notice on a consumer file prohibiting access to the file for purposes related to the extension of credit. By omission, non-lending purposes are thus not subject to the definition of a "security freeze."

Alaska Bankers Association
P.O. Box 100720 • Anchorage, Alaska 99510-0720 • 907-777-3011 • Fax 907-777-3029

April 11, 2007

Honorable John Coghill
Alaska House of Representatives
State Capitol, Room 214
Juneau, AK 99801-1182

Dear Representative Coghill:

The members of the Alaska Bankers Association are dedicated to protecting the privacy and security of sensitive customer information. Toward that end, the Alaska Bankers Association appreciates your desire to help protect our customers' financial information through your introduction of House Bill 65.

The Alaska Bankers Association supports many of the provisions proposed in HB 65, however, we would like to offer amendments that 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 amendments we are offering are the following:

Amendment #1 – Need for consistent and meaningful security breach requirements

As you are aware, there are a number of federal laws and numerous federal agencies that oversee the protection of customer information. Attached to this letter is a copy of the Interagency Guidelines for Information Security Standards. These guidelines primarily implement two statutes, Section 501(b) of the Gramm-Leach-Bliley Act, and Section 216 of the Fair and Accurate Credit Transactions Act.

These guidelines are drafted to ensure that customers are immediately notified of any material breach of information that has the potential to cause harm while, at the same time, guarding against causing undue customer concern by providing an exemption for incidents where the potential for misuse of information is negligible and unlikely.

The Alaska Bankers Association would like to see the language amended into the bill that would recognize any institution deemed in compliance with the extensive federal regulatory requirement is also deemed compliant under the provisions of this proposed legislation. Suggested draft amendments to this effect are attached and identified as "**Draft Amendment #1**."

Amendment #2 – SSN protection provision so restrictive they could inadvertently inhibit ability to protect customers

While HB 65 currently contains an exception on the prohibition on disclosing SSN numbers for consumer reports under Fair Credit Reporting Act, there is no exception for other types of information where SSN might be a necessary identifier such as fraud alerts.

Consequently, if the fraudulent use of a person's financial information is suspected, under the current provisions of this measure, access to SSN would not be available to help differentiate a fraudster from an innocent individual with a similar name.

The Alaska Bankers Association would like to offer language that would provide for a disclosure exemption when the disclosure is necessary to process an individual's requested transaction. Suggested draft amendments to this effect are attached and identified as "**Draft Amendment #2**."

Amendment #3 – Credit report challenge provisions could result in abuse

As currently drafted, HB 65 requires credit bureaus to stop reporting credit report information that has been challenged by the consumer until the disputed information has been re-verified. This would enable a devious consumer to challenge accurate information and immediately apply for credit, knowing that the bureau will not be able to report the challenged information for some time. Federal law and other state laws require the bureau to tag challenged information as "disputed," and are permitted to be reported until the 30-day reinvestigation period has run.

The Alaska Bankers Association would appreciate your consideration of an amendment that would conform HB 65 to federal and other existing state law requiring bureaus to tag challenged information as "disputed." Suggested draft amendments to this effect are attached and identified as "**Draft Amendment #3**."

On behalf of the Alaska Bankers Association, we appreciate the opportunity to work with you to make meaningful changes to state law that protect the privacy of our customers while also allowing us to provide the services and benefits resulting from the responsible transfer of information. We believe the amendments we are offering will help achieve this worthwhile goal.

If you have any questions or require additional information, please contact the Alaska Bankers Association lobbyist in Juneau, Thyes Shaub, at 907.463.5118.

Sincerely,

David A. Lawer, President

Enclosures

Cc: Representative Anna Fairclough
Representative Les Gara
Representative Mike Hawker
Representative Scott Kawasaki
Representative Beth Kerttula
Representative Bob Lynn
Representative Jay Ramras
Representative Ralph Samuels

Suggested Amendment to
Alaska House Bill No. 65

Amendment #1 – conforming language to existing federal regulatory requirements.

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

  "made a reasonable determination at to whether unintentional use 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)."

Amendment #2 - providing a SSN disclosure exemption when the disclosure is necessary to process an individual's requested transaction.

- 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.

Amendment #3 - preventing fraudulent use of credit report disputes

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 reverififed within thirty days, correct or delete such information in any subsequent consumer reports."