SB

222

SENATE COMMITTEE REPORT

DATE: 2/16/06

FURTHER:

DATE TURNED
IN TO OFFICE:_____

Judiciary Committee considered SENATE BILL NO. 222

SB 222 PROTECTION OF PERSONAL INFORMATION

"An Act relating to breaches of security involving personal information, consumer report security freezes, consumer credit monitoring, credit accuracy, protection of social security numbers, disposal of records, factual declarations of innocence after identity theft, filing police reports regarding identity theft, and furnishing consumer credit header information; and amending Rule 60, Alaska Rules of Civil Procedure."

and recommends:

[ ] be **replaced** with _____ **CS** _____ (_____)

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

[ ] attached amendment(s)

[ ] adopt Letter of Intent by _____ Committee

[ ] further referral to _____ _____ Committee

CS Senate Bill:
[ ] Same Title
[ ] New Title

SCS House Bill:
[ ] Same Title
[ ] Technical Title Change
[ ] New Title w/ SCR #_____

NEW FISCAL NOTE(S):

Department	Date	Fiscal	Indet.	Zero	FN#

PREVIOUS FISCAL NOTE(S):

Department	Date	Fiscal	Indet.	Zero	FN#

[ ] **APPROPRIATION - no fiscal note**

SIGNATURES AND RECOMMENDATIONS:	DO PASS	DO NOT PASS	NO REC	AMEND
[illegible]	X			
[illegible]	X			
[illegible]	X			
CHAIR: [illegible]	✓			

CHANGES IN CS SB 222, VERSION "S"

Friday, March 10, 2006

1. Page 2, line 2.
   Notification of breach only to impacted persons not entire databases.

2. Page 2, lines 12-13.
   Requires written notification by law enforcement when they lift a delay on notification.

3. Page 3, line 24.
   Deletes section 45.48.070 on Minimum Contacts.

4. Page 3, line 27.
   Breach of security includes acquisition or reasonable belief of acquisition.

5. Page 4, lines 7-21.
   Ensures clarity in the definition of "personal information" and include encrypted data when the encryption key has been accessed or acquired.

6. Page 6, lines 10 and 13-23.
   Clarifies that insurance companies can hold an application as incomplete (or other listed actions) when a security freeze is in place.

7. Page 8, line 19 and page 9, line 23.
   Clarifies language in the "Notice of Rights" outlined in section 45.48.170 to ensure consistency with the bill's effects.

8. Page 10, line 19.
   Deletes the section previously numbered 45.48.200 on Minimum Contacts.

9. Page 12, Line 8.
   Clarifies freeze exemptions to include credit score if to a consumer at their request.

10. Page 12, lines 14-18.
    Improves clarity and conforms to California law in the "re-seller" exemption.

11. Page 16, line 28 – page 17, line 3.
    Clarifies that local law may authorize collection of Social Security Numbers.

12. Page 17, lines 1-3.
    Clarifies that state agencies may adopt regulations to authorize collection of Social Security Numbers.

13. Page 17, lines 4-8.
    Ensures state or local agencies can disclose SSN to another state, local, or federal governmental agency when required to carry out the agency's duties.

14. Article five, pages 17-20.
    Adds government agencies to the disposal of records section.

SENATORS GRETCHEN GUESS and GENE THERRIAULT

24-LS1419\S
Bannister
3/10/06

CS FOR SENATE BILL NO. 222( )

IN THE LEGISLATURE OF THE STATE OF ALASKA

TWENTY-FOURTH LEGISLATURE - SECOND SESSION

BY

Offered:
Referred:

Sponsor(s): SENATORS THERRIAULT AND GUESS, Ellis

A BILL

FOR AN ACT ENTITLED

"An Act relating to breaches of security involving personal information, credit report security freezes, consumer credit monitoring, credit accuracy, protection of social security numbers, disposal of records, factual declarations of innocence after identity theft, filing police reports regarding identity theft, furnishing consumer credit header information, and truncation of credit and debit card information; and amending Rule 60, Alaska Rules of Civil Procedure."

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

*** Section 1.** 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 expedient 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 and provides the information collector with a written request for the delay. However, the information collector shall disclose the breach to the state resident as soon as 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;

(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 $250,000, that the affected class of state residents to be notified exceeds 500,000, or that the information collector does not have sufficient contact information to provide notice, by

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

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

(C) providing a notice to major statewide media.

Sec. 45.48.040. 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. 45.48.050. Waivers. A waiver of AS 45.48.010 - 45.48.090 is void and unenforceable.

Sec. 45.48.060. Violations. (a) If an information collector violates AS 45.48.010 - 45.48.090 with regard to the personal information of an individual, the individual or a state agency may bring a civil action in court to

(1) recover the damages suffered by the state resident;

(2) enjoin from further violations of AS 45.48.010 - 45.48.090 an information collector who engages in business and the security breach occurred to the personal information used or owned by the information collector in the business.

(b) The rights and remedies available under this section are in addition to any other rights and remedies available under another law.

(c) In this section, "state agency" means

(1) a department, division, or office in the executive branch of state government that has authority under the statutes of this state to regulate the operation of the information collector; or

(2) the Department of Law if another state agency does not have authority under the statutes of this state to regulate the operation of the information collector.

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) "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 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 information derived from the credit report 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;

(2) by telephone if the consumer provides the consumer credit reporting agency with certain personal identification; or

(3) through a secure electronic mail connection if the consumer credit reporting agency makes a secure electronic mail connection available to the consumer.

(b) A consumer credit reporting agency shall place a security freeze within five business days after receiving a request under (a)(1) of this section and immediately after receiving a request under (a)(2) or (3) of this section.

Sec. 45.48.120. Confirmation of security freeze. (a) Within five 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.

(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 or password to be used by the consumer when the consumer authorizes the release of the consumer's credit report or information derived from the report 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 information derived from the credit report 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 telephone, certified mail, or secure electronic mail connection, 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 or password 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) A consumer credit reporting agency that receives a request from a consumer under (b) of this section shall comply with the request immediately after

receiving the request by telephone or electronic mail or within three business days after receiving the request by certified mail.

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

(e) If a security freeze is in place on a consumer's credit report and information derived from the credit report 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 information derived from the credit report, the consumer credit reporting agency and, except as provided for insurers under (f) 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.

(f) 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

(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.

(g) A consumer credit reporting agency shall notify a consumer that a third party has attempted to access the consumer's credit report or information derived from the report if a third party requests a consumer credit reporting agency to provide the third party with access to the credit report or information, a security freeze has been placed, and the purpose of the access is not for the sole purpose of account review.

(h) 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 information derived from the credit report that a security freeze is in effect.

(i) 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), Internet, electronic mail, or another electronic method.

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

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

(2) the consumer made a material misrepresentation of fact to the consumer credit reporting agency when the consumer requested the security freeze under AS 45.48.110; if a consumer credit reporting agency intends to remove a security freeze on a consumer's credit report under this paragraph, the consumer credit reporting agency shall notify the consumer in writing five business days 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 if the consumer provides proper identification to identify the consumer and the unique personal identification number or password provided by the consumer credit reporting agency under AS 45.48.120.

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) 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 or password under AS 45.48.120, that is related to the placement of, removal of, or allowing access to a

credit report or information derived from a credit report on which a security freeze has been placed.

(b) If a consumer fails to retain a personal identification number or password 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 or password because the consumer failed to retain the personal identification number or password.

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 at no charge 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 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. When you place a security freeze on your credit report, within five business days you will be provided a personal identification number or password to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report 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 or password 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 or the specific period of time for which the report is to be available to third parties.

A consumer credit reporting agency that receives your request to temporarily lift a freeze on a credit report is required to comply with the request immediately after receiving your request if you make the request by telephone or electronic mail, or within three business days after receiving your request if you make the request by certified mail.

A security freeze does not apply to circumstances where you have an existing account relationship and a copy of your report is 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, a few days before actually 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 information derived from the credit report, 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. 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. 45.48.200. Limited application. A consumer credit information agency may not release all or a part of the information on a consumer that the consumer credit information agency has received from a consumer credit reporting agency if the consumer has placed a security freeze on the consumer credit reporting agency under AS 45.48.100.

Sec. 45.48.210. Reports not covered. The provisions of AS 45.48.100 - 45.48.290 do not apply to a credit report if the credit report is

(1) a report that only contains information relating to transactions or experiences between the consumer and the person making the report;

(2) a communication of the information that is described in (1) of this section or that is taken from a consumer's credit application if

(A) the communication is limited to internal communication

within the organization of the person making the report; and

(B) the consumer is informed by a clear and conspicuous written disclosure that the information contained in the credit application may be communicated as allowed under (A) of this paragraph, except that, if a credit application is taken by telephone, the consumer shall initially be informed orally when the application is taken, and a clear and conspicuous written disclosure shall be made to the consumer in the first written communication to the consumer after the application is taken;

(3) a report containing information solely about a consumer's character, general reputation, personal characteristics, or mode of living and the information is obtained through personal interviews with neighbors, friends, or associates of the consumer reported on, or others with whom the consumer is acquainted or who may have knowledge concerning those items of information; or

(4) a credit report furnished for use in connection with a transaction that consists of an extension of credit to be used solely for a commercial purpose.

Sec. 45.48.220. Exemptions. 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. 1681 - 1681w (Fair Credit Reporting Act);

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

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

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;

(3) "consumer credit information agency" means a person who acts only as a reseller of consumer information by assembling and merging 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;

(4) "consumer credit reporting agency" has the meaning given in AS 45.48.990, but does not include a consumer credit information agency;

(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 information derived from the credit report 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

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

Article 3. Consumer Credit Monitoring; Credit Accuracy.

Sec. 45.48.300. Required disclosure. A consumer credit reporting agency

shall, if a consumer makes the request and the request is not covered by the free disclosure provision of 15 U.S.C. 1681j(a) - (d) (Fair Credit Reporting Act), clearly and accurately disclose to the consumer the information described under AS 45.45.310.

Sec. 45.48.310. Information to be disclosed. (a) The following information shall be disclosed under AS 45.45.300:

(1) all information in the consumer's file when the consumer makes the request, except that this paragraph may not be construed to require a consumer credit reporting agency to disclose information concerning credit scores, risk scores, or other predictors that are governed by 15 U.S.C. 1681g;

(2) the sources of the information described in (1) of this subsection;

(3) an identification of each person, including each end user identified under 15 U.S.C. 1681e, who procured a report on the consumer

(A) for employment purposes during the two-year period that precedes the date when the consumer's request is made; or

(B) for a purpose other than employment purposes during the one-year period that precedes the date when the consumer's request is made;

(4) the dates, original payees, and amounts of any checks that

(A) provide the basis for an adverse characterization of the consumer; and

(B) are included in the file when the disclosure is made or can be inferred from the file;

(5) a record of all inquiries that were received by the consumer credit reporting agency during the one-year period that precedes the request and that identify the consumer in connection with a credit or insurance transaction that was not initiated by the consumer; and

(6) a statement that the consumer may request and obtain a credit score if the consumer requests the credit file and not the credit score.

(b) The information to be disclosed under (a)(3) of this section must include

(1) the name of the person or, if applicable, the full trade name under which the person conducts business; and

(2) the address and telephone number of the person if requested by the consumer.

(c) A consumer credit reporting agency is not required to disclose the information described in (a)(3) of this section if

(1) the end user is an agency of the United States government and procures the consumer's credit report from the consumer credit reporting agency to determine the eligibility of the consumer to receive access or continued access to classified information; in this paragraph, "classified information" has the meaning given in 15 U.S.C. 1681b; and

(2) the individual who is in charge of the end user makes a written finding as prescribed under 15 U.S.C. 1681b(b)(4)(A).

Sec. 45.48.320. Cost of disclosure. (a) A consumer credit reporting agency may impose a reasonable charge on a consumer for making a disclosure under AS 45.48.300. The charge may not exceed

(1) $2 for each of the first 12 requests from the consumer in a calendar year;

(2) $8 for each request beyond the 12 requests covered by (1) of this subsection in a calendar year.

(b) The consumer credit reporting agency shall disclose the charge to the consumer before making the disclosure under AS 45.48.300.

Sec. 45.48.330. Form of disclosure. (a) A consumer may make the request under AS 45.48.300 in writing, in person, by telephone if the consumer has made a written request for the disclosure, by electronic means if the consumer credit reporting agency offers electronic access for any other purpose, or by any other reasonable means that is available from the consumer credit reporting agency.

(b) To make a request in person under (a) of this section, the consumer shall, after reasonable notice to the consumer credit reporting agency, appear during normal business hours at the consumer credit reporting agency's place of business where the consumer credit reporting agency normally provides disclosures under AS 45.48.300.

Sec. 45.48.340. Timing of disclosure. A consumer credit reporting agency shall provide a consumer with the disclosure under AS 45.48.300 within

(1) 24 hours after the date on which the request is made if the disclosure is made by electronic means under AS 45.48.330(a); or

(2) five days after the date on which the request is made if the disclosure is made in writing, in person, by telephone, or by any other reasonable means that is available from the consumer credit reporting agency, except by electronic means.

Sec. 45.48.350. Credit accuracy. (a) A person who does business in the state by distributing information about an individual's credit history, score, or ranking shall, when notified that the information that the person is distributing is inaccurate, immediately stop distributing the information until the accuracy of the information can be verified or the inaccuracies in the information corrected.

(b) If a person who does business in the state by distributing information about an individual's credit history, score, or ranking releases information about an individual that is inaccurate, the person shall, as quickly as possible after discovering that inaccurate information is being distributed,

(1) repair, to the extent possible, the damage to the individual caused by the release of the inaccurate information; and

(2) pay fair and reasonable compensation to the individual for the damage caused to the individual by the release of the inaccurate information.

(c) If a person fails to comply with (b) of this section, an individual may bring an action in court to compel the person to comply with (b) of this section.

(d) In this section, "does business in the state" means engages in activities that provide at least the minimum contacts required by substantive due process for the state to exercise jurisdiction over the person who is engaging in the activities.

Article 4. Protection of Social Security Number.

Sec. 45.48.400. Use of social security number. (a) A person may not, without the consent of the individual.

(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 in order to access the site;

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

(A) state or federal law requires the social security number to be 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 being opened;

(6) refuse to do business with an individual because the individual does not consent to the receipt by the person of the social security number of the individual, unless the person is expressly required by state or federal law, in connection with doing business with an individual, to collect or submit the individual's social security number to the state or federal government; this paragraph does not prohibit a person from asking for another form of identification from the individual.

(b) Unless expressly required by federal or state law, a person may not sell, lease, loan, trade, rent, or otherwise disclose an individual's social security number to a third party for any purpose without the individual's written consent.

Sec. 45.48.410. Additional governmental prohibition; social security numbers. A person who is a state or local governmental agency, except for an agency of the judicial branch, may not ask an individual to provide the agency with a social security number unless state, federal, or local law expressly authorizes the agency to

ask the individual to provide the social security number to the agency. A state agency may adopt regulations under AS 44.62 (Administrative Procedure Act) to implement this section.

Sec. 45.48.415. Interagency disclosure. Notwithstanding the other provisions of AS 45.48.400 - 45.48.420, 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. 45.48.420. Penalties. (a) A person who knowingly violates AS 45.48.400 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 or 45.48.410 and may recover actual damages or $5,000, whichever amount is greater, and court costs and attorney fees allowed by the rules of court.

(c) A person who knowingly violates AS 45.48.400 is guilty of a class A misdemeanor.

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

Article 5. Disposal of Records.

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

(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.

Sec. 45.48.510. Measures to protect access. The measures required to be taken under 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; and

(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;

(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 comprehensively describe and classify as the official policy of the business or governmental agency in the writings of the business or governmental agency the policies and procedures that relate to the adequate destruction and proper disposal of personal records. In this section, "writings" includes corporate handbooks, employee handbooks, and similar corporate documents.

Sec. 45.48.540. Exemption. 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.

Sec. 45.48.550. Civil penalty. 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. 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 information that identifies, relates to,

describes, or is capable of being associated with a particular individual, and includes a name, signature, social security number, fingerprint, photograph, computerized image, physical characteristic, physical description, address, telephone number, passport number, driver's license, state identification number, date of birth, medical information, bank account number, credit card number, debit card number, and financial information;

(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 directories containing names, addresses, telephone numbers, or other information an individual has voluntarily consented to have publicly disseminated or listed.

Article 6. 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 has been filed against the perpetrator in the victim's name; or

(3) the victim's identity has been 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 shall

determine that a victim is factually innocent of a crime if the court finds that the petition or motion brought under AS 45.48.600 is meritorious and that

(1) there is not a reasonable cause to believe that the victim committed the crime for which the perpetrator of the identity theft was arrested, cited, convicted, or subject to a criminal complaint in the victim's name; or

(2) the victim's identity has been mistakenly associated with a record of a conviction of a 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 that is contained in the files, indexes, and other records of the court that are accessible by the public deleted, sealed, or labeled to show that the name and personal information is impersonated and does not reflect the defendant's identity.

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 motion, or any information submitted in support of the petition or motion, is found to contain a material misrepresentation or fraudulent material.

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 in order 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 7. Consumer Credit Header Information.

Sec. 45.48.800. Consumer credit header information. (a) A consumer credit reporting agency may not furnish by a written, an oral, or another method of communication a consumer's credit header information to a person unless the person has a permissible purpose under 15 U.S.C. 1681b (Fair Credit Protection Act) to obtain the consumer's credit report.

(b) In this section, "credit header information" means the social security number of a consumer, or a derivative of the social security number, the maiden name of the mother of the consumer, the birth date of the consumer, and other personally identifiable information of a consumer that is derived from nonpublic personal information, except the name, address, and telephone number of the consumer listed in a residential telephone directory available in the locality of the consumer.

Article 8. Truncation of Card Information.

Sec. 45.48.850. 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 five digits of the card number or the expiration date on any receipt provided to the cardholder 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) A person who knowingly violates this section is guilty of a class A misdemeanor.

(f) In this section,

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

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

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

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

Article 9. General Provisions.

Sec. 45.48.900. Relationship to federal law. If a provision of this chapter is preempted by federal law in a particular situation, the provision does not apply to the extent of the preemption.

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. 2.** The uncodified law of the State of Alaska is amended by adding a new section to

read:

INDIRECT COURT RULE AMENDMENT. AS 45.48.640, enacted by sec. 1 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.

* **Sec. 3.** The uncodified law of the State of Alaska is amended by adding a new section to read:

TRANSITION: IMPLEMENTATION. A person to whom AS 45.48.400, 45.48.410, 45.48.415, or 45.48.420, enacted by sec. 1 of this Act, applies shall make reasonable efforts to cooperate, through systems testing and other means, to ensure that the requirements of AS 45.48.400, 45.48.410, 45.48.415, and 45.48.420 that apply to the person are implemented on or before the effective date of AS 45.48.400, 45.48.410, 45.48.415, and 45.48.420. In this section, "person" has the meaning given in AS 45.48.990, but also includes an agency of the judicial branch.

24-LS1419\I
Bannister
2/21/06

CS FOR SENATE BILL NO. 222( )

IN THE LEGISLATURE OF THE STATE OF ALASKA

TWENTY-FOURTH LEGISLATURE - SECOND SESSION

BY

Offered:
Referred:

Sponsor(s): SENATORS THERRIAULT AND GUESS, Ellis

A BILL

FOR AN ACT ENTITLED

"An Act relating to breaches of security involving personal information, credit report security freezes, consumer credit monitoring, credit accuracy, protection of social security numbers, disposal of records, factual declarations of innocence after identity theft, filing police reports regarding identity theft, furnishing consumer credit header information, and truncation of credit and debit card information; and amending Rule 60, Alaska Rules of Civil Procedure."

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

*** Section 1.** 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 the state resident.

(b) An information collector shall make the disclosure required by (a) of this section in the most expedient 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 and provides the information collector with a written request for the delay. However, the information collector shall disclose the breach to the state resident as soon as notification would not any 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;

(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 $250,000, that the affected class of state residents to be notified exceeds 500,000, or that the information collector does not have sufficient contact information to provide notice, by

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

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

(C) providing a notice to major statewide media.

Sec. 45.48.040. 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. 45.48.050. Waivers. A waiver of AS 45.48.010 - 45.48.090 is void and unenforceable.

Sec. 45.48.060. Violations. (a) If an information collector violates AS 45.48.010 - 45.48.090 with regard to the personal information of an individual, the individual or a state agency may bring a civil action in court to

(1) recover the damages suffered by the state resident;

(2) enjoin from further violations of AS 45.48.010 - 45.48.090 an information collector who engages in business and the security breach occurred to the personal information used or owned by the information collector in the business.

(b) The rights and remedies available under this section are in addition to any other rights and remedies available under another law.

(c) In this section, "state agency" means

(1) a department, division, or office in the executive branch of state government that has authority under the statutes of this state to regulate the operation of the information collector; or

(2) the Department of Law if another state agency does not have authority under the statutes of this state to regulate the operation of the information collector.

Sec. 45.48.070. Minimum contacts. An information collector is subject to AS 45.48.010 - 45.48.090 if the information collector engages in activities that provide at least the minimum contacts required by substantive due process for the state to exercise jurisdiction over the information collector.

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

(1) "breach of the security" means 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) "personal information" means information in any form on an individual, other than, if applicable, the information collector, that is not currently lawfully available to the general public from federal, state, or local government records and that consists of

(A) a combination of an individual's first name or first initial, the individual's last name, and one or more of the following information elements, when the name or the information elements are not encrypted or redacted:

(i) the individual's social security number;

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

(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;

(B) an item listed in (A)(i) - (iv) of this paragraph if the item would be sufficient to engage in or attempt to engage in the theft of an individual's identity.

Article 2. Credit Report 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 information derived from the credit report 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;

(2) by telephone if the consumer provides the consumer credit reporting agency with certain personal identification; or

(3) through a secure electronic mail connection if the consumer credit reporting agency makes a secure electronic mail connection available to the consumer.

(b) A consumer credit reporting agency shall place a security freeze within five business days after receiving a request under (a)(1) of this section and immediately after receiving a request under (a)(2) or (3) of this section.

Sec. 45.48.120. Confirmation of security freeze. (a) Within five 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.

(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 or password to be used by the consumer when the consumer authorizes the release of the consumer's credit report or information derived from the report 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 information derived from the credit report 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 telephone, certified mail, or secure electronic mail connection, 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 or password 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) A consumer credit reporting agency that receives a request from a consumer under (b) of this section shall comply with the request immediately after receiving the request by telephone or electronic mail or within three business days after receiving the request by certified mail.

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

(e) If a security freeze is in place on a consumer's credit report and information derived from the credit report 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 information derived from the credit report, the consumer credit reporting agency and the third party may treat the third party's application as incomplete unless the consumer authorizes the access under (a) of this section.

(f) A consumer credit reporting agency shall notify a consumer that a third party has attempted to access the consumer's credit report or information derived from the report if a third party requests a consumer credit reporting agency to provide the third party with access to the credit report or information, a security freeze has been placed, and the purpose of the access is not for the sole purpose of account review.

(g) 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 information derived from the credit report that a security freeze is in effect.

(h) 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), Internet, electronic mail, or another electronic method.

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

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

(2) the consumer made a material misrepresentation of fact to the consumer credit reporting agency when the consumer requested the security freeze under AS 45.48.110; if a consumer credit reporting agency intends to remove a security freeze on a consumer's credit report under this paragraph, the consumer credit reporting agency shall notify the consumer in writing five business days 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 if the consumer provides proper identification to identify the consumer and the unique personal identification number or password provided by the consumer credit reporting agency under AS 45.48.120.

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) 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 or password under AS 45.48.120, that is related to the placement of, removal of, or allowing access to a credit report or information derived from a credit report on which a security freeze has been placed.

(b) If a consumer fails to retain a personal identification number or password 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 or password because the consumer failed to retain the personal identification number or password.

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 at no charge 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 under state law (AS 45.48.100 - 45.48.290).

The security freeze will prohibit a consumer credit reporting agency from releasing 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. When you place a security freeze on your credit report, within five business days you will be provided a personal identification number or password to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report 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 or password 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 or the specific period of time for which the report is to be available to third parties.

A consumer credit reporting agency that receives your request

to temporarily lift a freeze on a credit report is required to comply with the request immediately after receiving your request if you make the request by telephone or electronic mail, or within three business days after receiving your request if you make the request by certified mail.

A security freeze does not apply to circumstances where you have an existing account relationship and a copy of your report is 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, a few days before actually 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 or a user of your credit report.

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 information derived from the credit report, 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. 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. 45.48.200. Minimum contacts. A consumer credit reporting agency is subject to AS 45.48.100 - 45.48.290 if the consumer credit reporting agency engages in activities that provide at least the minimum contacts required by substantive due process for the state to exercise jurisdiction over the consumer credit reporting agency.

Sec. 45.48.210. Limited application. A consumer credit information agency may not release all or a part of the information on a consumer that the consumer credit information agency has received from a consumer credit reporting agency if the consumer has placed a security freeze on the consumer credit reporting agency under AS 45.48.100.

Sec. 45.48.220. Reports not covered. The provisions of AS 45.48.100 - 45.48.290 do not apply to a credit report if the credit report is

(1) a report that only contains information relating to transactions or experiences between the consumer and the person making the report;

(2) a communication of the information that is described in (1) of this section or that is taken from a consumer's credit application if

(A) the communication is limited to internal communication within the organization of the person making the report; and

(B) the consumer is informed by a clear and conspicuous

written disclosure that the information contained in the credit application may be communicated as allowed under (A) of this paragraph, except that, if a credit application is taken by telephone, the consumer shall initially be informed orally when the application is taken, and a clear and conspicuous written disclosure shall be made to the consumer in the first written communication to the consumer after the application is taken;

(3) a report containing information solely about a consumer's character, general reputation, personal characteristics, or mode of living and the information is obtained through personal interviews with neighbors, friends, or associates of the consumer reported on, or others with whom the consumer is acquainted or who may have knowledge concerning those items of information; or

(4) a credit report furnished for use in connection with a transaction that consists of an extension of credit to be used solely for a commercial purpose.

Sec. 45.48.230. Exemptions. 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. 1681 - 1681w (Fair Credit Reporting Act

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

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

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;

(3) "consumer credit information agency" means a person who

(A) assembles and sells consumer information obtained from consumer credit reporting agencies; and

(B) does not

(i) maintain a permanent information system of consumer information;

(ii) evaluate information on consumers for credit reports; or

(iii) furnish credit reports to third parties.

(4) "consumer credit reporting agency" has the meaning given in AS 45.48.990, but does not include a consumer credit information agency;

(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 information derived from the credit report 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

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

Article 3. Consumer Credit Monitoring; Credit Accuracy.

Sec. 45.48.300. Required disclosure. A consumer credit reporting agency shall, if a consumer makes the request and the request is not covered by the free disclosure provision of 15 U.S.C. 1681j(a) - (d) (Fair Credit Reporting Act), clearly and accurately disclose to the consumer the information described under AS 45.45.310.

Sec. 45.48.310. Information to be disclosed. (a) The following information shall be disclosed under AS 45.45.300:

(1) all information in the consumer's file when the consumer makes the request, except that this paragraph may not be construed to require a consumer credit reporting agency to disclose information concerning credit scores, risk scores, or other predictors that are governed by 15 U.S.C. 1681g;

(2) the sources of the information described in (1) of this subsection;

(3) an identification of each person, including each end user identified under 15 U.S.C. 1681e, who procured a report on the consumer

(A) for employment purposes during the two-year period that precedes the date when the consumer's request is made; or

(B) for a purpose other than employment purposes during the one-year period that precedes the date when the consumer's request is made;

(4) the dates, original payees, and amounts of any checks that

(A) provide the basis for an adverse characterization of the consumer; and

(B) are included in the file when the disclosure is made or can be inferred from the file;

(5) a record of all inquiries that were received by the consumer credit reporting agency during the one-year period that precedes the request and that identify the consumer in connection with a credit or insurance transaction that was not initiated by the consumer; and

(6) a statement that the consumer may request and obtain a credit score if the consumer requests the credit file and not the credit score.

(b) The information to be disclosed under (a)(3) of this section must include

(1) the name of the person or, if applicable, the full trade name under which the person conducts business; and

(2) the address and telephone number of the person if requested by the consumer.

(c) A consumer credit reporting agency is not required to disclose the information described in (a)(3) of this section if

(1) the end user is an agency of the United States government and procures the consumer's credit report from the consumer credit reporting agency to determine the eligibility of the consumer to receive access or continued access to classified information; in this paragraph, "classified information" has the meaning given in 15 U.S.C. 1681b; and

(2) the individual who is in charge of the end user makes a written finding as prescribed under 15 U S.C. 1681b(b)(4)(A).

Sec. 45.48.320. Cost of disclosure. (a) A consumer credit reporting agency may impose a reasonable charge on a consumer for making a disclosure under AS 45.48.300. The charge may not exceed

(1) $2 for each of the first 12 requests from the consumer in a calendar year;

(2) $8 for each request beyond the 12 requests covered by (1) of this subsection in a calendar year.

(b) The consumer credit reporting agency shall disclose the charge to the consumer before making the disclosure under AS 45.48.300.

Sec. 45.48.330. Form of disclosure. (a) A consumer may make the request under AS 45.48.300 in writing, in person, by telephone if the consumer has made a written request for the disclosure, by electronic means if the consumer credit reporting agency offers electronic access for any other purpose, or by any other reasonable means that is available from the consumer credit reporting agency.

(b) To make a request in person under (a) of this section, the consumer shall, after reasonable notice to the consumer credit reporting agency, appear during normal business hours at the consumer credit reporting agency's place of business where the consumer credit reporting agency normally provides disclosures under AS 45.48.300.

Sec. 45.48.340. Timing of disclosure. A consumer credit reporting agency shall provide a consumer with the disclosure under AS 45.48.300 within

(1) 24 hours after the date on which the request is made if the disclosure is made by electronic means under AS 45.48.330(a); or

(2) five days after the date on which the request is made if the disclosure is made in writing, in person, by telephone, or by any other reasonable means that is available from the consumer credit reporting agency, except by electronic means.

Sec. 45.48.350. Credit accuracy. (a) A person who does business in the state by distributing information about an individual's credit history, score, or ranking shall, when notified that the information that the person is distributing is inaccurate, immediately stop distributing the information until the accuracy of the information can be verified or the inaccuracies in the information corrected.

(b) If a person who does business in the state by distributing information about an individual's credit history, score, or ranking releases information about an individual that is inaccurate, the person shall, as quickly as possible after discovering that inaccurate information is being distributed,

(1) repair, to the extent possible, the damage to the individual caused by the release of the inaccurate information; and

(2) pay fair and reasonable compensation to the individual for the damage caused to the individual by the release of the inaccurate information.

(c) If a person fails to comply with (b) of this section, an individual may bring an action in court to compel the person to comply with (b) of this section.

(d) In this section, "does business in the state" means engages in activities that provide at least the minimum contacts required by substantive due process for the state to exercise jurisdiction over the person who is engaging in the activities.

Article 4. Protection of Social Security Number.

Sec. 45.48.400. Use of social security number. (a) A person may not, without the consent of the individual,

(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 in order to access the site;

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

(A) state or federal law requires the social security number to be 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 being opened;

(6) refuse to do business with an individual because the individual does not consent to the receipt by the person of the social security number of the individual, unless the person is expressly required by state or federal law, in connection with doing business with an individual, to collect or submit the individual's social security number to the state or federal government; this paragraph does not prohibit a person from asking for another form of identification from the individual.

(b) Unless expressly required by federal or state law, a person may not sell, lease, loan, trade, rent, or otherwise disclose an individual's social security number to a third party for any purpose without the individual's written consent.

Sec. 45.48.410. Additional governmental prohibition A person who is a state or local governmental agency, except for an agency of the judicial branch, may

not ask an individual to provide the agency with a social security number unless state or federal law expressly authorizes the agency to ask the individual to provide the social security number to the agency.

Sec. 45.48.420. Penalties. (a) A person who knowingly violates AS 45.48.400 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 or 45.48.410 and may recover actual damages or $5,000, whichever amount is greater, and court costs and attorney fees allowed by the rules of court.

(c) A person who knowingly violates AS 45.48.400 is guilty of a class A misdemeanor.

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

Article 5. Disposal of Records.

Sec. 45.48.500. Disposal of records. (a) A business shall take, in connection with and after the disposal of the records, all reasonable measures necessary to protect against unauthorized access to or use of the records of the business that contain personal information.

(b) Notwithstanding (a) of this section, if a business 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 is not liable for the disposal of records under AS 45.48.500 - 45.48.590 after the business has relinquished control of the records to the third party for the destruction of the records.

Sec. 45.48.510. Measures to protect access. The measures required to be taken under 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; and

(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;

(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. Business policy and procedures. A business shall comprehensively describe and classify as the business's official policy in the writings of the business the policies and procedures that relate to the adequate destruction and proper disposal of personal records. In this section, "writings" includes corporate handbooks, employee handbooks, and similar corporate documents.

Sec. 45.48.540. Exemption. A business is not required to comply with AS 45.48.500 - 45.48.530 if federal law requires that the business act in a way that does not comply with AS 45.48.500 - 45.48.530.

Sec. 45.48.550. Civil penalty. An individual or a business that knowingly violates AS 45.48.500 - 45.48.590 is liable to the state for a civil penalty not to exceed $3,000. 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) "personal information" means information that identifies, relates to, describes, or is capable of being associated with a particular individual, and includes a name, signature, social security number, fingerprint, photograph, computerized image, physical characteristic, physical description, address, telephone number, passport number, driver's license, state identification number, date of birth, medical information, bank account number, credit card number, debit card number, and financial information;

(4) "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 directories containing names, addresses, telephone numbers, or other information an individual has voluntarily consented to have publicly disseminated or listed.

Article 6. 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 has been filed against the perpetrator in the victim's name; or

(3) the victim's identity has been 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 shall determine that a victim is factually innocent of a crime if the court finds that the petition or motion brought under AS 45.48.600 is meritorious and that

(1) there is not a reasonable cause to believe that the victim committed the crime for which the perpetrator of the identity theft was arrested, cited, convicted, or subject to a criminal complaint in the victim's name; or

(2) the victim's identity has been mistakenly associated with a record of a conviction of a 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 that is contained in the files, indexes, and other records of the court that are accessible by the public deleted, sealed, or labeled to show that the name and personal information is impersonated and does not reflect the defendant's identity.

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 motion, or any information submitted in support of the petition or motion, is found to contain a material misrepresentation or fraudulent material.

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 in order 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 7. Consumer Credit Header Information.

Sec. 45.48.800. Consumer credit header information. (a) A consumer credit reporting agency may not furnish by a written, an oral, or another method of communication a consumer's credit header information to a person unless the person has a permissible purpose under 15 U.S.C. 1681b (Fair Credit Protection Act) to obtain the consumer's credit report.

(b) In this section, "credit header information" means the social security number of a consumer, or a derivative of the social security number, the maiden name of the mother of the consumer, the birth date of the consumer, and other personally identifiable information of a consumer that is derived from nonpublic personal information, except the name, address, and telephone number of the consumer listed in a residential telephone directory available in the locality of the consumer.

Article 8. Truncation of Card Information.

Sec. 45.48.850. 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 five digits of the card number or the expiration date on any receipt provided to the cardholder 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) A person who knowingly violates this section is guilty of a class A misdemeanor.

(f) In this section,

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

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

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

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

Article 9. General Provisions.

Sec. 45.48.900. Relationship to federal law. If a provision of this chapter is preempted by federal law in a particular situation, the provision does not apply to the extent of the preemption.

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

INDIRECT COURT RULE AMENDMENT. AS 45.48.640, enacted by sec. 1 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.

*** Sec. 3.** The uncodified law of the State of Alaska is amended by adding a new section to read:

TRANSITION: IMPLEMENTATION. A person to whom AS 45.48.400, 45.48.410, or 45.48.420, enacted by sec. 1 of this Act, applies shall make reasonable efforts to cooperate, through systems testing and other means, to ensure that the requirements of AS 45.48.400, 45.48.410, and 45.48.420 that apply to the person are implemented on or before the effective

date of AS 45.48.400, 45.48.410, and 45.48.420.

ALASKA STATE LEGISLATURE

SENATOR GENE THERRIAULT
SENATOR GRETCHEN GUESS

Sponsor Statement

Senate Bill 222:

"An Act relating to breaches of security involving personal information, consumer report security freezes, consumer credit monitoring, credit accuracy, protection of social security numbers, disposal of records, factual declarations of innocence after identity theft, filing police report regarding identity theft, and furnishing consumer credit header information; and amending Rule 60, Alaska Rules of Civil Procedure."

The intent of SB 222 is to protect consumers from the growing problem of identity theft and fraud. The measures are designed to secure consumers' private information and ensure consumers will be able to affordably access their credit reports. This problem is growing and consumers must have the tools necessary to fight and prevent identity theft and consumer fraud.

The following are the provisions of the bill.

- **Notification of Security Breaches.** This section requires persons, businesses, and government entities, which collect an individual's nonpublic personal data, to notify consumers when this information may have been compromised.
- **Freeze Access To Reports.** This provision enables consumers to freeze access to their credit report until the consumer releases the information to a specific requestor for a one time or an on-going basis.
- **Protect Credit Header Information.** This provision requires a consumer-reporting agency to restrict who receives credit header information. Credit header information includes the following: Name, Last Known Address, Employer, Mother's Maiden Name, Social Security Number, and Telephone Number.
- **Right to File a Police Report on ID Theft.** This provision would require police in the victim's home jurisdiction to take a report from the victim of identity theft regardless of where the theft occurs.
- **Factual Declaration of Innocence after ID Theft.** This provision allows a victim to petition the court to declare their innocence, and allows the state to create a database of valid claims of identify theft.
- **Affordable Access to Credit Reports.** This provision requires the credit bureaus to provide customers with monthly access to their credit reports for a fee of $2.00 per report.
- **Protecting Social Security Number.** This section protects an individual's social security number by preventing businesses and the state from using it on paperwork unless required by federal law.
- **Disposal of Records.** This provision requires complete destruction of records, electronic and paper, which contain personal information.

Thank you for your consideration.

Brian Hove

From: Chris Wyatt [chris_wyatt@gov.state.ak.us]
Sent: Monday, February 27, 2006 4:48 PM
To: Brian Hove
Subject: SB 222

Attachments: SB222-GOV-OMB-2-27-06-1.pdf

SB222-GOV-OMB-2-27-06-1.pdf (1...

Brian

I have attached a FN on SB 222 from OMB that umbrellas all State Departments. Please have this note replace all others.....Chris

FISCAL NOTE

STATE OF ALASKA
2006 LEGISLATIVE SESSION

Fiscal Note Number:
Bill Version: CSSB 222
() Publish Date:

Revision Date/Time (Note if correction):
Dept. Affected: All
Title: Protection of personal information
RDU
Component
Sponsor: Sens. Therriault and Guess
Requester: Sen. Judiciary Committee
Component No.

Expenditures/Revenues (Thousands of Dollars)

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

OPERATING EXPENDITURES	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011	FY 2012
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 (FY2006) cost: 0.0
Mark this box (X) If funding for this bill is included in the Governor's FY 2007 budget proposal:

POSITIONS

Full-time						
Part-time						
Temporary						

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

This legislation imposes a number of new requirements on State government regarding the protection of personal information, such as Social Security numbers. For example, the bill prohibits the transmission of Social Security numbers a the Internet unless encrypted or otherwise secured. The bill also would prohibit State agencies from collecting Social Security numbers unless specifically authorized by State or federal law.

It appears that State agencies could incur significant costs to comply with this legislation. The total of these costs cannot be accurately projected at this time.

Prepared by: Jack Kreinheder, Senior Analyst
Phone 465-4676
Division: Office of Management and Budget
Date/Time 2/27/06 4:35 PM

Approved by: Cheryl Frasca, Director
Date 2/27/2006
Agency: Office of Management and Budget

(Revised 9/7/2005 OMB)

Talking Points on SB 222 – Identity Theft Protection

ACLI respectfully requests your consideration of the attached amendments to SB 222 relating to breaches of security involving personal information, protection of social security numbers and disposal of records for the following reasons:

Article 1 Breach of Security Involving Personal Information (Sec. 45.48.010-45.48.090)

- ACLI member companies recognize that their customers expect them to maintain the security as well as the confidentiality of their personal information; and acknowledge their affirmative and continuing obligation to protect the confidentiality and security of their customers' personal information.

- ACLI member companies are generally supportive of legislation requiring notification to customers when their computerized personal information has been accessed by unauthorized persons if the security of customers' personal information is threatened.

- To avoid unnecessarily alarming consumers and unnecessary administrative costs, ACLI member companies believe that no notification should be required if the security of customers' information is not truly jeopardized, such as where the information is protected by encryption or other method or technology that renders the information unreadable or useable.

- Similarly, they do not believe that notice should be required (or that a breach of security should be deemed to have occurred) if the business determines with reasonable certainty that misuse of the information is not likely to occur.

- As always, there needs to be an appropriate balance between the costs of providing notice when consumer information is really vulnerable to identity theft and the costs of providing notice when no such jeopardy exists.

Article 4 – Protection of Social Security Number (Sec. 45.48.400-45.48-410)

- In addition to legal requirements imposed by state and federal law, many of our business practices affecting the quality and completeness of customer services rely on Social Security Numbers.
- Social Security Numbers are integral to fraud investigations.
- Social Security Numbers are used to find missing/lost policyholders to inform them that they are entitled to proceeds.
- Social Security Numbers are needed to transfer assets from one financial institution to another, e.g., CDs, mutual funds, annuities. Financial organizations generally do not have the account numbers of the other institution. Social Security Numbers help verify the client's identity, which reduces error, delay and misplaced assets.
- Insurers use Social Security Numbers as the fastest and most accurate way to access information on clients who have multiple products when the customers do not have the account or policy numbers, thus assuring quality service.
- Call Centers use Social Security Numbers as one important element in authenticating callers as customers. A prohibition would interfere with convenient customer service by phone.

- ACLI member companies believe that enforcement of financial institutions' compliance with the use and disclosure of Social Security Numbers should be exclusively with their functional regulators (i.e., by the state insurance commissioner with respect to life insurers).

Article 5 – Disposal of Records (Sec. 45.48.500-45.48.590)

- The Gramrn Leach Bliley Act and 3 A.C 26.705 confirm that financial institutions have a continuing and affirmative obligation to protect *both* the security and the confidentiality of their customers' personal information and require financial institutions to have policies and procedures to provide this protection.

- In view of the extensive requirements already imposed on financial institutions by the GLBA and the Alaska privacy rules, there is no need to subject insurers to additional security requirements on retaining and disclosing of customers' personal information.

Article 4. Protection of Social Security Number.

Sec. 45.48.400. Use of social security number.

~~(6) refuse to do business with an individual because the individual does not consent to the receipt by the person of the social security number of the individual, unless the person is expressly required under federal law, in connection with doing business with an individual, to submit the individual's social security number to the federal government.~~

(b) A person, other than a "financial institution," as defined under section 509(3) of the federal Gramm, Leach Bliley Act (15 USC 6801 et. seq., or a "licensee" as defined in 3 AAC 26.749(a)(16), may not sell, lease, loan, trade, rent, or otherwise disclose an individual's social security number to a third party for any purpose without the individual's written consent.

Sec. 45.48.410. Penalties. (a) Compliance with the requirements imposed under AS 45.48.400 by a "financial institution," as defined under section 509(3) of the federal Gramm, Leach Bliley Act (15 USC 6801 et. seq., or a "licensee" as defined in 3 AAC 26.749(a)(16),shall be enforceable by the Alaska regulatory or supervisory authority having primary jurisdiction over that person.
(b)Compliance with the requirements imposed under AS 45.48.400 by persons other than those described in subsection (a) of this section shall be enforceable as follows: (i) A person who knowingly violates AS 45.48.400 is liable to the state for a civil penalty not to exceed 3,000.
~~(b)~~(ii) An individual may bring a civil action in court against a person who knowingly violates AS 45.48.400 and may recover actual damages or $5,000, whichever amount is greater, and court costs and attorney fees allowed by the court rules.
~~(c)~~(iii) A person who knowingly violates AS 45.48.400 is guilty of a class A misdemeanor.
~~(d)~~(iv) In this section, "knowingly" has the meaning given in AS 11.81.900.

Article 5 – Disposal of Records (Sec. 45.48.500-45.48.590)

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

(1) "business" means a person other than a "financial institution," as defined under section 509(3) of the federal Gramm, Leach Bliley Act (15 USC 6801 et. seq., or a "licensee" as defined in 3 AAC 26.749(a)(16), who: (A) conducts business in the state; or (B) 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;

Consumers Union

February 9, 2006

Re: Support of S 222 and HB 226

Consumers Union, the non-profit independent publisher of *Consumer Reports* ®, appreciates this opportunity to submit its views on providing consumers with tools to protect themselves against identity theft. We support bills S 222 and HB 226, which provide all Alaska consumers with additional identity theft protections such as notice of a data security breach and the option of a security freeze on their credit files at a low or no cost. These bills provide key elements in protecting all Alaska consumers from the cost, stress, and time lost due to identity theft.

Identity theft is a serious and increasingly more common crime in this "information age." According to the Federal Trade Commission, in 2003, nearly 10 million Americans were victims of identity theft, costing businesses and financial institutions nearly $48 billion and consumers $5 billion. When identity thieves open new accounts in a consumer's name, the victim ends up spending, on average, $500 and countless hours cleaning up the damage. The personal costs can be devastating; identity theft can create unimaginable family stress when victims are turned down for mortgages, student loans, and even jobs.

One year ago, consumers nationwide first learned of data security breaches only because of one state's law requiring that its residents be told, and 38 state Attorneys General (including then Attorney General Renke) subsequently demanded that their states' residents be informed as well. The Privacy Rights Clearinghouse, a non-profit, non-partisan privacy education and advocacy organization estimates that over 52 million people have had their personal data put at risk due to security breaches. (See http://privacyrights.org/ar/ChronData Breaches.htm). Since ChoicePoint's February 2005 revelations, nearly half of the nation's states have enacted a notice of security breach law.

Notice of a data security breach helps inform consumers to watch for identity theft more promptly after a breach occurs and leads to better and greater data security. A security freeze gives consumers the personal option to take preventative and proactive steps to stop identity thieves from using stolen personal information to open new credit or other new accounts in consumers' names.

A security freeze allows consumers to control who gains access to the personal information contained in credit files. The security freeze blocks access to new creditors to credit reports and credit scores derived from those reports, until the consumer affirmatively unlocks the file. This would help prevent identity thieves from achieving their ultimate goal – opening up new accounts to accumulate debt in their victims' names, ruining credit reports and credit scores.

To explain how a security freeze works, a consumer initially activates the freeze by placing a request with the credit bureaus. After the freeze has been placed, the consumer can then "thaw" or lift the freeze by providing the credit bureaus with a PIN, allowing specified new creditors into the credit files for a specified period of time. The security freeze helps prevent identity thieves from achieving their ultimate goal – opening up new accounts to accumulate debt in their victims' names, which leads to a ruined credit report and credit score.

A growing number of states have provided consumers with the option of a security freeze. Twelve states now give this right, and most to all consumers can now choose to use the security freeze to prevent identity thieves from opening new accounts in their good names.

We urge you to support strong legislation that provides greater identity theft protections for consumers in Alaska. Both S 222 and HB 226 would provide Alaska's consumers with necessary tools to better protect themselves against identity theft.

Please feel to contact either myself or Gail Hillebrand at 415/431-6747 should you have any questions.

Sincerely,

Michelle Jun
Staff Attorney
Financial Privacy Now
Consumers Union

Comparison of State Security Freeze Laws

State	Who Can Place Security Freeze	Fees	Effective Date	How to Request Security Freeze	Circumstances when Access to a Frozen Credit Report Allowed[1]	State Security Breach Law?
California	All residents	ID theft victims: None Others: $10 (per CRA) to place freeze, $10 for temporary global lifting of freeze, $12 for temporary lifting of freeze for one creditor	January 1, 2003	Freeze must be requested in writing by certified mail	1, 2, 3, 4, 5, 6, 7, 8	Yes
Colorado	All residents	No fee for first freeze; $10 to place a second freeze, $10 for global lift; $12 for temporary lifting for one creditor	July 1, 2006	Freeze must be requested in writing by certified mail	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	No
Connecticut	All residents	$10 to place, lift, or lift temporarily; $12 for lift for one creditor	January 1, 2006	Freeze can be requested in writing by certified mail or other secure method authorized by CRA	1, 2, 6, 7, 8, 14	Yes
Illinois	Victims of ID theft only	None	January 1, 2006	Freeze must be requested in writing by certified mail	1, 2, 3, 4, 5, 6, 7, 8	Yes
Louisiana	All residents	ID theft victims and residents age 62 or older: None Others: $10 to place, $8 to lift	July 1, 2005	Freeze must be requested in writing by certified mail	1, 3, 6, 8, 14, 15, 16, 17, 18	Yes

Maine	All residents	ID theft victims: None Others: up to $10 to place, remove, temporarily lift, have PIN reissues, $12 for lift for a specific creditor	February 1, 2206	Freeze must be requested in writing by certified mail	1, 2, 3, 4, 5, 6, 7, 8	Yes
Nevada	All residents	ID theft victims: None Others: up to $15 to place, $18 to lift, $20 for lift for a specific creditor	October 1, 2005	Freeze must be requested in writing by certified mail	1, 2, 3, 6, 7, 8, 14, 15, 19, 20, 21	Yes
New Jersey	All residents	None for initial freeze, up to $5 to remove, temporarily lift or have PIN reissued	January 1, 2006	Freeze can be requested in writing by certified or overnight mail, or by secure electronic mail connection with CRA	1, 2, 3, 5, 6, 7, 8	Yes
North Carolina	All residents	ID theft victims: None Others: up to $10 to place, remove, or suspend the freeze	December 1, 2005	Freeze must be requested in writing by certified mail	1, 2, 3, 4, 5, 6, 7, 8, 9, 14, 18	Yes
Texas	Victims of ID theft only	$8 (adjusted for inflation) to place, none to remove	September 1, 2003	Freeze must be requested in writing by certified mail, placement of security freeze at one CRA must be honored by all	1, 2, 3, 4, 5, 6, 7, 8, 16, 17, 18	Yes
Vermont	Victims of ID theft only	None	July 1, 2005	Freeze must be requested in writing by certified mail	1, 2, 3, 4, 5, 6, 7, 8	No

Washington	Victims of ID theft or those notified of a security breach of their computerized personal information	None	July 24, 2005.	Freeze must be requested in writing by certified mail	1, 2, 3, 4, 5, 6, 7, 8, 14	Yes

[1] For this section, the following numbers are used:
1= An entity the consumer has a financial obligation or account with
2= Authorized party pursuant to a court order, warrant, or subpoena
3= For child support purposes
4= State agency responsible for investigating Medicaid fraud
5= State agency responsible for investigating delinquent taxes or enforcing state tax laws
6= For prescreening purposes as identified under the FCRA
7= Credit monitoring service to which the consumer has subscribed
8= CRA to provide the consumer with a copy of his or her credit report upon the consumer's request
9= Insurance agent for the purpose of insurance underwriting
10= A pension plan acting to determine the consumer's eligibility for plan benefits or investigating fraud
11= A person conducting a pre-sentence investigation in a criminal matter or parole officer supervising an offender
12= A licensed hospital with which consumer has a contract or debt
13= Law enforcement agencies investigating a crime or conducting a criminal background check
14= Federal, State, or local governmental entity pursuant to their statutory responsibilities
15= Private collection agency assisting the collection of an existing debt
16= CRA which acts only as a reseller and does not maintain a permanent database of credit information
17= A check services or fraud prevention services company
18= A deposit account information service company in reviewing a consumer request for a deposit account
19= An entity which the consumer has an existing business relationship with for any purpose relating to that business relationship
20= A person holding a license issued by state gaming commission
21= Employer using credit report for pre-employment screening or for decisions or investigations of current/former employees

Comparison of State Security Breach Notification Laws

State	Entities Covered	Information Covered	Notification Requirements	Further Duties	Enforcement	Exemptions	Private Right of Action
Arkansas	Commercial, charitable, educational, or nonprofit entities including state agencies	Personal information: Name + SSN, DL, account number/identifier with access code, medical information	Notification without unreasonable delay to individuals whose unencrypted computerized data containing personal information breached if entity suffering breach determines breach presents a reasonable likelihood of harm to customers.	None	State AG	Does not apply to entity regulated by state or federal law that provides greater protection to personal information	No
California	Any person, government agency or business that owns or licenses computerized data containing personal information	Personal information: Name + SSN, DL, account number/identifier with access code	Notification without unreasonable delay to individuals whose unencrypted computerized data containing personal information breached	None	State AG	None	Yes
Connecticut	Persons who conduct business in the state that owns or licenses computerized data containing personal information	Personal information: Name + SSN, DL, account number/identifier with access code	Notification without unreasonable delay to individuals whose unencrypted computerized data containing personal information breached	None	State AG	None	No

State	Entities Covered	Information Covered	Notification Requirements	Further Duties	Enforcement	Exemptions	Private Right of Action
Delaware	Persons who conduct business in the state that owns or licenses computerized data containing personal information	Personal information: Name + SSN, DL, account number/identifier with access code, medical information	Notification without unreasonable delay to individuals whose unencrypted computerized data containing personal information breached	Must promptly provide written notification of the nature and circumstances of breach to Consumer Protection Division of the Department of Justice	State AG, Consumer Protection Division of the Department of Justice	Does not apply to entity regulated by state or federal law that provides greater protection to personal information	Yes, treble damages plus attorney fees
Florida	Persons who conduct business in the state and maintains computerized data containing personal information	Personal information: Name + SSN, DL, account number/identifier with access code	Notification within 45 days following discovery of breach to individuals whose unencrypted computerized data containing personal information breached. Notification not required if after consultation with federal/state/local agencies responsible for law enforcement, business determines harm to consumers not likely as a result of breach	Entity suffering breach must coordinate with CRAs if breach includes information on at least 1,000 individuals	Department of Legal Affairs. Penalties for non-notification increase with time since security breach	None	No
Georgia	Information brokers	Personal information: Name + SSN, DL, account number/identifier with access code	Notification without unreasonable delay to individuals whose unencrypted computerized data containing personal information breached	Entity suffering breach must coordinate with CRAs if breach includes information on at least 10,000 individuals	State AG	None	No

State	Entities Covered	Information Covered	Notification Requirements	Further Duties	Enforcement	Exemptions	Private Right of Action
Illinois	Data collection including government agencies, educational institutes, public and private entities that collects, handles, or disseminates nonpublic personal information	Personal information: Name + SSN, DL, account number/identifier with access code	Notification without unreasonable delay to individuals whose unencrypted computerized data containing personal information breached	None	State AG	None	Yes
Indiana	State agencies holding computerized personal information	Personal information: Name + SSN, DL, account number/identifier with access code	Notification without unreasonable delay to individuals whose unencrypted computerized data containing personal information breached	Agency suffering breach must coordinate with CRAs if breach includes information on at least 1,000 individuals	State AG	None	No
Louisiana	Persons who conduct business in the state including state agencies, that owns or licenses computerized data containing personal information	Personal information: Name + SSN, DL, account number/identifier with access code	Notification without unreasonable delay to individuals whose unencrypted computerized data containing personal information breached	None	State AG	None	No

State	Entities Covered	Information Covered	Notification Requirements	Further Duties	Enforcement	Exemptions	Private Right of Action
Maine	Information brokers	Personal information: Name + SSN, DL, account number/identifier with access code	Notification without unreasonable delay to individuals whose unencrypted computerized data containing personal information breached	Agency suffering breach must notify appropriate state regulator of breach, must also coordinate with CRAs if breach includes information on at least 1,000 individuals	Department of Professional and Financial Regulation, State AG for information brokers not regulated by Department of Professional and Financial Regulation	None	No
Minnesota	Persons who conduct business in the state and maintains computerized data containing personal information	Personal information: Name + SSN, DL, account number/identifier with access code	Notification without unreasonable delay to individuals whose unencrypted computerized data containing personal information breached	Agency suffering breach must coordinate with CRAs if breach includes information on at least 500 individuals	State AG	Does not apply to financial institutions or HIPAA entities	No
Montana	Persons who conduct business in the state and maintains computerized data containing personal information	Personal information: Name + SSN, DL, account number/identifier with access code	Notification without unreasonable delay to individuals whose unencrypted computerized data containing personal information breached	Agency suffering breach must coordinate with CRAs	Consumer Protection Office	Insurance-support organizations follow same breach laws, but Montana Insurance Commissioner has authority	No

State	Entities Covered	Information Covered	Notification Requirements	Further Duties	Enforcement	Exemptions	Private Right of Action
Nevada	Data collectors: includes business entities, government agencies, educational institutions, and associations who handle, collect, or disseminate nonpublic personal information	Personal information: Name + SSN, DL, account number/identifier with access code	Notification without unreasonable delay to individuals whose unencrypted computerized data containing personal information breached	Entity suffering breach must coordinate with CRAs if breach includes information on at least 1,000 individuals	State AG or a district attorney of any county	Data collectors in compliance with GLB exempted	No
New Jersey	Commercial, charitable, or nonprofit entities including state, county, or local government entities	Personal information: Name + SSN, DL, account number/identifier with access code	Notification without unreasonable delay to individuals whose unencrypted computerized data containing personal information breached unless entity suffering breach establishes that misuse of information is not reasonably possible. Must keep written documentation of evidence for 5 years	Entity suffering breach must coordinate with CRAs if breach includes information on at least 1,000 individuals. Must also notify State Police in advance of disclosure of breach	State AG	None	No

State	Entities Covered	Information Covered	Notification Requirements	Further Duties	Enforcement	Exemptions	Private Right of Action
New York	Persons who conduct business in the state and own or license computerized data containing private information, as well as state or local government agencies	Personal information: Name + SSN, DL, account number/identifier with access code	Notification without unreasonable delay to individuals whose unencrypted, or encrypted with acquired encryption key computerized data containing private information breached	Notification must include contact information of entity suffering breach and a description of the categories of information exposed by the breach. Also require notification to State AG, Consumer Protection Board, and the State Office of Cyber Security and Critical Infrastructure Coordination. Entity suffering breach must coordinate with CRAs if breach includes information on at least 5,000 individuals.	State AG	None	No
North Carolina	Persons who conduct business in the state and owns or licenses computerized data containing personal information	Personal information: Name + SSN, DL, account number, password/PIN that would provide access to a consumer's financial account or resources, digital signatures,	Notification without unreasonable delay to individuals whose unencrypted, un-redacted, or encrypted with acquired encryption key computerized data containing personal	Notification must include: description of breach incident, type of personal information that was breached, contact information for further information. If breach	State AG	Any financial institution subject to and in compliance with Federal Interagency Guidance Response Programs for Unauthorized	No

		biometric data	information breached and illegal use of personal information has occurred or is reasonably likely to occur, or creates a material risk of harm to the consumer	includes information on at least 1,000 individuals, Consumer Protection Division of the Attorney General's Office and CRAs must be notified		Access to Consumer Information and Customer Notice exempted	
North Dakota	Persons who conduct business in the state and owns or licenses computerized data containing personal information	Personal information: Name + SSN, DL, account number/identifier with access code, date of birth, maiden name of individual's mother, employee number, digital signature	Notification without unreasonable delay to individuals whose unencrypted computerized data containing personal information breached	None	State AG	Any financial institution subject to and in compliance with Federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and Customer Notice exempted	No
Ohio	Persons who conduct business in the state, as well as state or local government agencies	Personal information: Name + SSN, DL, account number/identifier with access code	Notification without unreasonable delay (no later than 45 days following discovery of the breach) to individuals whose unencrypted, un-redacted computerized data containing personal information breached and is reasonably believed will cause a risk of ID theft or fraud	Entity suffering breach must coordinate with CRAs if breach includes information on at least 1,000 individuals.	State AG	Financial institutions subjected to federal law requiring notification of security breach incidents exempted. Exempts entities regulated by sections 1171 to 1179 of Social Security Act	No

State	Entities Covered	Information Covered	Notification Requirements	Further Duties	Enforcement	Exemptions	Private Right of Action
Pennsylvania	Commercial, charitable, or nonprofit entities that maintain, stores, or manages computerized data including personal information	Personal information: Name + SSN, DL, account number/identifier with access code	Notification without unreasonable delay to individuals whose unencrypted, un-redacted, or encrypted with acquired encryption key computerized data containing personal information breached and entity suffering breach reasonably believe has caused or will cause loss or injury	Entity suffering breach must coordinate with CRAs if breach includes information on at least 1,000 individuals.	State AG	Any financial institution subject to and in compliance with Federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and Customer Notice exempted. Financial institutions subjected to federal rules or regulations requiring notification of security breach incidents exempted	No
Rhode Island	Any person or business that conducts business in the state and owns or licenses computerized data containing personal information	Personal information: Name + SSN, DL, account number/identifier with access code	Notification without unreasonable delay to individuals whose unencrypted computerized data containing personal information breached	None	State AG	Financial institutions subjected to state or federal law providing greater protections to personal information exempted. Does not apply to HIPAA entities	Yes

State	Entities Covered	Information Covered	Notification Requirements	Further Duties	Enforcement	Exemptions	Private Right of Action
Tennessee	Any business or state or local government agency that owns or licenses computerized data containing personal information	Personal information: Name + SSN, DL, account number/identifier with access code	Notification without unreasonable delay to individuals whose unencrypted computerized data containing personal information breached	Entity suffering breach must coordinate with CRAs if breach includes information on at least 1,000 individuals.	State AG	Financial institutions subject to GLB exempted	Yes
Texas	Any person or business that conducts business in the state and owns or licenses computerized data containing sensitive personal information	Personal information: Name + SSN, DL, account number/identifier with access code	Notification without unreasonable delay to individuals whose computerized data containing personal information breached	Entity suffering breach must coordinate with CRAs if breach includes information on at least 10,000 individuals.	State AG	None	No
Washington	Any business or state or local government agency that owns or licenses computerized data containing personal information	Personal information: Name + SSN, DL, account number/identifier with access code	Notification without unreasonable delay to individuals whose computerized data containing personal information breached. Notification not required if it is a technical breach of security that does not seem reasonably likely to subject consumers to a risk of criminal activity.	None	State AG	None	Yes

A Chronology of Data Breaches Reported Since the ChoicePoint Incident

Posted: April 20, 2005
Updated January 24, 2006

Privacy Rights CLEARINGHOUSE

3100 - 5th Ave., Suite B
San Diego, CA 92103
Voice: (619) 298-3396
Fax: (619) 298-5681
Web: www.privacyrights.org
Contact Us:
www.privacyrights.org/inquiryform.html

HOME

A Chronology of Data Breaches Reported Since the ChoicePoint Incident

The data breaches noted below have been reported because the personal information compromised includes data elements useful to identity thieves, such as Social Security numbers, account numbers, and driver's license numbers.

The catalyst for reporting data breaches to the affected individuals has been the California law that requires notice of security breaches, the first of its kind in the nation, implemented July 2003.
www.privacyrights.org/ar/SecurityBreach.htm
www.privacy.ca.gov/recommendations/secbreach.pdf

This chronology below begins with ChoicePoint's 2/15/05 announcement of its data breaches because it was a watershed event in terms of disclosure to the affected individuals. Since then, the "best practice" has been to disclose breaches to individuals nationwide -- in a sense, adopting California's notice requirement nationally.

In the meantime, over half the states have considered legislation on security breach notices and security freezes in 2005, and several states passed laws requiring that individuals be notified of security breaches. For a list of those states enacting breach and freeze laws, visit the Consumers Union web site here:
Security breach notice laws: www.consumersunion.org/campaigns/Breach_laws_May05.pdf
Security freeze laws: www.consumersunion.org/campaigns/learn_more/002355indiv.html
State security freeze bills pending in 2006: www.financialprivacynow.org

And visit the PIRG site here: www.pirg.org/consumer/credit/statelaws.htm.

Congress is considering several bills this year in which security breach notices would be mandated nationwide. See http://thomas.loc.gov. See also EPIC's bill-track list, www.epic.org/privacy/bill_track.html.

Here are other sources for security breach information:

- Identity Theft Resource Center, www.idtheftcenter.org/breaches.pdf
- Adam Shostack's blog, www.emergentchaos.com/archives/cat_breaches.html
- Attrition, www.attrition.org/errata/dataloss.html
- World Privacy Forum, Security Breaches in the Digital Medical Environment (scroll to

section D of testimony),
www.worldprivacyforum.org/testimony/NCVHStestimony_092005.html

DATE MADE PUBLIC	NAME	TYPE OF BREACH	NUMBER
Feb. 15, 2005	ChoicePoint	Bogus accounts established by ID thieves	145,000
Feb. 25 , 2005	Bank of America	Lost backup tape	1,200,000
Feb. 25, 2005	PayMaxx	Exposed online	25,000
March 8, 2005	DSW/Retail Ventures	Hacking	100,000
March 10, 2005	LexisNexis	Passwords compromised	32,000
March 11, 2005	Univ. of CA, Berkeley	Stolen laptop	98,400
March 11, 2005	Boston College	Hacking	120,000
March 12, 2005	NV Dept. of Motor Vehicle	Stolen computer	8,900
March 20, 2005	Northwestern Univ.	Hacking	21,000
March 20, 2005	Univ. of NV., Las Vegas	Hacking	5,000
March 22, 2005	Calif. State Univ., Chico	Hacking	59,000
March 23, 2005	Univ. of CA, San Francisco	Hacking	7,000
March 28, 2005	Univ. of Chicago Hospital	Dishonest insider	unknown
April ?, 2005	Georgia DMV	Dishonest insider	465,000
April 5, 2005	MCI	Stolen laptop	16,500
April 8, 2005	Eastern National	Hacker	15,000
April 8, 2005	San Jose Med. Group	Stolen computer	185,000
April 11, 2005	Tufts University	Hacking	106,000
April 12, 2005	LexisNexis	Passwords compromised	Additional 280,000
April 14, 2005	Polo Ralph Lauren/HSBC	Hacking	180,000
April 14,	Calif. Fastrack	Dishonest Insider	4,500

2005			
April 15, 2005	CA Dept. of Health Services	Stolen laptop	21,600
April 18, 2005	DSW/ Retail Ventures	Hacking	Additional 1,300,000
April 20, 2005	Ameritrade	Lost backup tape	200,000
April 21, 2005	Carnegie Mellon Univ.	Hacking	19,000
April 26, 2005	Mich. State Univ's Wharton Center	Hacking	40,000
April 26, 2005	Christus St. Joseph's Hospital	Stolen computer	19,000
April 28, 2005	Georgia Southern Univ.	Hacking	"tens of thousands"
April 28, 2005	Wachovia, Bank of America, PNC Financial Services Group and Commerce Bancorp	Dishonest insiders	676,000
April 29, 2005	Oklahoma State Univ.	Missing laptop	37,000
May 2, 2005	Time Warner	Lost backup tapes	600,000
May 4, 2005	CO. Health Dept.	Stolen laptop	1,600 (families)
May 5, 2005	Purdue Univ.	Hacking	11,360
May 7, 2005	Dept. of Justice	Stolen laptop	80,000
May 11, 2005	Stanford Univ.	Hacking	9,900
May 12, 2005	Hinsdale Central High School	Hacking	2,400
May 16, 2005	Westborough Bank	Dishonest insider	750
May 18, 2005	Jackson Comm. College, Michigan	Hacking	8,000
May 18, 2005	Univ. of Iowa	Hacking	30,000
May 19, 2005	Valdosta State Univ., GA	Hacking	40,000
May 20, 2005	Purdue Univ.	Hacking	11,000
May 26, 2005	Duke Univ.	Hacking	5,500
May 27, 2005	Cleveland State Univ.	Stolen laptop **Update 12/24:** CSU found the stolen	[44,420] Not included in total below

		laptop	
May 28, 2005	Merlin Data Services	Bogus acct. set up	9,000
May 30, 2005	Motorola	Computers stolen	unknown
June 6, 2005	CitiFinancial	Lost backup tapes	3,900,000
June 10, 2005	Fed. Deposit Insurance Corp. (FDIC)	Not disclosed	6,000
June 16, 2005	CardSystems	Hacking	40,000,000
June 17, 2005	Kent State Univ.	Stolen laptop	1,400
June 18, 2005	Univ. of Hawaii	Dishonest Insider	150,000
June 22, 2005	Eastman Kodak	Stolen laptop	5,800
June 22, 2005	East Carolina Univ.	Hacking	250
June 25, 2005	Univ. of CT (UCONN)	Hacking	72,000
June 28, 2005	Lucas Cty. Children Services (OH)	Exposed by email	900
June 29, 2005	Bank of America	Stolen laptop	18,000
June 30, 2005	Ohio State Univ. Med. Ctr.	Stolen laptop	15,000
July 1, 2005	Univ. of CA, San Diego	Hacking	3,300
July 6, 2005	City National Bank	Lost backup tapes	unknown
July 7, 2005	Mich. State Univ.	Hacking	27,000
July 19, 2005	Univ. of Southern Calif. (USC)	Hacking	270,000 possibly accessed; "dozens"exposed
July 21, 2005	Univ. of Colorado-Boulder	Hacking	42,000
July 30, 2005	San Diego Co. Employees Retirement Assoc.	Hacking	33,000
July 30, 2005	Calif. State Univ., Dominguez Hills	Hacking	9,613
July 31, 2005	Cal Poly-Pomona	Hacking	31,077
Aug. 2, 2005	Univ. of Colorado	Hacking	36,000

Aug. 9, 2005	Sonoma State Univ.	Hacking	61,709
Aug. 9, 2005	Univ. of Utah	Hacking	100,000
Aug. 10, 2005	Univ. of North Texas	Hacking	39,000
Aug. 17, 2005	Calif. State University, Stanislaus	Hacking	900
Aug. 19, 2005	Univ. of Colorado	Hacking	49,000
Aug. 22, 2005	Air Force	Hacking	33,300
Aug. 27, 2005	Univ. of Florida, Health Sciences Center/ChartOne	Stolen Laptop	3,851
Aug. 30, 2005	J.P. Morgan, Dallas	Stolen Laptop	Unknown
Aug. 30, 2005	Calif. State University, Chancellor's Office	Hacking	154
Sept. 10, 2005	Kent State Univ.	Stolen Computers	100,000
Sept. 15, 2005	Miami Univ.	Exposed Online	21,762
Sept. 16, 2005	ChoicePoint (2nd notice, see 2/15/05 for 145,000)	ID thieves accessed; also misuse of IDs & passwords.	9,903
Sept. 17, 2005	North Fork Bank, NY	Stolen laptop (7/24/05) with mortgage data	9,000
Sept. 19, 2005	Children's Health Council, San Jose CA	Stolen backup tape	5,000 - 6,000
Sept. 22, 2005	City University of New York	Exposed online	350
Sept. 23, 2005	Bank of America	Stolen laptop with info of Visa Buxx users (debit cards)	Not disclosed
Sept. 28, 2005	RBC Dain Rauscher	Illegitimate access to customer data by former employee	100+ customers' records compromised out of 300,000
Sept. 29, 2005	Univ. of Georgia	Hacking	At least 1,600
Oct. 12, 2005	Ohio State Univ. Medical Center	Exposed online. Appointment information including SSN, DOB, address, phone no., medical	2,800

		no., appointment reason, physician.	
Oct. 15, 2005	Montclair State Univ.	Exposed online	9,100
Oct. 21, 2005	Wilcox Memorial Hospital, Hawaii	Lost backup tape	130,000
Nov. 1, 2005	Univ. of Tenn. Medical Center	Stolen laptop	3,800
Nov. 4, 2005	Keck School of Medicine, USC	Stolen computer	50,000
Nov. 5, 2005	Safeway, Hawaii	Stolen laptop	1,400 in Hawaii, perhaps more elsewhere
Nov. 8, 2005	ChoicePoint	Bogus accounts established by ID thieves Total affected now reaches 162,000 (See Feb. 15 & Sept. 16)	17,000 more
Nov. 9, 2005	TransUnion	Stolen computer	3,623
Nov. 11, 2005	Georgia Tech Ofc. of Enrollment Services	Stolen computer, Theft 10/16/05	13,000
Nov. 11, 2005	Scottrade Troy Group	Hacking	Unknown
Nov. 19, 2005	Boeing	Stolen laptop with HR data incl. SSNs and bank account info.	161,000
Dec. 1, 2005	Firstrust Bank	Stolen laptop	100,000
Dec. 1, 2005	Univ. of San Diego	Hacking. Faculty, students and employee tax forms containing SSNs	7,800
Dec. 2, 2005	Cornell Univ.	Hacking. Names, addresses, SSNs, bank names and acct. numbers.	900
Dec. 6, 2005	WA Employment Security Dept.	Stolen laptop. Names, SSNs and earnings of former employees.	530
Dec. 12, 2005	Sam's Club/Wal-Mart	Unknown. Exposed credit card data at gas stations.	Unknown
Dec. 16, 2005	La Salle Bank, ABN AMRO Mortgage Group	Backup tape with residential mortgage customers lost in	[2,000,000] Not included in total below

		shipment by DHL, containing SSNs and account information. **Update 12/20:** DHL found the lost tape	
Dec. 16, 2005	Colorado Tech. Univ.	Email erroneously sent containing names, phone numbers, email addresses, Social Security numbers and class schedules.	1,200
Dec. 20, 2005	Guidance Software, Inc.	Hacking. Customer credit card numbers	3,800
Dec. 22, 2005	Ford Motor Co.	Stolen computer. Names and SSNs of current and former employees.	70,000
Dec. 25, 2005	Iowa State Univ.	Hacking. Credit card information and Social Security numbers.	5,500
Dec. 28, 2005	Marriot International	Lost backup tape. SSNs, credit card data of time-share owners	206,000
Jan. 1, 2006	University of Pittsburgh Medical Center, Squirrel Hill Family Medicine	6 Stolen computers. Names, Social Security numbers, birthdates	700
Jan. 2, 2006	H&R Block	SSNs exposed in 40-digit number string on mailing label	Unknown
Jan. 9, 2006	Atlantis Hotel - Kerzner Int'l	Dishonest insider or hacking. Names, addresses, credit card details, Social Security numbers, driver's licence numbers and/or bank account data.	55,000
Jan. 12, 2006	People's Bank	Lost computer tape containing names, addresses, Social Security numbers, and checking account numbers.	90,000
Jan. 17, 2006	City of San Diego, Water & Sewer Dept.	Dishonest employee accessed customer account files, including SSNs, and committed identity	Unknown

		theft on some individuals.	
Jan. 21, 2006	California Army National Guard	Stolen briefcase with personal information of National Guardsmen including a "seniority roster," Social Security numbers and dates of birth.	"hundreds of officers"
Jan. 23, 2006	Univ. of Notre Dame	Hackers accessed Social Security numbers, credit card information and check images of school donors.	Unknown
Jan. 24, 2006	Univ. of WA Medical Center	Stolen laptops containing names, Social Security numbers, maiden names, birth dates, diagnoses and other personal data.	1,600
TOTAL			**52,188,132**

HOME TOP

AARP Alaska

February 21, 2006

Honorable Ralph Seekins, Chair
Senate Judiciary Committee
Alaska State Capitol, Room 125
Juneau, Alaska 99801-1182

RE: SB222 (Therriault and Guess)--Support

Dear Chair Seekins:

On behalf of the members of AARP in Alaska, we urge you and your colleagues on the Senate Judiciary Committee to support SB 222, authored by your Committee colleagues Senators Gene Therriault and Gretchen Guess and co-sponsored by Senate Minority Leader Johnny Ellis.

The Problem
Identity theft is an important issue to AARP. Identity theft is a serious crime that is both widespread and costly. According to a Federal Trade Commission (FTC) survey released in January 2006, Alaska ranked first among all states in the number of fraud complaints, per 100,000 population, and 26th in the number of identify theft victims made to the ID Theft Clearinghouse. This is not just a problem for the lower 48. There were 421 ID theft complaints made in 2005 from Alaskans to the National Identity Theft Data Clearinghouse.

People whose identities are stolen can spend months or years – and their hard earned money – cleaning up the mess thieves made of their good name and credit record. In the meantime, victims may lose job opportunities, be refused loans for education, housing or automobiles, or even get arrested for crimes they did not commit. In addition, the almost daily news reports about data breaches and mishandling of consumers' personal identifying information demonstrate how important it is to safeguard the personal information that not only identifies us, but also provides entrée to our most sensitive financial information. The newspaper USA Today reported that in 2005, at least 130 reported breaches exposed more than 55 million people to potential identity theft.

A security freeze lets consumers stop identity thieves from getting credit in their names. The security freeze blocks or freezes access to consumers' credit files. In most instances, businesses will not issue new credit to an applicant when the businesses cannot obtain credit information about the person. If consumers freeze their credit files, it does not prevent them from obtaining new credit. Consumers can simply "thaw" the freeze. Once the business providing the new credit obtains the credit reports and credit scores, the freeze can be renewed.

Federal Action

In December 2003, Congress amended the Fair Credit Reporting Act (FCRA), which provides consumer protections regarding the use, accuracy and privacy of consumer credit reports. Through the enactment of the Fair and Accurate Credit Transactions Act (FACT Act)[1], several important consumer protections regarding identity theft were added to FCRA. One of the identity theft provisions was the "one-call" fraud alert. The fraud alert provision permits a notation to be placed on the credit report of consumers who are or believe they may be victims of identity theft. The notation asks issuers of credit to check with the consumers prior to issuing new credit. The fraud alert does not prevent access to the credit report, nor does it prevent the issuance of new credit. The fraud alert should not be confused with a security freeze.

State Action

Twelve (12) states have enacted security freeze laws.[2] While these laws vary in some ways, they all have a common goal – to provide consumers some control over who can gain access to their credit files. As Alaska develops a security freeze law, there are several issues that should be given special consideration.

Who Can Place A Freeze?

AARP believes that all consumers should be able to place a freeze on their credit files. State and federal laws already provide a number of protections for victims of identity theft. Consumers now need a law that will give them the opportunity to protect themselves. Eight states (CA, CO, CT, LA, ME, NV, NJ, NC) currently permit all consumers to place a security freeze. Four states (IL, TX, VT, WA) have laws that apply only to victims of identity theft. However, it should be noted that in each of these states except Texas, bills have been introduced and are moving forward to expand coverage of the laws to all consumers.

Placing and Lifting a Freeze

Security freeze laws are fairly uniform with regard to how a consumer can request a freeze. All states require the request to be in writing and sent by certified mail. AARP believes that consideration should be given to other methods for requesting a freeze as long as the method is secure and the Consumer Reporting Agencies establish policies and procedures to ensure that they can provide proper verification of the consumer. Such methods as a secure electronic mail connection can significantly reduce the amount of time that will be required to place, remove or temporarily lift a freeze. At the present time, most state laws require the freeze be lifted in no more than three (3) days. New Jersey's law set a "15 minute goal" for temporarily lifting a freeze. If this reduction in time can be achieved, consumers will be able to take advantage of those instant credit offers made by retailers, even if they have placed a freeze on their credit files.

---

[1] Pub. L. No. 108-159 (2003).

[2] California, Colorado, Connecticut, Illinois, Louisiana, Maine, Nevada, New Jersey, North Carolina, Texas, Vermont and Washington.

Fees

The issue of fees has caused some significant variations in state laws. Colorado and New Jersey do not require any consumers to pay a fee to place a freeze on their credit files. All of the other states except Connecticut and Texas permit identity theft victims to place a freeze without paying a fee. Louisiana also permits residents 62 years of age and older to avoid paying to place a freeze. For everyone else, the fees for placing a freeze range from low of $8.00 in Texas to a high of $15.00 in Nevada. There is also significant variation in fees charged depending on whether the temporary lifting of the freeze is global versus applying to a specific creditor.

AARP believes that the amount of the fee charged should be reasonable and supports whatever efforts are made to reduce the number of fees that must be paid by the consumer to have a security freeze. The $5.00 fee proposed in SB 222 is reasonable and affordable.

AARP believes that all consumers should have the choice to place a freeze on their credit files. First, the freeze is the best form of identity theft protection that consumers currently have at their disposal. Even though it is by no means a 100% guarantee of safety, it can provide some piece of mind for consumers. Second, the freeze provides consumers a measure of control over their financial security that is not otherwise available. Finally, while the freeze is not for everyone, it should be available for those who wish to have it.

Concern

We asked AARP's attorney that specializes in Identify Theft to review this bill. The only concern she had was the preemption clause. AARP's position is that the State of Alaska needs to maintain the right to protect our citizens and the preemption provision undermines that right. As you know, currently preemption is unsettled law and is being debated in several courts. Eventually this issue will be settled by the courts. Until that happens, state law should prevail, particularly since federal law provides less protection.

Conclusion

Privacy is of considerable concern to the 84,000 AARP members in Alaska, and surveys that we have conducted across the country show that most do not believe that their personal information is being adequately protected. We are grateful that Senators Therriault, Guess and Ellis have taken the time to consider this important issue and we encourage your Committee to support adoption of this legislation for the citizens of our state. We also welcome the opportunity to work with the authors and support legislation that will protect Alaskans from the devastating crime of identity theft.

AARP recommends an "AYE" vote on SB 222.

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 Charlie Huggins
Senator Gene Therriault
Senator Hollis French
Senator Gretchen Guess

Consumers Union

February 9, 2006

Re: Support of S 222 and HB 226

Consumers Union, the non-profit independent publisher of *Consumer Reports* ®, appreciates this opportunity to submit its views on providing consumers with tools to protect themselves against identity theft. We support bills S 222 and HB 226, which provide all Alaska consumers with additional identity theft protections such as notice of a data security breach and the option of a security freeze on their credit files at a low or no cost. These bills provide key elements in protecting all Alaska consumers from the cost, stress, and time lost due to identity theft.

Identity theft is a serious and increasingly more common crime in this "information age." According to the Federal Trade Commission, in 2003, nearly 10 million Americans were victims of identity theft, costing businesses and financial institutions nearly $48 billion and consumers $5 billion. When identity thieves open new accounts in a consumer's name, the victim ends up spending, on average, $500 and countless hours cleaning up the damage. The personal costs can be devastating; identity theft can create unimaginable family stress when victims are turned down for mortgages, student loans, and even jobs.

One year ago, consumers nationwide first learned of data security breaches only because of one state's law requiring that its residents be told, and 38 state Attorneys General (including then Attorney General Renke) subsequently demanded that their states' residents be informed as well. The Privacy Rights Clearinghouse, a non-profit, non-partisan privacy education and advocacy organization estimates that over 52 million people have had their personal data put at risk due to security breaches. (See http://privacyrights.org/ar/ChronData Breaches.htm). Since ChoicePoint's February 2005 revelations, nearly half of the nation's states have enacted a notice of security breach law.

Notice of a data security breach helps inform consumers to watch for identity theft more promptly after a breach occurs and leads to better and greater data security. A security freeze gives consumers the personal option to take preventative and proactive steps to stop identity thieves from using stolen personal information to open new credit or other new accounts in consumers' names.

A security freeze allows consumers to control who gains access to the personal information contained in credit files. The security freeze blocks access to new creditors to credit reports and credit scores derived from those reports, until the consumer affirmatively unlocks the file. This would help prevent identity thieves from achieving their ultimate goal – opening up new accounts to accumulate debt in their victims' names, ruining credit reports and credit scores.

To explain how a security freeze works, a consumer initially activates the freeze by placing a request with the credit bureaus. After the freeze has been placed, the consumer can then "thaw" or lift the freeze by providing the credit bureaus with a PIN, allowing specified new creditors into the credit files for a specified period of time. The security freeze helps prevent identity thieves from achieving their ultimate goal – opening up new accounts to accumulate debt in their victims' names, which leads to a ruined credit report and credit score.

A growing number of states have provided consumers with the option of a security freeze. Twelve states now give this right, and most to all consumers can now choose to use the security freeze to prevent identity thieves from opening new accounts in their good names.

We urge you to support strong legislation that provides greater identity theft protections for consumers in Alaska. Both S 222 and HB 226 would provide Alaska's consumers with necessary tools to better protect themselves against identity theft.

Please feel to contact either myself or Gail Hillebrand at 415/431-6747 should you have any questions.

Sincerely,

Michelle Jun
Staff Attorney
Financial Privacy Now
Consumers Union

AkPIRG
Alaska Public Interest Research Group
P.O. Box 101093 | 507 E Street, Suite 213 | p: 907.278.3661
Anchorage, AK 99510 | Anchorage, AK 99501 | f: 907.278.9300

AkPIRG Testimony on SB 222 Protection of Personal Information

Senate Judiciary Committee

Thank you for the opportunity to speak in favor of Senate Bill 222. It is encouraging to see the Legislature working together to protect Alaskan consumers from Identity Theft.

It's been a year since the Choicepoint Inc. data breach that began a deluge of dangerous releases of consumers' personal, financial information. More than 52 million people have been put in danger of identity theft because of security breaches since that time, according to the Privacy Rights Clearinghouse.

Alaska topped the nation in fraud complaints last year: 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.

The two most important measures of SB 222 will mandate that consumers be notified after a security breach and will allow consumers to freeze their credit reports.

Twenty-seven states have filed security freeze bills, including California and Texas which have filed bills to strengthen their existing security freeze laws. There are now a total of twelve states with laws allowing consumers to restrict access to their credit reports, with more states taking this necessary step to protect consumers.

Security breach notification legislation was introduced in at least 35 states. As of January 2006, at least 23 states have passed security breach notification laws.

It is time for Alaska to take these steps to better protect Alaskan consumers. Other provisions in SB 226 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.

Sincerely,

Steve Cleary
AkPIRG Director

STATE OF ALASKA
DIVISION OF MOTOR VEHICLES

REQUEST FOR RESEARCH OF MOTOR VEHICLE RECORD

Requestor (Owner/Manager Name) Business Name

AK Driver's License Number* Date of Birth* Social Security Number*

*A photocopy of the driver's license or social security card is required for verification purposes

You can only obtain the information if you can certify that you are authorized to receive the information for one of the reasons outlined under REQUESTOR'S CERTIFICATION below.

Please complete and sign the statement to prevent delaying your request

REQUESTOR'S CERTIFICATION

I certify that I am authorized to receive the motor vehicle record information for the reason checked below:

_____ **1. I am the owner of record of this vehicle.**

_____ **2. I have the written permission of the/all owner(s) and lienholder (if lienholder is an individual) of record of this vehicle. (attach owner's and leinholder's permissions)**

_____ **3. I am an agent, employee, or contractor of a business and this information will be used to verify information submitted in the course of this business.**

Owner's Name _____

Owner's Address _____

_____ **4. The requested information is to be used in connection with a civil, criminal, administrative or arbitration proceeding in a court or government agency or before a self-regulatory body.**

_____ **5. I am an agent, employee or contractor for an insurer or an insurance support agency and the information will be used in connection with claims investigation activities, anti-fraud activities, rating or underwriting.**

_____ **6. The information will be used to provide notice to owners of a towed, impounded or abandoned vehicle.**

I certify under penalty of law that I am authorized as an individual or as an employee, agent or contractor of a business to receive motor vehicle record information as provided in AS 28.10.505 for the reason checked above. I further certify that this information will not be sold or disclosed except as provided by law.

_____ / / 20 _____

Signature **Date**

ChoicePoint

The Importance of Social Security Numbers

In recent years, the issue of Social Security Number (SSN) privacy has been one of the most contentious and debated - mostly focused on the potential for misuse associated with the number that plays such an important role in our Information Age. From stories of Internet stalkers to identity theft, those who oppose the use of the SSN by businesses and governments have a compelling story of the worst-case scenario. However, the fact remains that SSNs are one of the strongest personal identifiers available to verify a person's identity, tie lost or hidden assets to their owners, and locate and apprehend fugitives. Using SSNs, consumers have benefited from instant credit and lower insurance rates and society has benefited from reunited families and apprehended criminals. Because of these benefits and because privacy concerns can be mitigated through the responsible use of information, ChoicePoint supports the continued availability and responsible use of SSNs for decisions that matter.

SSNs help businesses authenticate a consumer's identity when opening an account or conducting a customer transaction. For example, SSNs serve as a unique identifier in the insurance industry to match the individual with records obtained in the underwriting process. This use ensures that the information used is accurate and refers specifically to the applicant. Furthermore, SSNs are used to administer accounts and ensure prompt claims payments.

Likewise, employers rely on SSNs to administer background checks for prospective employees. In an increasingly anonymous world where millions of Americans move every year, there has to be a constant identifier that can be used to tie together records and information from across the country. By requiring an SSN from a prospective employee, employers can more easily locate previous addresses - including those not disclosed on an application - and focus records searches in those areas. This makes the system more efficient and more likely to mitigate the risks of making a poor hiring decision.

The use of SSNs is not just a matter of businesses trying to make money. Public sector agencies depend on SSNs to fulfill their duties. The National Center for Missing and Exploited Children (NCMEC) uses information products to reunite missing and runaway children with their parents or legal guardians. The SSN plays an important role in this job. For example, the suspect's SSN is one of the first items obtained by NCMEC so that other databases and disparate information can be collected and analyzed in an attempt to locate the suspect and, hopefully, the missing child. ChoicePoint's information products have led to the recovery of 771 missing children by NCMEC.

In addition, child support enforcement and welfare fraud prevention agencies depend on SSNs to crosscheck multiple private and public databases to verify identities and application information and to prevent fraud. These agencies use SSNs to match public records that would indicate hidden assets.

While SSNs can be an important component of public records, it is important to recognize that companies like ChoicePoint do not use public records to "harvest" SSNs. Rather, where the SSN exists in a public record that item is an important verification element so that the record retriever can be assured that the bankruptcy file on "John Smith" they have obtained from the courthouse is about the right John Smith. By limiting the availability of SSNs in public records, governments are reducing efficiencies in the private sector and, where they are customers of public record companies, reducing their own efficiency in locating delinquent parents, screening welfare recipients, and conducting police investigations.

continued

While we believe that the SSN is a very important identifier that must be available to government and businesses, ChoicePoint does not want to see SSNs widely available to the general public and supports efforts to restrict their use in this market. In addition, we support strong penalties for those who use SSNs to misappropriate the identities of others for fraud or to harm the individual. We have supported federal legislation that meets this important balancing test and will continue to police ourselves and our industry to ensure that misuse is punished.

We ask public policy makers to consider the important role that SSNs play in our Information Economy when they consider restrictions on their availability and use. Concerns for individual anonymity and privacy must be balanced with society's requirements for accountability by its members. Only by allowing for the responsible use of information can these often conflicting goals be balanced.

ChoicePoint® 1000 Alderman Drive Alpharetta, GA 30005 800.342.5339 www.choicepoint.net

ChoicePoint (NYSE: CPS) is the leading provider of identification and credential verification services for making smarter decisions in today's fast-paced world, serving the information needs of business, government and individuals. ChoicePoint is committed to protecting personal privacy and promoting the responsible use of information to help create a safer world. For more information about ChoicePoint, visit the Company's Web site at www.choicepoint.net.

The Importance of Credit Header Information

Although there is no common definition of a credit header, a credit header consists of identifying information, typically a consumer's name, address, month and year of birth, and may also include a social security number. Credit headers do not contain credit information.

ChoicePoint provides information and verification products and services that rely on identifying information from credit headers. These products and services are used by private and charitable organizations, businesses, law enforcement, and government 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.

Existing Law: 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.

ChoicePoint adheres to the strict requirements of FCRA and GLBA.

Credit Header Uses in Reducing Financial Fraud, including Identity Theft:

- *Insurance companies*. Credit header data is critical in helping prevent fraudulent insurance claims and are used widely to verify identity to ensure that insurance claims are not paid to undeserving individuals.
- *Financial Institutions*. Banks 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.
- *Retailers*. 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.
- *Law enforcement*. Credit heard information provides the most current contact information enabling law enforcement to locate witnesses and suspects, make arrests, thwart unlawful activities, and collect criminal fines.
- *Child Support Enforcement*. Credit headers are widely used by government law enforcement agencies to locate deadbeat parents and enforce outstanding child support debts.

- *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.

Reasons for Opposition to Regulation of Credit Header information:

- *Credit header information is all ready regulated*. Since credit header information is strictly regulated by FCRA and GLBA, additional laws are unnecessary.

- *Credit headers do not contain credit information*. The FCRA and similar state laws are not intended to impose restrictions on credit headers because the information in credit headers does not bear on credit worthiness.

- *Credit header information has valuable societal uses*. Prohibiting or restricting the ability to gain access to a credit header will significantly restrict access to this information for critical societal uses