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

(1) "consumer" means an individual;

(2) "consumer report" means a written, oral, or other communication of information by a consumer 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;

(3) "consumer 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 consumer reports to third parties;

(4) "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;

(5) "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 and 45.48.410, enacted by sec. 1 of this Act, apply shall make reasonable efforts to cooperate, through systems testing and other means, to ensure that the requirements of AS 45.48.400 and 45.48.410 are implemented on or before the effective date of AS 45.48.400 and 45.48.410.

Consumers Union

Febr ary 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, 200[illegible]	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 or ' r, 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 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	N·
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 o 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

FISCAL NOTE

STATE OF ALASKA
2006 LEGISLATIVE SESSION

Fiscal Note Number:
Bill Version: SB222-DOT-530-01-24-06
() Publish Date:

Revision Date/Time (Note if correction):
Dept. Affected: DOT&PF
Title: Security of personal information
RDU: DOT&PF
Component: Commissioner's Office
Sponsor: Therriault
Requester:
Component No.: 530

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)*
Based upon current information, DOT&PF is unable to determine what fiscal impact, if any, the bill would have on the department's budget.

Prepared by: John Manly
Division: Legislative Liaison, DOT&PF
Phone: 465-8994
Date/Time: 1/24/06 4:00 PM
Approved by: Mike Barton
Agency: Commissioner, DOT&PF
Date: 1/24/06

(Revised 9/7/2005 OMB)

WRIGHT SERVICES

Wright Services, Inc.
5454 Shaune Drive
Juneau, Alaska 99801-9539

January 24, 2006

Senator Con Bunde, Chairman
Senate Labor & Commerce Committee
State Capitol Room 506
Juneau, Alaska 99801

Dear Senator Bunde:

As a victim of identity theft several years ago, I support the Legislature's effort to prevent identity theft and protect consumer privacy, and I commend the efforts of Senators Therriault and Guess to protect Alaskans against identity theft.

However, I am troubled by Section 45.48.400(6), starting at line 27 of page 15 of the bill, which prevents businesses such as ours from refusing to do business with consumers who will not furnish us with their Social Security number. In spite of the fact that it was never intended to be used as a national identifier, the SSN is now the standard identifier used by financial institutions, credit agencies, government agencies, and the judicial system.

We own and manage almost 500 units of rental housing in Juneau and Anchorage, and require all applicants to furnish us with their name, date of birth, and Social Security number. We do not usually conduct credit checks, but instead conduct court record searches on all applicants.

Without an applicant's Social Security number, we cannot properly screen applicants so that we do not rent properties to applicants with criminal histories (especially sex offenders) or a history of evictions or small claims actions.

If a tenant ends up owing us money, whether by eviction, a small claims action, or by leaving without notice, and we have a judgment against her or him, we cannot garnish the debtor's Permanent Fund Dividend or bank accounts without their Social Security number.

We treat all applications confidentially, as fair housing laws require. All our employees who handle applications are instructed that the information is confidential. Any documents containing personal identifying or financial information are kept confidential and shredded when discarded.

We request that paragraph 6 be deleted from Section 45.48.400 before SB 222 passes out of your committee.

Thanks you for your attention to our concerns. Please contact me at 780-5454 if you wish further information or comments.

Sincerely,

Thom Buzard
General Manager

Lisa Corrigan is here to testify for the Alaska Bankers Association.
- Handouts for committee

Senate Bill 222
Testimony before Senate Labor & Commerce Committee – 1/24/06

My name is Lisa Corrigan. I am the E.V.P. and Chief Operating Officer of Alaska Pacific Bank, a small community bank headquartered in Juneau. I also serve as President of the Alaska Bankers Association, which represents nine banks and includes state and federally chartered financial institutions.

Alaskan bankers share the concerns of the bill sponsors and are dedicated to protecting the privacy and security of sensitive customer information. My comments pertain to three points of clarification that bankers would like to see incorporated into this important legislation.

1. The first issue relates to Section 1, Disclosure of breach of security, on page 1. The first paragraph appears to require banks to notify the affected customer bases of a security breach, *regardless of whether sensitive customer information has actually been accessed for unauthorized purposes*. Bankers are currently operating under interagency guidance that differs on this important point.

Section 501(b) of the GLBA required all banking regulators to publish uniform standards to assist banks in establishing safeguards to protect the security and confidentiality of customer information. These safeguards include protecting against unauthorized access to or use of customer information that could result in substantial harm to any customer.

These standards are issued in the form of interagency guidance that directs banks to complete a comprehensive risk assessment of the likelihood of and vulnerablility to unauthorized access to sensitive customer information, and to subsequently develop and implement a response program in the event of an apparent security breach.

The response program includes an immediate investigation to determine the likelihood that sensitive information has been or will be misused. If the bank determines through this process that such misuse has occurred or *it is reasonably possible that misuse will occur*, notification of affected customers is required as soon as possible.

The Alaska Bankers Association would like to see the language in this section changed to parallel the existing federal regulatory requirements.

Office of Thrift Supervision
Department of the Treasury *Managing Director, Examinations, Supervision, and Consumer Protection*
1700 G Street, N.W., Washington, DC 20552 • (202) 906-7984

December 14, 2005

MEMORANDUM FOR: **CHIEF EXECUTIVE OFFICERS**

FROM: Scott M. Albinson Scott M. Albinson

SUBJECT: Compliance Guide
Interagency Guidelines Establishing Information Security Standards

The Office of Thrift Supervision, together with the other Federal Banking Agencies (Agencies), jointly issued the *Interagency Guidelines Establishing Information Security Standards* (Security Guidelines), formerly known as the *Interagency Guidelines Establishing Standards for Safeguarding Customer Information.* The Security Guidelines primarily implement two statutes, Section 501(b) of the Gramm-Leach-Bliley Act, and Section 216 of the Fair and Accurate Credit Transactions Act of 2003.

The Security Guidelines establish standards for administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information, and the proper disposal of customer and consumer information. Under the Security Guidelines, each financial institution must develop and maintain an effective written information security program tailored to the complexity of its operations.

The Agencies are jointly issuing the attached Compliance Guide (Guide) as a resource to assist financial institutions in their efforts to comply with the Security Guidelines. The Guide summarizes a financial institution's obligations to protect customer information and to dispose properly of customer and consumer information. The Guide also has an Appendix, which lists resources that may be helpful in designing an information security program.

If you have questions about the Guide, contact Kathleen M. McNulty, Technology Program Manager, Information Technology Risk Management, at 202-906-6322, or kathleen.mcnulty@ots.treas.gov.

Attachment

CORRECTION

THE FOLLOWING DOCUMENT(S)
HAVE BEEN REFILMED TO
ASSURE LEGIBILITY OR PAGINATION

Lisa Corrigan is here to testify for the Alaska Bankers Association.
- Handouts for Committee

Senate Bill 222
Testimony before Senate Labor & Commerce Committee – 1/24/06

My name is Lisa Corrigan. I am the E.V.P. and Chief Operating Officer of Alaska Pacific Bank, a small community bank headquartered in Juneau. I also serve as President of the Alaska Bankers Association, which represents nine banks and includes state and federally chartered financial institutions.

Alaskan bankers share the concerns of the bill sponsors and are dedicated to protecting the privacy and security of sensitive customer information. My comments pertain to three points of clarification that bankers would like to see incorporated into this important legislation.

1. The first issue relates to Section 1, Disclosure of breach of security, on page 1. The first paragraph appears to require banks to notify the affected customer bases of a security breach, *regardless of whether sensitive customer information has actually been accessed for unauthorized purposes*. Bankers are currently operating under interagency guidance that differs on this important point.

Section 501(b) of the GLBA required all banking regulators to publish uniform standards to assist banks in establishing safeguards to protect the security and confidentiality of customer information. These safeguards include protecting against unauthorized access to or use of customer information that could result in substantial harm to any customer.

These standards are issued in the form of interagency guidance that directs banks to complete a comprehensive risk assessment of the likelihood of and vulnerablility to unauthorized access to sensitive customer information, and to subsequently develop and implement a response program in the event of an apparent security breach.

The response program includes an immediate investigation to determine the likelihood that sensitive information has been or will be misused. If the bank determines through this process that such misuse has occurred or *it is reasonably possible that misuse will occur*, notification of affected customers is required as soon as possible.

The Alaska Bankers Association would like to see the language in this section changed to parallel the existing federal regulatory requirements.

2. Our second suggestion is an amendment regarding delays in providing notice of a breach to affected persons, due to an ongoing investigation by law enforcement agencies. The intent is the same, but the new language protects investigations by an appropriate law enforcement agency. in addition to the Alaska Department of Law.

Page 2 line 7-12: After "Notification of Law Enforcement" delete all material through line 12.

Insert: "Notice of the breach may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the information collector with a written request for the delay. However, the information collector should notify the state resident as soon as notification will no longer interfere with the investigation."

3. Finally, under Article 4. Protection of Social Security Number, we are requesting a simple substitution of one word. Banks may be required to collect a social security number in order to properly identify a customer under the Patriot Act, yet may never be required to submit the social security number to the federal government, such as when a customer is not the primary signer on an account.

Page 15 line 30: Delete "submit"
Insert "obtain"

Thank you for the opportunity to provide testimony on Senate Bill 222 on behalf of the Alaska Bankers Association.

Lisa Corrigan
790-5104

Office of Thrift Supervision
Department of the Treasury *Managing Director, Examinations, Supervision, and Consumer Protection*
1700 G Street, N.W., Washington, DC 20552 • (202) 906-7984

December 14, 2005

MEMORANDUM FOR: **CHIEF EXECUTIVE OFFICERS**

FROM: Scott M. Albinson

SUBJECT: Compliance Guide
Interagency Guidelines Establishing Information Security Standards

The Office of Thrift Supervision, together with the other Federal Banking Agencies (Agencies), jointly issued the *Interagency Guidelines Establishing Information Security Standards* (Security Guidelines), formerly known as the *Interagency Guidelines Establishing Standards for Safeguarding Customer Information.* The Security Guidelines primarily implement two statutes, Section 501(b) of the Gramm-Leach-Bliley Act, and Section 216 of the Fair and Accurate Credit Transactions Act of 2003.

The Security Guidelines establish standards for administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information, and the proper disposal of customer and consumer information. Under the Security Guidelines, each financial institution must develop and maintain an effective written information security program tailored to the complexity of its operations.

The Agencies are jointly issuing the attached Compliance Guide (Guide) as a resource to assist financial institutions in their efforts to comply with the Security Guidelines. The Guide summarizes a financial institution's obligations to protect customer information and to dispose properly of customer and consumer information. The Guide also has an Appendix, which lists resources that may be helpful in designing an information security program.

If you have questions about the Guide, contact Kathleen M. McNulty, Technology Program Manager, Information Technology Risk Management, at 202-906-6322, or kathleen.mcnulty@ots.treas.gov.

Attachment

Interagency Guidelines Establishing Information Security Standards

Small-Entity Compliance Guide

I. INTRODUCTION

Purpose and Scope of the Guide

This Small-Entity Compliance Guide[1] is intended to help financial institutions[2] comply with the *Interagency Guidelines Establishing Information Security Standards* (Security Guidelines).[3] The guide summarizes the obligations of financial institutions to protect customer information and illustrates how certain provisions of the Security Guidelines apply to specific situations. The appendix lists resources that may be helpful in assessing risks and designing and implementing information security programs.

Although this guide was designed to help financial institutions identify and comply with the requirements of the Security Guidelines, it is not a substitute for the Security Guidelines. Moreover, this guide only addresses obligations of financial institutions under the Security Guidelines and does not address the applicability of any other federal or state laws or regulations that may pertain to policies or practices for protecting customer records and information.

Background and Overview of Security Guidelines

The Security Guidelines implement section 501(b) of the Gramm-Leach-Bliley Act (GLB Act)[4] and section 216 of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act).[5] The Security Guidelines establish standards relating to administrative, technical, and physical safeguards to ensure the security, confidentiality, integrity and the proper disposal of customer information.

---

[1] The guide is issued in accordance with the Small Business Regulatory Enforcement Fairness Act of 1996, Pub. L. No. 104-121, 110 Stat. 857, *reprinted in* 5 U.S.C.A. § 601, note (West Supp. 2004).

[2] This guide applies to the following types of financial institutions: National banks, Federal branches and Federal agencies of foreign banks and any subsidiaries of these entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers) (OCC); member banks (other than national banks), branches and agencies of foreign banks (other than Federal branches, Federal agencies, and insured State branches of foreign banks), commercial lending companies owned or controlled by foreign banks, Edge and Agreement Act Corporations, bank holding companies and their nonbank subsidiaries or affiliates (except brokers, dealers, persons providing insurance, investment companies, and investment advisers) (Board); state non-member banks, insured state branches of foreign banks, and any subsidiaries of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers) (FDIC); and insured savings associations and any subsidiaries of such savings associations (except brokers, dealers, persons providing insurance, investment companies, and investment advisers) (OTS).

[3] 66 Fed. Reg. 8616 (Feb. 1, 2001) and 69 Fed. Reg. 77610 (Dec. 28, 2004) promulgating and amending 12 C.F.R. Part 30, app. B (OCC); 12 C.F.R. Part 208, app. D-2 and Part 225, app. F (Board); 12 C.F.R. Part 364, app. B (FDIC); and 12 C.F.R. Part 570, app. B (OTS). Citations to the Security Guidelines in this guide omit references to part numbers and give only the appropriate paragraph number.

[4] 15 U.S.C. § 6801.

[5] 15 U.S.C. § 1681w.

that information. The Security Guidelines provide that financial institutions must contractually require their affiliated and non-affiliated third party service providers that have access to the financial institution's customer information to protect that information.

- The Privacy Rule limits a financial institution's disclosure of nonpublic personal information to unaffiliated third parties, such as by selling the information to unaffiliated third parties. Subject to certain exceptions, the Privacy Rule prohibits disclosure of a consumer's nonpublic personal information to a nonaffiliated third party unless certain notice requirements are met and the consumer does not elect to prevent, or "opt out of," the disclosure.[9] The Privacy Rule requires that privacy notices provided to customers and consumers describe the financial institution's policies and practices to protect the confidentiality and security of that information. It does not impose any other obligations with respect to safeguarding customers' or consumers' information.

II. IMPORTANT TERMS USED IN THE SECURITY GUIDELINES

Customer Information

The Security Guidelines require financial institutions to safeguard and properly dispose of customer information. Customer information is any record containing nonpublic personal information about an individual who has obtained a financial product or service from the institution that is to be used primarily for personal, family, or household purposes and who has an ongoing relationship with the institution.

Customer Information Systems

Customer information systems means any method used to access, collect, store, use, transmit, protect, or dispose of customer information. ¶ I.C.2 of the Security Guidelines. Customer information systems encompass all the physical facilities and electronic facilities a financial institution uses to access, collect, store, use, transmit, protect, or dispose of customer information. The Security Guidelines apply specifically to customer information systems because customer information will be at risk if one or more of the components of these systems are compromised.

Information Security Program

An *information security program* is the written plan created and implemented by a financial institution to identify and control risks to customer information and customer information systems and to properly dispose of customer information. The plan includes policies and procedures regarding the institution's risk assessment, controls, testing, service-provider oversight, periodic review and updating, and reporting to its board of directors.

---

[9] The Privacy Rule defines a "consumer" to mean an individual who obtains or has obtained a financial product or service that is to be used primarily for personal, family, or household purposes. For example, an individual who applies to a financial institution for credit for personal purposes is a consumer of a financial service, regardless of whether the credit is extended. Privacy Rule § __.3(e).

- Assessing the likelihood and potential damage of identified threats, taking into consideration the sensitivity of the customer information;

- Assessing the sufficiency of the policies, procedures, customer information systems, and other arrangements in place to control the identified risks; and

- Applying each of the foregoing steps in connection with the disposal of customer information.

Identifying Reasonably Foreseeable Internal and External Threats

A risk assessment must be sufficient in scope to identify the reasonably foreseeable threats from within and outside a financial institution's operations that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems, as well as the reasonably foreseeable threats due to the disposal of customer information. The scale and complexity of its operations and the scope and nature of an institution's activities will affect the nature of the threats an institution will face.

For example, a financial institution should review the structure of its computer network to determine how its computers are accessible from outside the institution. If the computer systems are connected to the Internet or any outside party, an institution's assessment should address the reasonably foreseeable threats posed by that connectivity.

The risk assessment also should address the reasonably foreseeable risks to:

- Customer information stored on systems owned or managed by service providers, and

- Customer information disposed of by the institution's service providers.

Assessing the Likelihood and Potential Damage of Identified Threats

In addition to identifying reasonably foreseeable threats to customer information, customer information systems, and customer information that a financial institution disposes of, a risk assessment must evaluate the potential damage from these threats. The Security Guidelines allow latitude to determine the sensitivity of customer information in the course of assessing the likelihood of and potential damage from the identified threats.

For example, to determine the sensitivity of customer information, an institution could develop a framework that analyzes the relative value of this information to its customers based on whether improper access to or loss of the information would result in harm or inconvenience to them.

In the course of assessing the potential threats identified, an institution should consider its ability to identify unauthorized changes to customer records. In addition, it should take into consideration its ability to reconstruct the records from duplicate records or backup information systems.

Risk assessment is an ongoing process. Financial institutions should continually review their current policies and procedures to make certain they are adequate to safeguard customer information and customer information systems. The review of policies and procedures should also ensure the proper disposal of customer information. Financial institutions should also include their review and findings in their written information security program. The institution must also update the risk assessment, as necessary, to account for system changes before they are implemented, or new products or services before they are offered.

IV. DESIGNING SECURITY CONTROLS

The Security Guidelines require a financial institution to design an information security program to control the risks identified through its assessment, commensurate with the sensitivity of the information and the complexity and scope of its activities. Thus, an institution must consider a variety of policies, procedures, and technical controls and adopt those measures that it determines appropriately address the identified risks.

The Security Guidelines provide a list of measures that an institution must consider and, if appropriate, adopt. These are:

- Access controls on customer information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing customer information to unauthorized individuals who may seek to obtain this information through fraudulent means;

- Access restrictions at physical locations containing customer information, such as buildings, computer facilities, and records storage facilities to permit access only to authorized individuals;

- Encryption of electronic customer information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access;

- Procedures designed to ensure that customer information system modifications are consistent with the institution's information security program;

- Dual control procedures, segregation of duties, and employee background checks for employees with responsibilities for or access to customer information;

- Monitoring systems and procedures to detect actual and attempted attacks on or intrusions into customer information systems;

- Response programs that specify actions to be taken when the institution suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies; and

In addition to considering the measures required by the Security Guidelines, each institution may need to implement additional procedures or controls specific to the nature of its operations. An institution may implement safeguards designed to provide the same level of protection to all customer information, provided that the level is appropriate for the most sensitive classes of information.

Insurance coverage is not a substitute for an information security program. Although insurance may protect an institution or its customers against certain losses associated with unauthorized disclosure, misuse, alteration, or destruction of customer information, the Security Guidelines require a financial institution to implement and maintain controls designed to prevent those acts from occurring.

Develop and Implement A Response Program

The Agencies have issued an interpretation of the Security Guidelines regarding programs to respond to unauthorized access to customer information, the *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice* (Incident Response Guidance).[13] According to the Incident Response Guidance a financial institution should develop and implement a response program as part of its information security program. The response program should address unauthorized access to or use of customer information that could result in substantial harm or inconvenience to a customer.

The components of an effective response program include:

- Assessment of the nature and scope of the incident and identification of what customer information has been accessed or misused;
- Prompt notification to its primary federal regulator once the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information;
- Notification to appropriate law enforcement authorities, in addition to filing a timely Suspicious Activity Report, in situations involving Federal criminal violations requiring immediate attention;
- Measures to contain and control the incident to prevent further unauthorized access to or misuse of customer information, while preserving records and other evidence; and
- Notification to customers when warranted.

[13] 70 Fed. Reg. 15736 (Mar. 29, 2005) promulgating 12 C.F.R. Part 30, app. B, Supplement A (OCC); 12 C.F.R. Part 208, app. D-2, Supplement A and Part 225, app. F, Supplement A (Board); 12 C.F.R. Part 364, app. B, Supplement A (FDIC); and 12 C.F.R. Part 570, app. B, Supplement A (OTS).

- Provide staff members responsible for building or maintaining computer systems and local and wide-area networks with adequate training, including instruction about computer security; and

- Train staff to properly dispose of customer information.

VI. TESTING KEY CONTROLS

The Security Guidelines require a financial institution to test the key controls, systems, and procedures of its information security program. ¶ III.C.3 of the Security Guidelines. The institution's risk assessment should determine the scope, sequence, and frequency of testing.

The Agencies expect an institution or its consultant to regularly test key controls at a frequency that takes into account the rapid evolution of threats to computer security. Testing may vary over time depending, in part, on the adequacy of any improvements an institution implements to prevent access after detecting an intrusion. Independent third parties or staff members, other than those who develop or maintain the institution's security programs, must perform or review the testing.

VII. OVERSEEING SERVICE PROVIDERS

The Security Guidelines set forth specific requirements that apply to a financial institution's arrangements with service providers. An institution must:

- Exercise appropriate due diligence in selecting its service providers;

- Require its service providers by contract to implement appropriate measures designed to meet the objectives of the Security Guidelines; and

- Where indicated by its risk assessment, monitor its service providers to confirm that they have satisfied their obligations under the contract described above.

As stated in section II of this guide, a service provider is *any* party that is permitted access to a financial institution's customer information through the provision of services directly to the institution. Examples of service providers include a person or corporation that tests computer systems or processes customers' transactions on the institution's behalf, document-shredding firms, transactional Internet banking service providers, and computer network management firms.

institution a copy. Where this is the case, an institution should make sure that the information is sufficient for it to conduct an accurate review, that all material deficiencies have been or are being corrected, and that the reports or test results are timely and relevant.

The institution should include reviews of its service providers in its written information security program.

VIII. ADJUSTING THE PROGRAM

A financial institution should adjust its information security program to reflect the results of its ongoing risk assessment and the key controls necessary to safeguard customer information and ensure the proper disposal of customer information. It should adjust the program to take into account changes in technology, the sensitivity of its customer information, internal or external threats to information, and the institution's own changing business arrangement such as mergers, acquisitions, alliances and joint ventures, outsourcing arrangements, and changes in customer information systems.

For example, the institution should ensure that its policies and procedures regarding the disposal of customer information are adequate if it decides to close or relocate offices. A change in business arrangements may involve disposal of a larger volume of records than in the normal course of business.

IX. RESPONSIBILITIES OF AND REPORTS TO THE BOARD OF DIRECTORS

Under the Security Guidelines, a financial institution's board of directors, or an appropriate committee of the board, must satisfy specific requirements designed to ensure that the institution's information security program is developed, implemented, and maintained under the supervision of those who are ultimately responsible. At the outset, the board, or appropriate committee, must approve the written information security program. Thereafter, the board or appropriate committee must oversee the implementation and maintenance of the program. These duties include assigning specific responsibility for implementing the program and reviewing management reports. ¶ III.A of the Security Guidelines.

Correspondingly, management must provide a report to the board, or an appropriate committee, at least annually that describes the overall status of the information security program and compliance with the Security Guidelines. The report should describe material matters relating to the program.

For example, whether an institution conducts its own risk assessment or hires another person to conduct it, management should report the results of that assessment to the board or an appropriate committee.

The Security Guidelines provide an illustrative list of other material matters that may be appropriate to include in the report, such as decisions about risk management and control, arrangements with service providers, results of testing, security breaches or violations and

APPENDIX

Note: This list of resources is intended to further assist financial institutions in complying with the *Interagency Guidelines Establishing Information Security Standards*. The listed organizations provide information on computer security, with a focus on risk-assessment methodologies and the design and implementation of computer security programs. Any mention of a commercial product is for information purposes only and does not imply a recommendation or endorsement by the Agencies.

Center for Internet Security (CIS) – A nonprofit cooperative enterprise that helps organizations reduce the risk of business and e-commerce disruptions resulting from inadequate security configurations. CIS develops security benchmarks through a global consensus process. Its members include the American Institute of Certified Public Accountants (AICPA), Financial Management Service of the U.S. Department of the Treasury, and Institute for Security Technology Studies (Dartmouth College). www.cisecurity.org

CERT Coordination Center – A center for Internet security expertise operated by Carnegie Mellon University. CERT provides security-incident reports, vulnerability reports, security-evaluation tools, security modules, and information on business continuity planning, intrusion detection, and network security. It also offers training programs at Carnegie Mellon. CERT has developed an approach for self-directed evaluations of information security risk called Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE). www.cert.org/octave/

Information Systems Audit and Control Association (ISACA) – An association that develops IT auditing and control standards and administers the Certified Information Systems Auditor (CISA) designation. ISACA developed Control Objectives for Information and Related Technology (COBIT) as a standard for IT security and control practices that provides a reference framework for management, users, and IT audit, control, and security practitioners. www.isaca.org/cobit.htm

International Organization for Standardization (ISO) – A network of national standards institutes from 140 countries. Published *ISO/IEC 17799:2000, Code of Practice for Information Security Management*. :www.iso.org. Interested parties should also review the *Common Criteria for Information Technology Security Evaluation.* http://niap.nist.gov/cc-scheme/index.html

Internet Security Alliance (ISA) – A collaborative effort between Carnegie Mellon University's Software Engineering Institute, the university's CERT Coordination Center, and the Electronic Industries Alliance (a federation of trade associations). ISA provides access to information on threats and vulnerability, industry best practices, and developments in Internet security policy. www.isalliance.org

FISCAL NOTE

STATE OF ALASKA
2006 LEGISLATIVE SESSION

Fiscal Note Number:
Bill Version: SB222-DPS-AST-1-23-06
() Publish Date:

Revision Date/Time (Note if correction):
Dept. Affected: Public Safety

Title: An Act relating to breaches of security involving personal information, consumer report security...
RDU: Alaska State Troopers
Component: AST Detachments

Sponsor: Senator Therriault
Requester: Senate Labor and Commerce Committee
Component No.: 2325

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	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**
CAPITAL EXPENDITURES						
CHANGE IN REVENUES ( )						

FUND SOURCE (Thousands of Dollars)

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

Estimate of any current year (FY2006) cost: 0.0
Mark this box (X) if funding for this bill is included in the Governor's FY 2006 budget proposal:

POSITIONS

Full-time						
Part-time						
Temporary						

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

Passage of this legislation will have no fiscal impact as it would be absorbed by the current assets of the Department of Public Safety.

Prepared by: Lieutenant James Helgoe
Phone 907-269-4532
Division: Alaska State Troopers
Date/Time 1/23/06 1:54 PM

Approved by: Commissioner William Tandeske
Date 1/23/2006
Agency: Department of Public Safety

(Revised 9/23/2004 OMB)

FISCAL NOTE

STATE OF ALASKA
2006 LEGISLATIVE SESSION

Fiscal Note Number:
Bill Version: **SB222-DOLWD-CO-01-23-05**
() Publish Date:

Revision Date/Time (Note if correction):
Title: **Protection of Personal Information**

Department: **Labor and Workforce Development**
RDU: **Office of the Commissioner**
Component: **Commissioner's Office**

Sponsor: **Senators Therriault, Guess**
Requester: **Senate L&C**

Component Number: **340**

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: None
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)*

See Attached

Prepared by: **Guy Bell, Assistant Commissioner** Phone: **465-2700**
Division: **Commissioner's Office** Date/Time: **1/23/06 4:00 PM**
Approved by: **Greg O'Claray, Commissioner** Date: **1/23/2006**
Agency: **Department of Labor and Workforce Development**

(Revised 9/7/2005 OMB)

ANALYSIS: (continued)

* The costs of complying with the notification provisions of this legislation are dependant on whether and where a security breach occurs and cannot be determined at this time.

The Administrative Services Division, Labor Market Information component has two data files, one with 50,000 records and one with over 600,000 and estimates the costs could vary from minimal to as much as $26.0 depending on which of two data files was breached.

The Workers' Compensation Division receives documents with confidential personal information pertaining to approximately 30,000 individuals each year and depending on the scope of the breach costs could be as much as $100.0.

The Labor Standards & Safety Division receives thousands of documents with confidential personal information each year and depending on the scope of the breach costs could be as much as $130.0.

The Employment Security Division system has in excess of 500,000 records containing confidential personal information, a breach of the system would be addressed through posting on the internet website at minimal cost to the department.

The Business Partnerships Division has 46,000 records with confidential personal information and receives approximately 6,000 additional records each year. Depending on the scope of the security breach costs could be in excess of $60.0.

The Alaska Vocational Technical Center has approximately 50,000 records with confidential personal information and receives approximately 1,500 additional records each year. Depending on the scope of the security breach costs could be in excess of $60.0.

STATE OF ALASKA

OFFICE OF THE GOVERNOR

BILL ANALYSIS

DEPARTMENT	DIVISION	BILL NUMBER	SPONSOR
Health & Social Services	Finance and Managment Services	SB 222	THERRIAULT

SHORT TITLE OF BILL
SECURITY INVOLVING PERSONAL INFORMATION

DEPARTMENT POSITION
Neutral

PREPARED BY	DATE	COMMISSIONER'S SIGNATURE	DATE
Janet Clarke, Asst. Comm.	01/18/2006	Karleen Jackson	01/24/2006

SUMMARY

OTHER AGENCIES AFFECTED BY BILL	CONSTITUENT GROUP(S) AFFECTED BY BILL
ORGANIZATIONAL SUPPORT FOR BILL	**ORGANIZATIONAL OPPOSITION TO BILL**

FISCAL IMPACT ☐ NONE ☐ FISCAL NOTE ATTACHED

BACKGROUND/LEGISLATIVE INTENT

Disclosure of breach of security involving personal information.

ANALYSIS OF BILL/PROGRAM EFFECTS

Article 1 – Breach of Security Involving Personal Information

The Department is a "person" for purposes of this proposed chapter. See proposed AS 45.48.900(4).

Under Article 1 of the proposed legislation, the Department:

(a) Will be required to disclose breaches of security of its information systems containing personal information to each state resident whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person;

AMENDMENTS PROPOSED

The cost of private causes of action is unknown. Monetary liability would follow for "damages suffered by the individual" for failure to provide notice. Thus, there is exposure only if the Department does not notify individuals of breaches. But, if there is such a failure, the scope and kind of damages are undefined. Even absent proof of financial damage, an individual could argue that they suffered emotionally from the failure to notify. While such claims would not likely be successful absent physical injury, it is recommended that damages be limited to financial damages suffered as a result of the failure to notify.

PLEASE ATTACH A SEPARATE SHEET FOR ADDITIONAL COMMENTS OR ANALYSIS

STATE OF ALASKA **BILL NO. SB 222**
2006 LEGISLATIVE SESSION
ANALYSIS CONTINUATION

ANALYSIS OF BILL/PROGRAM EFFECTS

(b) Must, with some exception if a Department of Law investigation is occurring, notify promptly such impacted individuals by written document or permissible electronic means. Class notice would be permitted if the cost of individual notice exceeds $250,000, the class of persons exceeds 500,000 people, or the Department does not have sufficient contact information to provide individual notice; and

(c) Will be subject to lawsuit and damages suffered by a state resident for a breach.

Personal information is defined as a combination of the individual's first initial or first name, last name, and his or her social security number, driver's license or state identification number, or numbers of the individual's financial accounts and access codes to the accounts. See proposed AS 45.48.090(3). A "breach of security" is defined as the "unauthorized acquisition of information that compromises the security, confidentiality, or integrity of personal information maintained by the information collector." See proposed AS 45.48.090(1).

The Department maintains many information databases that contain names and other identifying features, such as social security numbers. The Department has and will likely be subject to future attempts to breach its security systems. Based on past incidents, it is likely the Department will not be able to tell whose personal information was accessed; although it will be able to reasonably conclude that some information may have been accessed. This would require notice to a large class of individuals. Individual notice will be required, unless the exceptions identified at AS 45.48.020 - 45.48.040 are implicated.

The legislation does not require notice if the personal information was encrypted. Based on our HIPAA security compliance efforts, encryption of Electronic Protected Health Information is recommended only during transmission of data (not for its storage). The costs of encryption software for transmission have not yet been determined. If it is the Department's intent to avoid exposure entirely under this statute, we would need to determine the costs for encryption of stored data. It also should be remembered that information system is not a defined term and some may argue for a broad interpretation of the term.

This legislation can have a fiscal impact upon the Department for costs of notice, for requiring encryption of all personal information, the investment of storage devices to support the storage of all server access log information, the investment in software products to support the review of server access system logs, to conduct security assessments through contract engagement with a third party security firm, the investment in security assessment tools to be used to conduct security assessments on a scheduled basis, the training of 1-2 network services staff on network security procedures and for damages for failing to notify individuals of breaches of security.

STATE OF ALASKA **BILL NO. SB 222**
2006 LEGISLATIVE SESSION
ANALYSIS CONTINUATION

ANALYSIS OF BILL/PROGRAM EFFECTS

Article 2 -- Consumer Report Security Freeze

The Department is not a consumer reporting agency for purposes of this Article. However, Article 2 will impact the ability of the Department to receive information regarding an individual from a consumer reporting agency, absent consumer consent, if a consumer report security freeze is in place. Disclosures to Department are still permissible when the Department is investigating fraud. AS 45.48.220(5). Disclosures are also permissible for prescreening allowed under the federal Fair Credit Reporting Act. AS 45.48.220(7).

Article 3 -- Consumer Credit Monitoring; Credit Accuracy is not applicable to the Department.

Article 4 -- Protection of Social Security Number

Article 4 restricts persons, including the Department, from.

(a) Intentionally communicating or otherwise making available to the general public an individual's social security number;

(b) Printing an individual's social security number on a card required to access products or services;

(c) Requiring an individual from transmitting his or her social security number over the internet, unless the site is secure or the number is encrypted;

(d) Requiring an individual to use his or her social security number to access an internet site, unless a password, unique identification number, or another authentication device is required for access;

(e) Printing the social security number on materials mailed to the individual, unless state or federal law requires such printing;

(f) Refusing to do business with an individual who refuses to disclose his or her social security number, unless the Department is expressly required to submit the individualÃ?Â¢??s social security number to the federal government; or

(g) Selling, leasing, loaning, trading, renting or disclosing an individual's social security number to a third party for any purpose without the individual's written consent.

ANALYSIS OF BILL/PROGRAM EFFECTS

Article 4 contains thoughtful restrictions on the use and disclosure of social security numbers. The concern is the proposed AS 45.48.400(b), which would restrict the Department from disclosing an individual's social security number to a third party for any purpose without an individual's written consent. The section would restrict disclosures of documents that contain a social security number to third parties that have a legitimate need to receive the document. This would include third party payers of health care, other health care providers, law enforcement, and the Department of Law. This restriction could result in large administrative costs, e.g., reviewing and redacting all documents that contain the social security number.

Article 5 – Disposal of Records

Article 5 addresses the disposal of records containing personal information. The restrictions of this section are no greater than the restrictions required by HIPAA. However, individual suit is permitted for violation of the requirements of this section. See proposed AS 45.48.550. HIPAA does not permit private causes of action, but rather leaves enforcement through civil and criminal penalty to the Office for Civil Rights. There is, however, a question of whether the Department is a "business" subject to the requirements of Article 5. See proposed definition of business at AS 45.48.500(1). It is recommended that the Department should seek clarification of whether it qualifies as a "business" for purposes of this proposed article.

Article 6 – Factual Declaration of Innocence after Identity Thef

Article 6 is not applicable to the Department.

Article 7 – Consumer Credit Header Information

Article 7 is not directly applicable to the Department. It does potentially restrict the ability of the Department to receive consumer credit header information.

AMENDMENTS PROPOSED

Information system is not a defined term. "Damages" is also not a defined term. Some may argue it includes emotional distress damages.

Article 4 -- Protection of Social Security Number

A potential fix is to provide that these disclosures are permissible when the recipient third party has a legitimate business reason for receiving the document on which the social security number is contained and promises not to wrongfully use or disclose the number.

Consumers Union

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

April 1, 2005

The Honorable Gretchen Guess
Alaska State Senate
State Capitol, Room 423
Juneau, AK 99801-1182
907-465-2435 (fax)

Re: Support for SB 149, Breaches of Security and Security Freeze for Credit Reports

Dear Senator Guess:

Consumers Union, the independent, nonprofit publisher of *Consumer Reports*, supports SB 149, relating to Breaches of Security and Security Freeze for Credit Reports. A security freeze is a key tool to prevent identity thieves from getting credit in the consumer's name, by allowing consumers to lock up, or "freeze" access to their consumer credit files for credit granting purposes. A requirement to notify consumers of a breach of security will enable consumers to take preventative steps, including placing a security freeze, at a time when they may be able to head off an identity thief before the consumer experiences ruined credit and other harmful consequences of ID theft.

Security freeze

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

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

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

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

Federal law is inadequate to prevent identity theft

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

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

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

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

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

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

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

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

Notice of security breach

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

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

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

Very truly yours,

Gail Hillebrand

Gail Hillebrand

Consumers Union

Publisher of Consumer Reports

Freeze Identity Thieves Out of Consumers' Credit Files:

Support State Credit Report Security Freeze Laws

Credit card companies, merchants, credit bureaus and other businesses do not adequately safeguard consumers' private financial information, making it relatively easy for thieves to steal this data and use it to take out new credit or to rack up charges on existing accounts. As a result, identity theft is one of the fastest growing financial crimes. Nearly 10 million Americans fall victim each year, and the Identity Theft Resource Center reports that victims spend an average of $1,495 and 500 hours to restore their credit histories and their good names. Identity theft also costs U.S. businesses nearly $48 billion annually.

Consumers need additional tools to help prevent identity theft before it happens. Many states are considering legislation that would allow people to lock identity thieves out of their credit files with a security freeze. With a security freeze in place, a consumer's credit report and credit score cannot be shared with any potential creditors unless the consumer decides to unlock the files by contacting the credit bureaus and providing a security code.

A security freeze can help prevent identity theft. Most businesses will not issue new credit or loans to an individual without first reviewing his or her credit report or credit score. If an individual's credit file is frozen and an imposter applies for credit in that individual's name, a creditor likely would deny the imposter's application, preventing an instance of identity theft. In addition, if a request for credit is made on a frozen account, then the credit bureau would be required to notify the consumer about the attempted fraud.

Under a state security freeze law, people who choose to freeze access to their credit report may temporarily lift the freeze for new loans and credit they apply for themselves. When a consumer initially activates the freeze, the credit bureau will issue a unique PIN to the consumer that can be used to "thaw" or lift the security freeze for a particular creditor. Credit bureaus must release the report within three business days of such a request, and are permitted and encouraged to develop faster methods of releasing credit reports on request of the consumer. In addition, existing creditors will continue to have access to an individual's credit report.

State security freeze laws would give consumers the right to decide for themselves whether or not to place a security freeze on their reports.

Frequently Asked Questions

How is a security freeze different from fraud alerts or blocking of information generated by a thief?

A security freeze is a mechanism to prevent identity theft. Only a security freeze allows the consumer to control who has access to his or her credit file. The federal Fair Credit Reporting Act allows identity theft victims to block the reporting of specific information in their credit reports that is the result of identity theft. But fraud blocking is a way to begin to undo damage after it has been done. Fraud blocking does not prevent identity theft. Fraud blocking does not prevent the release of a credit report; it only limits certain fraud-related information from being included in the report after the consumer discovers that information. Similarly, a fraud alert does not prevent a credit report from being issued. Under the federal Fair Credit Reporting Act, when a fraud alert is attached to a credit file, creditors must take additional steps to verify a credit applicant's identity before extending credit. The fraud alert, however, does not prevent the potential creditor from seeing the report, and it does not prevent the credit bureau from selling or sharing the credit report.

A security freeze grants each consumer the right to prevent the credit bureau from issuing his or her credit report for the purpose of issuing new credit. It freezes access to the report except for circumstances such as review of existing accounts, other limited purposes, or the express permission of the consumer.

Would anyone have access to a consumer's credit file if it is frozen?

Yes, these proposed state bills include a few necessary exemptions to the freeze. Security freezes would not apply to any person or entity with which consumers have existing accounts, nor to a limited number of other parties who may access the files for purposes not related to issuing credit, such as law enforcement agencies and certain governmental agencies that need them for investigations and other statutory responsibilities.

Do states have the right to enact security freeze legislation under federal law?

A state law establishing a security freeze right should not be preempted by the federal Fair Credit Reporting Act. No provision of federal law preempts the ability of a state to restrict when a credit reporting agency allows access to a credit report. Federal law addresses the contents of credit files, not who can see them. Federal law also requires credit bureaus, upon the request of a consumer to: (1) put a fraud alert into the consumer's file to warn potential users of the report that new credit should not be extended without first verifying the identity of the credit applicant, and (2) block the reporting of any information in a consumer's file that the consumer identifies as information resulting from an identity theft. States are preempted from imposing requirements regarding the same conduct required by certain specific provisions of federal law, such as these provisions. States are not preempted from other steps to prevent or mitigate identity theft. States should be free to enact security freeze legislation.

Which states already have security freezes?

California, Louisiana, Texas, and Vermont have security freeze laws, the Texas and Vermont statutes are limited to victims of identity theft. The California and Louisiana laws allow consumers who have not been victims of identity theft to control who gets access to their credit files for credit granting purposes.

G \Groups\Credit & Finance\Gail\Wallet\2005\Security Freeze Factsheetwlogo doc

IDENTITY THEFT FACT SHEET

Source: FTC's NCPW 2005 Quiz – Identity Theft: When Fact Becomes Fiction

1. ID theft is the fastest growing white-collar crime in the U.S. 27 million Americans have been victims of the crime in the past five years, nearly 10 million people last year.
2. Identity thieves can get personal information from you by:
   - Stealing your wallet or purse
   - Stealing your mail
   - Rummaging through your trash, and
   - Using personal information they find on the Internet about you

   For additional information on how ID thieves can steal your identity, go to: www.consumer.gov/idtheft/understanding_idt.html#2
3. If you are getting rid of your computer, it is not enough to delete files using mouse and keyboard commands. Use a "wipe" utility program to overwrite the entire hard drive. This makes files unrecoverable.
4. ID thieves that obtain your personal information can: (1) call your credit card issuer and change the mailing address on your card, (b) open a new credit card account or bank account in your name, (c) file for bankruptcy under your name to avoid paying off debts they've incurred, and (d) counterfeit checks or drain your bank account.
5. Here are some ways for you to minimize your risk of becoming a victim of ID theft.:
   - Don't give out personal information by email, Internet, phone or mail unless you initiated contact and you are certain you know who you are dealing with
   - Don't carry your social security card with you
   - Carry only the identification information and credit/debit cards that you actually need
   - Password protect your credit card, bank and phone accounts.
   - For additional tips, go to: www.consumer.gov/idtheft/protect_againstidt.html#5
6. If you are a victim of ID theft, place a fraud alert on your credit report. This will help prevent if thieves from opening additional accounts in your name.
7. If you think someone has stolen your personal information or identification, do the following:
   - Immediately close all your credit card or bank accounts
   - Place a fraud alert with any one of the three national consumer reporting companies
   - Contact the Social Security Administration to get a new Social Security number
   - Alert issuing agencies for your driver's license and other identification documents
8. If you have high speed Internet connection, such as DSL or cable modem, get a firewall program to prevent uninvited guests from accessing your computer.
9. Signs you could be a victim of ID theft:
   - Fail to receive bills or other mail
   - Receive credit cards for which you did not apply
   - Are denied credit for no apparent reason
   - Get calls or letters from debt collectors or businesses about merchandise or services you didn't buy
10. Don't tape computer and website passwords to your computer. Safeguard these passwords. Also, when creating passwords, use a combination of letters (upper and lower case), numbers and symbols.

The Mercury News
MercuryNews.com

Local News

Posted on Wed, Apr. 13, 2005

Credit freeze can halt ID theft

RELATED LINKS
- How to freeze your credit

VICTIMS MAY LIMIT CROOKS' USE OF DATA

By Matthai Chakko Kuruvila
Mercury News

The revelation Tuesday that as many as 310,000 people may have had their personal information stolen from a LexisNexis database underscores how vulnerable consumers are to identity theft.

But what can you do if you're the victim of such hacks?

If you're a Californian, you can freeze your credit so crooks can't open new accounts in your name. While that provides peace of mind, it also comes with some costs. Anytime consumers want to sign up for a new cell phone, get a new credit card or engage in a number of activities involving a credit check, they have to "unfreeze" their credit.

You won't be able to do that at the register. The process of "thawing" your credit can take up to three days -- and $10 for each period of time you want it unsealed.

"It's a balance," said Gail Hillebrand, senior attorney for San Francisco-based Consumers Union, which is lobbying other states to adopt California's credit-freeze laws. "It's a little bit of inconvenience when you want access to your credit file, but it's a lot of protection."

The freeze law went into effect Jan. 1, 2004. It's different than a fraud alert, which also is filed with credit bureaus but only suggests to creditors that they take additional steps to verify someone's identity.

For some, the security freeze is well worth the hassle.

'Call it insurance'

After being notified three years ago by a credit card company that someone had tried to obtain a card in her name, Barbara Haviluk didn't want to take any further risks. She froze all her credit reports after the law went into effect.

"Just call it insurance," said Haviluk, 61, a Carlsbad resident. "Until I completely froze my credit, it was unnerving that somebody out there had my information."

Also Tuesday, a General Motors spokeswoman confirmed that GM MasterCard cardholders had been notified their data may have been exposed when a national retailer suffered a security breach.

The latest news follows disclosures last week by the San Jose Medical Group that computers containing the medical records of 185,000 current and former patients were stolen in March.

Despite the recent incidents, credit bureaus and bankers aren't sure a freeze is worth the trouble.

"I think consumers have gotten very used to the convenience of credit," said Anissa Yates, vice president for the California Bankers Association. "It would take something like freezing their credit file to make them aware of the many ways credit touches their daily life."

A credit freeze means no more instant credit card discounts at the department store, nor quick financing at a car dealership.

Hillebrand and other consumer advocates say it's a small price to pay considering the alternative. If you're the victim of identity theft and a criminal signs up for multiple credit cards in your name, the process of protecting yourself is laborious.

Steps to take

You must file a police report, fill out an affidavit with the Federal Trade Commission and contact each of the three credit bureaus that keep your data.

In addition, you'll also have to contact each department store or credit card company that authorized the card or loan and make sure they're not re-reporting the fraudulent, but unpaid, charges to your name.

A California security freeze doesn't "protect you from the initial theft, but it protects you from many of the adverse effects of that theft," Hillebrand said.

Those thefts seem to be growing by the day. LexisNexis' parent company, Reed Elsevier, revealed Tuesday that there were 59 incidents over the past two years where thieves used the passwords of legitimate users to look at Social Security numbers, driver's license numbers and other information.

The company plans to personally contact each person whose information was exposed and offer free credit reports, credit monitoring for one year and fraud insurance.

But of the first 30,000 LexisNexis potential victims notified in March, only 2 percent had contacted the company to accept their offer of free credit reports and credit monitoring, according to LexisNexis.

In February, Bank of America lost computer data tapes containing personal information -- including Social Security numbers -- on 1.2 million federal employees.

Georgia-based ChoicePoint also disclosed in February that a security breach may have compromised the data of 145,000 people nationally.

Feinstein bill

The rash of breaches and proposed legislation by Sen. Dianne Feinstein, D-Calif., has prompted a Senate judiciary hearing today. Feinstein's bill would require that companies nationwide notify possible victims of privacy breaches -- something that is currently only required in California.

The state's "security freeze" also is unique to California, although a similar option will be available in Louisiana beginning July 1. Texas also permits security freezes, although it is only available to victims of identity theft.

Freeze legislation is now pending in 19 states, according to Consumers Union.

Contact Matthai Chakko Kuruvila at mkuruvila@mercurynews.com or (408) 920-2722.

adn.com
Anchorage Daily News

Identity thieves may have hit Alaska

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

By RICHARD RICHTMYER
Anchorage Daily News

(Published: February 24, 2005)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Identity crisis?

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

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

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

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

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

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

Print Page | Close Window

LexisNexis acknowledges more ID theft

Personal info on 310,000 people possibly stolen, 10 times more than what was disclosed last month.

April 12, 2005: 4:49 PM EDT
By Caleb Silver, CNN Business News Producer

NEW YORK (CNN) - LexisNexis, which compiles and sells personal and financial data on U.S. consumers, said Tuesday that personal information on 310,000 people nationwide may have been stolen.

That number is nearly 10 times higher than the figure LexisNexis disclosed last month when it first reported that its databases had been breached.

LexisNexis said in March that 32,000 people had been potentially affected by the breaches.

In a press release on its Web site, the company said it will notify an additional 278,000 individuals whose data may have been stolen, adding that it is working with law enforcement authorities to see if any of the stolen data has been misused.

Letters will be sent this week to people who may have been affected by the security breach. To date, none of the individuals who were notified that some of their information was accessed last month have experienced any form of identity theft, according to the company.

The firm's Anglo-Dutch parent Reed Elsevier said the identity thefts relate to the misappropriation of IDs and passwords from customers of its Seisint division, which provides information on consumers to third parties like collections companies and federal agencies.

Today's disclosure comes just after an investigation by Reed Elsevier determined that its databases had

Related stories

- Fund clients vulnerable to ID theft?
- ID theft: The real risk
- Damage control for identity theft
- ChoicePoint: More ID theft warnings

Video — More video

LexisNexis is acknowledging that personal information on 310,000 people may have been stolen. CNN's Daniel Sieberg reports.
Play video

Top Stories

Investors too eager?
Markets fly post-Fed
Superfast downloaders sued
Mission: Security
Ventas to buy Provident for $1.2 billion

— powered by —

YOUR E-MAIL ALERTS

Identity Theft
LexisNexis
Activate or CREATE YOUR OWN
Manage alerts | What is this

been fraudulently breached 59 times using stolen passwords.

The thieves, who obtained information including addresses and Social Security numbers, did not hack into the computer system and although they were able to get ahold of sensitive password information, the company says it is not certain how the passwords were acquired.

ChoicePoint (down $0.02 to $38.96, Research), an information clearinghouse similar to Seisint, was a victim of a similar scheme earlier in the year. Thieves posed as real estate agents and the company then gave them access to personal information in its database.

How safe is your computer? Click here to find out.

If you think you are a victim, click here.

NewsNight with Aaron Brown (10 p.m. ET): Find out how to protect yourself from scams to steal your identity.

The Hot List

Tax-friendly places '05

5 island hideaways off the beaten path

In King Bruce's mines at Lazard

More Personal Tech

Apple's Tiger software out April 29

HP unveils iPod models

LexisNexis acknowledges more ID theft

contact us | magazine customer service | site map | glossary | RSS | press room

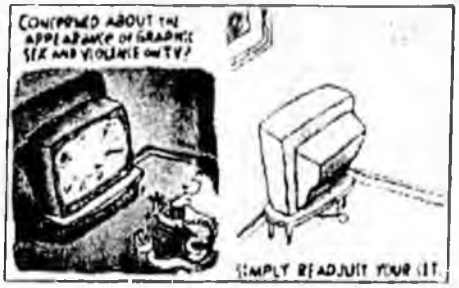
OTHER NEWS: CNN | SI | Fortune | Business2.0

= Money subscribers = Premium content

adn.com
nchorage Daily News

Protect the information

Legislation overdue to fight identity theft, help consumers



(Peter Dunlap-Shohl)

(Published: December 1, 2005)

It's been nine months since ChoicePoint, a nationwide data broker, announced that thieves last year obtained access to sensitive information on at least 145,000 people.

As The Wall Street Journal reported, the ChoicePoint disclosure, which was required by California state law, "set off a wave of corporate confessions" of lost or stolen personal data. Others to apologize this year have included CardSystems Solutions, which processes credit card transactions; banking firm HSBC, which manages MasterCard accounts for GM; LexisNexis, a nationwide database firm; and some of the biggest names in corporate America, including Bank of America and Time Warner.

And still consumers are waiting for Congress to do something to help protect people in such cases against identify theft. Alaskans, too, are waiting for their elected officials to do something on the state level.

About half the states have passed security-breach notification laws, similar to California's 2003 statute, but a federal law would be preferable for several reasons. It would be better for businesses than dealing with a patchwork of state laws; it would be more effective in dealing with a problem that crosses state borders; and it would be easier for consumers who deal with banks, credit card companies, Internet shops and credit agencies across the country.

The California law, and similar legislation introduced in Congress and the Alaska Legislature, requires businesses to notify people if their personal information is stolen. It's hard to believe such a simple warning could be so difficult to legislate, but that's what happens when businesses object to government rules and consumer advocates run into corporate lobbyists.

Proposals before legislatures around the country would allow consumers to freeze their credit reports to block the misuse of the data; restrict the collection and use of such information, specifically Social Security numbers; require the destruction of some personal records; and improve consumer access to their own credit reports.

On the federal level, several bills were introduced this year, proposing varied solutions. The House Energy and Commerce Committee approved a bill, but it required notification of consumers only when the security breach posed a significant risk of identity theft. Democrats say that is too lax a standard and oppose the measure. Skeptics worry Congress may do nothing again next year.

But in Alaska, there's hope. Democratic Sen. Gretchen Guess of Anchorage and Republican Sen. Gene Therriault of North Pole are working together to draft a compromise bill for consideration during the legislative session that convenes in January.

The senators are looking to incorporate key consumer-protection measures in their bill. Several legislators introduced bills on the problem last year. Though none made it as far as a vote by the full House or Senate, committee hearings provided the senators with clues of the trouble spots to avoid and key pieces to include.

More than 430 Alaskans were victimized by identify theft in 2004, almost double the 2003 total, according to the Federal Trade Commission. That's too many victims. Consumers deserve better protections.

BOTTOM LINE: We hope Sens. Guess and Therriault can persuade their colleagues to pass legislation in the fight against identity theft.

Sharing

Neighbor to Neighbor needs you

The tradition of Christmas giving is as old as the Christmas story itself. And in Alaska, the tradition of giving to the less fortunate goes back to the early mining camps, where miners and merchants organized celebrations featuring entertainment and presents for their poorer neighbors.

The tradition lives on in Anchorage through the annual Neighbor to Neighbor campaign, sponsored by the Daily News in conjunction with social service

agencies. The Daily News created the fund in 1984 as a nonprofit entity, separate from the newspaper, and has raised more than $1.4 million over the years. Every cent raised goes to agencies providing assistance to individuals and families in need: None of the money is spent on administrative overhead.

No agents or solicitors are out in the community asking for funds. Donations may be mailed to the Neighbor to Neighbor Fund, care of the Anchorage Daily News at P.O. Box 149001, Anchorage 99514, or donors may drop by the newspaper office just north of DeBarr Road, west of Bragaw Street. You may also donate online by visiting www.adn.com/neighbor.

This year the paper is doing five Neighbor to Neighbor stories -- appearing on consecutive Sundays -- describing working people struggling with poverty and illness, the kind of people for whom a modest amount of financial help can make a big difference. The first story appeared last Sunday.

Nine agencies will benefit from the fund: Abused Women's Aid in Crisis, Alaska Family Resource Center, Alaska Native Justice Center, Alaska Aids Assistance Association, Hospice of Anchorage, Kids Are People (Wasilla), Catholic Social Services, Lutheran Social Services of Alaska and The Salvation Army. Descriptions of the agencies -- their mission, their activities -- appear with the Sunday stories, which also are available online.

Neighbor to Neighbor spreads the holiday spirit throughout our community. It has become a tradition because of you, because of your generosity. Please join the Daily News again in the Neighbor to Neighbor campaign.

BOTTOM LINE: Please join us in helping our neighbors this holiday season.

Print Page | Close Window

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.

LEGAL SERVICES

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

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

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

MEMORANDUM January 17, 2006

SUBJECT: SB 222 relating to personal information
(Work Order No. 24-LS1419\A)

TO: Senator Gretchen Guess
Attn: Wayne

FROM: Theresa Bannister
Legislative Counsel

You have requested a sectional summary of the above-described bill. As a preliminary matter, note that a sectional summary of a bill should not be considered an authoritative interpretation of the bill and the bill itself is the best statement of its contents.

Section 1. Adds a new chapter related to the protection of personal information.

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

Sec. 45.48.010 requires a person who owns or uses personal information (that includes personal information on a state resident) to disclose a breach of the information system containing the personal information to the state resident.

Sec. 45.48.020 allows an information collector to delay disclosing the breach of its information system if the Department of Law determines that the disclosure may compromise an investigation.

Sec. 45.48.030 describes the methods that an information collector is to use to disclose the breach of its information system.

Sec. 45.48.040 establishes a limited exception to what is considered a security breach. Relates to employees and agents of the information collector.

Sec. 45.48.050 makes a waiver of Article 1 void and unenforceable.

Sec. 45.48.060 establishes rights and remedies that are available for a violation of Article 1.

Sectional Analysis

Sec. 45.48.070 states that an information collector is subject to Article 1 if the information collector has at least the minimum contacts required by substantive due process for the state to exercise jurisdiction over the information collector.

Sec. 45.48.090 defines terms for Article 1.

Article 2. Consumer Report Security Freeze (secs. 45.48.100 - 45.48.290).

Sec. 45.48.100 allows a consumer to prohibit a consumer reporting agency from releasing the consumer's report or information derived from the report without the consumer's express authorization.

Sec. 45.48.110 describes how the consumer makes a request for a security freeze and states when the consumer reporting agency is required to place the freeze after receiving the request.

Sec. 45.48.120 requires the consumer reporting agency to send the consumer confirmation of the freeze and a personal identification number or password.

Sec. 45.48.130 requires, if a consumer requests it, that a consumer reporting agency allow access by a third party to a consumer's report or information during a security freeze. Describes how the consumer is to make the request and states when the consumer reporting agency is required to comply. Prohibits an agency from releasing a report or information to a third party during a freeze without the consumer's prior express authorization. Requires an agency to notify a consumer if a third party has attempted to access the consumer's report or information during a security freeze, and the purpose is not solely for account review. States that this section does not prevent an agency from telling a third party requesting access that a security freeze is in effect. Allows a consumer reporting agency to use telephone, facsimile, or electronic means to implement this section when consistent with certain requirements. [Please note that sec. 45.48.130(h) needs to be corrected. It appears that ", Internet, electronic mail, or another electronic method" should be deleted at the end of the subsection.]

Sec. 45.48.140 prohibits a consumer reporting agency from removing a security freeze except under certain identified conditions. Requires a consumer reporting agency to remove a freeze immediately after receiving the consumer's request that meets certain conditions.

Sec. 45.48.150 prohibits a consumer reporting agency, when dealing with a third party, from suggesting, stating, or implying that a consumer's security freeze reflects a negative credit score, history, report, or rating.

Sec. 45.48.160 prohibits a consumer reporting agency from charging a consumer for taking an action related to the placement of or removal of a freeze, for allowing access to a report on which a freeze has been placed, or to take other related action. Makes an

exception for repeated loss of personal identification numbers or passwords by the consumer.

Sec. 45.48.170 requires a consumer reporting agency to give a consumer the notice described in this section when the agency is required to give a consume: a summary of rights under 15 U.S.C. 1681g of the federal Fair Credit Reporting Act.

Sec. 45.48.180 requires an agency that violates a security freeze by releasing a report or information to notify the consumer involved and identify the information released and the third party who received the information.

Sec. 45.48.190 establishes the remedies and penalties available for a violation of Article 2.

Sec. 45.48.200 states that a consumer reporting agency is subject to Article 2 if the agency has at least the minimum contacts required by substantive due process for the state to exercise jurisdiction over the agency.

Sec. 45.48.210 states that Article 2 does not apply to certain consumer reports and describes these reports.

Sec. 45.48.220 establishes certain exemptions for Article 2.

Sec. 45.48.290 defines terms for Article 2.

Article 3. Consumer Credit Monitoring; credit accuracy (secs. 45.48.300 - 45.48.340).

Sec. 45.48.300 requires a consumer reporting agency, upon request by a consumer, to disclose certain described information, unless the request is covered by the free disclosure provisions of 15 U.S.C. 1681j(a) - (d) of the Fair Credit Reporting Act.

Sec. 45.48.310 describes the information required to be disclosed under the previous section.

Sec. 45.48.320 allows a consumer reporting agency to impose a reasonable charge for making a disclosure under sec. 45.48.300. Sets ceilings on the charge. Requires the agency to disclose the charge before making the disclosure.

Sec. 45.48.330 describes how a consumer may make a disclosure request.

Sec. 45.48.340 states when a consumer reporting agency is to provide the required disclosure.

Sec. 45.48.350 requires a person who does business in the state by distributing information about an individual's credit history, score, or ranking to immediately stop

distributing the information when notified of an inaccuracy until the accuracy can be verified or the inaccuracy corrected. Requires the person to repair the damage and pay compensation, and allows the individual to bring an action in court if the person does not comply.

Article 4. Protection of Social Security Number (secs. 45.48.400 - 45.48.410).

Sec. 45.48.400 establishes certain restrictions on how a person may, without the consent of the individual, use an individual's social security number or require an individual to use the individual's social security number. Prohibits a person from selling, leasing, loaning, trading, renting, or otherwise disclosing an individual's social security number to a third party without the individual's written consent.

Sec. 45.48.410 establishes certain penalties and remedies for knowing violations of sec. 45.48.400.

Article 5. Disposal of Records (sec. 45.48.500 - 45.48.590).

Sec. 45.48.500 requires a business, when (and after) disposing of records containing personal information, to take reasonable measures necessary to protect against unauthorized access to or use of the records. Limits the liability of a business under this section after relinquishing control of the records, if the business has otherwise complied with this Article 2 when selecting the third party for the record destruction.

Sec. 45.48.510 describes what the measures required to be taken under sec. 45.48.500 include.

Sec. 45.48.520 describes what the due diligence required by sec. 45.48.510(3) ordinarily includes.

Sec. 45.48.530 requires a business to comprehensively describe and classify as official policy of the business the policies and procedures that relate to the adequate destruction and proper disposal of personal records.

Sec. 45.48.540 establishes a civil penalty for a knowing violation of Article 5.

Sec. 45.48.550 allows an individual damaged by a violation of Article 5 to bring a civil action to enjoin further violations and to recover damages, court costs, and attorney fees.

Sec. 45.48.590 defines terms for Article 5.

Article 6. Factual Declaration of Innocence after Identity Theft; Right to File Police Report Regarding Identity Theft (secs. 45.48.600 - 45.48.690).

Sec. 45.48.600 allows, in the listed situations, a victim of identity theft to petition the superior court for a determination that the victim is factually innocent of a crime. Also allows the Department of Law to petition for the determination, or the superior court to make a determination on its own motion.

Sec. 45.48.610 allows a determination of factual innocence to be heard and made on certain items and information submitted by the parties or ordered by the court.

Sec. 45.48.620 establishes the criteria for a court to determine that a victim is factually innocent of a crime. If met, requires the court to issue an order indicating the determination.

Sec. 45.48.630 authorizes a court, after issuing an order under sec. 45.48.620, to order the victim's information that is contained in court records accessible by the public to be deleted, sealed, or labeled to show that it does not reflect the defendant's identity.

Sec. 45.48.640 allows a court that has issued an order under sec. 45.48.620 to vacate the order under certain circumstances.

Sec. 45.48.650 states that the Supreme Court may develop a form for the order under sec. 45.48.620.

Sec. 45.48.660 authorizes the Department of Law to establish a data base of individuals who have been victims of identity theft and who have received an order under sec. 45.48.620. Indicates who may access the date base.

Sec. 45.48.670 authorizes the Department of Law to establish a toll-free telephone number to provide access to information in the data base established under sec. 45.48.660.

Sec. 45.48.680 requires a local law enforcement agency with jurisdiction over the individual's actual place of residence to make a report of an individual's identity theft allegations and to provide the individual with a copy.

Sec. 45.48.690 defines terms for Article 6.

Article 7. Consumer Credit header Information (sec. 45.48.800).

Sec. 45.48.800 prohibits a consumer reporting agency from furnishing 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 report. Defines "credit header information."

Article 8. General Provisions (secs. 45.48.900 - 45.48.995).

Sec. 45.48.900 states that a provision of this chapter that is preempted by or conflicts with federal law in a particular situation does not apply to the extent of the preemption or conflict.

Sec. 45.48.990 defines terms for this chapter.

Sec. 45.48.995 titles the chapter the Alaska Personal Information Protection Act.

Section 2. Indicates that a section of the new chapter changes a court rule.

Section 3. Adds a transition provision for Article 4.

Note: Please note that sec. 45.48.130(h) needs to be corrected. It appears that ", Internet, electronic mail, or another electronic method" should be deleted at the end of the subsection.

If I may be of further assistance, please advise.

TLB:med
06-037.med

ALASKA STATE LEGISLATURE

SENATOR GENE THERRIAULT
SENATOR GRETCHEN GUESS

Explanation of Changes

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."

This documents lists minor changes made to Senate Bill 149 in creating Senate Bill 222, a unification of SB 149 (Sen. Guess) and SB 180 (Sen. Therriault).

Security Freeze provisions added from SB 180

- Consumer report security freeze provisions do not apply to the following.
  1. communication of consumer information within an organization if the information was collected directly by the organization and the consumer is notified it may be communicated internally *(lines 6–9 and 10-21 on page 8 of SB 180, excluding "or made to another person who is owned by, or affiliated with, the person making the report" from lines 13-14).*

  2. reports containing information solely about a consumer's character, general reputation, personal characteristics, or mode of living if the information is obtained through personal interviews *(lines 28–31 on page 8 of SB 180).*

  3. reports furnished for use in connection with a transaction that consists of an extension of credit to be used solely for a commercial purpose *(lines 2–4 on page 9 of SB 180).*

- In article two on consumer report security freezes, the section in SB 149 on "Violations, remedies, and penalties" *(lines 10-23, page 9)* was replaced with analogous language in SB 180 on "Violations and remedies" *(lines 12-31, page 7).*

Consumer Credit Monitoring provision added from SB 180

- In article three on consumer credit monitoring, language from SB 180 on "credit accuracy" was included in SB 222 *(lines 29-31 on page 10 and lines 1-16 on page 11 of SB 180).* This language requires a person whose business is distributing information about an individual's credit history, score, or ranking to immediately stop distributing the information upon notification that the information is inaccurate.

Other minor changes made to existing language in SB 149

- In article one on disclosure of breaches of security, regulatory/supervisory authorities with the primary jurisdiction over the person or business (e.g., Division of Insurance for insurance companies) enforce compliance. The Attorney General has jurisdiction for security breaches when there is no other regulatory authority.

- In article one on disclosure of breaches of security, the definition of "breach of security" is expanded beyond paper-based methods to include digital data and other media, thereby allowing for future technologies used for data storage and security.

- In article five on disposal of records, businesses are not held liable for the destruction of records once they have relinquished control of them (e.g., professional shredding company).

Drafting change made when creating SB 222

- While the "credit header information" section remains in article seven, the "right to file" section was moved from article seven to article six to allow more clear titling of article seven as "Credit Header Information" rather than "Miscellaneous provisions."