HB

65

Cindy Smith

From: Sen. Hollis French
Sent: Wednesday, March 26, 2008 12:34 PM
To: Cindy Smith
Subject: FW: Amendment to SCS CSHB 65(L&C)
Importance: High

Please place this in the bill file

From: Jack McRae [mailto:Jack.McRae@premera.com]
Sent: Wednesday, March 26, 2008 12:28 PM
To: Sen. Hollis French
Cc: Jerry Reinwand
Subject: Amendment to SCS CSHB 65(L&C)
Importance: High

Dear Senator French,

I am writing on behalf of Premera Blue Cross Blue Shield of Alaska to express concern about a provision in SCS CSHB 65(L&C), "an act relating to breaches of security involving personal information . . ."

Proposed new section AS 45.48.410, subsection (a) (page 17, lines 28-31), prohibits businesses from requesting or collecting an individual's social security number. Subsection (b) (page 18, lines 1-24) sets forth exemptions to the prohibition contained in subsection (a). There is no exemption for health insurers, hospital and medical services corporations or disability insurers. It is imperative that such exemptions be added to the bill.

Insuring entities currently use enrollees' social security numbers for purposes of coordinating benefits available under health insurance policies and accurately paying disability insurance benefits. The need to coordinate benefits arises when families are covered by more than one health insurance plan, typically one provided through each parent's employment. In such cases, each company will enroll the family using its own unique methodology of assigning identification numbers. When a claim is submitted for coverage by one of the plans, the insurer must coordinate with the other company to determine appropriate payment for covered benefits. The two companies need a common identifier to assure accuracy and timeliness of payment, and the social security number fills that need in current practice. Obtaining social security numbers is also imperative for coordinating benefits for individuals covered by both Medicare and a commercial insurance plan, as Medicare's health insurance claim number is typically a derivative of the beneficiary's social security number. Likewise, the social security number is indispensable for accurate administration of income replacement disability benefits. Such payments may be taxable to the insured and must be reported to the IRS under the proper social security number.

Insuring entities currently request and maintain social security numbers for these purposes. This practice serves consumers by facilitating administration of their claims and assuring payment accuracy. In Alaska, the practice is allowed and protected under federal Gramm-Leach-Bliley and HIPAA privacy laws and by administrative rules adopted by the Alaska Division of Insurance effective in 2005 (3 AAC 26 sections 605-749). Amending SCS CSHB 65(L&C) to allow current practice to continue will do nothing to undermine the consumer protections that are in place.

Therefore, we request that the following language be added to SCS CSHB 65(L&C) to section 45.48.410(b) on page 18 after line 24:

"(7) to an insurer or hospital and medical service corporation regulated under AS Title 21."

Without the amendment, Premera Blue Cross Blue Shield of Alaska cannot support the bill.

Thank you for your consideration of this request. Please let me know if you have questions or would like to discuss this matter further.

Jack

Jack C. McRae
Senior Vice President
425/918-5757
jack.mcrae@premera.com

LEGAL SERVICES

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

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

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

MEMORANDUM April 1, 2008

SUBJECT: SCS CSHB 65(JUD) relating to personal information
(Work Order No. 25-LS0311\W)

TO: Senator Hollis French
Chair of the Senate Judiciary Committee
Attn: Cindy Smith

FROM: Theresa Bannister
Legislative Counsel

This memo accompanies the bill described above.

1. Federal preemption. As you are probably aware, because the bill deals with an area that is heavily, and, in some areas exclusively, regulated by the Federal Credit Reporting Act[1] (FCRA), there is an issue whether the FCRA preempts any of the new provisions. Please be aware that while it appears that most of the general areas in the bill have not been directly regulated by FCRA, a few provisions of the bill have preemption issues. The FCRA's provisions regarding what it preempts are not clear.

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

3. AS 45.48.400(a)(5)(A). Please be aware this provision contains "expressly" in conjunction with "local, state, or federal law." You have removed the other occurrences of "expressly."

If I may be of further assistance, please advise.

TLB:med
08-241.med

Enclosure

---

[1] 15 U.S.C. 1681 et seq.

ALASKA STATE HOUSE OF REPRESENTATIVES

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

Session

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

REPRESENTATIVE JOHN COGHILL

SPONSOR STATEMENT
SENATE CS FOR CS FOR HB 65 (L&C) (25-LS0311\T)

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

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

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

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

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

ALASKA STATE HOUSE OF REPRESENTATIVES

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

Session

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

REPRESENTATIVE JOHN COGHILL

SECTIONAL

SENATE CS FOR CS FOR HB 65 (L&C) 25-LS0311\T

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

Section 1 AS 40.21.110 Care of records – this sets out the ownership of public records and how they are to be managed from creation to disposal.

Section 2 AS 44.64.030(a) adds a new paragraph (40) AS 45.48.080(c) which is part of the new Chapter 48 Personal Information Protection Act.

Section 3 AS 45 is amended by adding a new chapter *Personal Information Protection Act.* This new chapter contains a total of seven (7) Articles with individual sections.

Article 1.
Breach of Security Involving Personal Information

Sec. 45.48.010 Disclosure of breach of security.
Describes what a person who owns or uses personal information must do in case of a breach of information.

Sec. 45.48.020 Allowable delay in notification.
Describes reasons for delaying notification of a breach of information.

Sec. 45.48.030 Methods of notice.
Describes the methods to be used to notify a person that there has been a breach of information. Lists exceptions to the methods of notification relating to cost and number of consumers to be notified.

Sec. 45.48.040 Notification of certain other agencies.
Describes when it is necessary to notify other consumer reporting agencies about a breach. There are exceptions to these requirements are also set out.

Sec. 45.48.050 Exception for employees and agents.
Lists exceptions for acquisition of personal information by an employee or agent of an information collector.

Sec. 45.48.060 Waivers.
No waivers of these sections are allowed.

Sec. 45.48.070 Treatment of certain breaches.
A breach of information by an information recipient must be reported to the information distributor so they can comply with the notification requirements if the breach occurred to an information system maintained by the information distributor.

Sec. 45.48.080 Violations.
Sets out fines for violations of 45.48.010-45.48.090 by a governmental agency that is an information collector, and information collectors who are not governmental agencies.

Sec. 45.48.090 Definitions.
Defines the following terms: breach of the security; covered person, governmental agency, information collector; information distributor; information recipient; and personal information.

Article 2.
Credit Report and Credit Score Security Freeze

Sec. 45.48.100 Security freeze authorized.
Rights of consumers to prohibit release of their personal information.

Sec. 45.48.110 Placement of security freeze.
Sets out procedures for a consumer to request a consumer credit reporting agency to freeze their information.

Sec. 45.48.120 Confirmation of security freeze.
Describes the responsibility of the consumer credit reporting agency to notify the consumer when a security freeze has been placed.

Sec. 45.48.130 Access and a tions during security freeze.
Describes how a consumer can allow access to their information by a third party when a security freeze is in place; how an insurer is to treat a consumer's application if a security freeze prevents access to the consumer's information, and what changes are allowed when a security freeze is in place, and notification requirements. Defines "official information" and "technical change".

Sec. 45.48.140 Removal of security freeze.
Sets out procedure for removing a security freeze, how the request for the freeze is to be made, how the consumer credit reporting agency shall respond, and what identifiers are necessary to remove the freeze.

Sec. 45.48.150 Prohibition.
Sets out guidelines for reporting to third parties when a security freeze is in place.

Sec. 45.48.160 Charges.
Charges to a consumer regarding placing and lifting a security freeze.

Sec. 45.48.170 Notice of rights.
Additional notices to be given when a consumer is provided a summary of rights under the Fair Credit Reporting Act (FCRA).

Sec. 45.48.180 Notification after violation.
Describes the notice required if a consumer credit reporting agency violates a security freeze.

Sec. 45.48.190 Resellers.
Requires that a consumer credit reporting agency acting as a reseller honor a security freeze that is placed by another consumer reporting agency.

Sec. 45.48.200 Violations and penalties.
Describes the rights of a consumer who suffers damages as a result of a breach of their personal information.

Sec. 45.48.210 Exemptions.
Lists exemptions to the use of credit information when a security freeze is in place.

Sec. 45.48.290 Definitions.
Defines the following terms: account review, consumer, consumer credit reporting agency, reseller of consumer information, security freeze, and third party.

Article 3.
Protection of Social Security Number

Sec. 45.48.400 Use of social security number.
Sets out guidelines for handling a person's social security number.

Sec. 45.48.410 Request and collection.
Sets out prohibitions and exemptions for requesting or collecting an individual's social security number.

Sec. 45.48.420 Sale, lease, loan, trade, or rental.
Prohibitions and exemptions regarding third party use of social security numbers.

Sec. 45.48.430 Disclosure.
Prohibitions and exemptions regarding disclosure of social security numbers to third parties.

Sec. 45.48.440 Interagency disclosure.
Describes when and to whom disclosure is authorized.

Sec. 45.48.450 Exception for employees, agents, & independent contractors.
Describes when and to whom disclosure is authorized.

Sec. 45.48.460 Employment-related exception.
Describes when use of a social security number should not be restricted.

Sec. 45.48.470 Agency regulations.
Procedures for adopting regulations necessary for a state agency to carry out their duties and responsibilities.

Sec. 45.48.480 Penalties.
Rights of the state and individuals against persons that knowingly violate these sections and what damages and attorney fees may be recovered.

Article 4.
Disposal of Records

Sec. 45.48.500 Disposal of records.
This sets out the measures to be followed when disposing of records which contain personal information.

Sec. 45.48.510 Measures to protect access.
Describes the measures that may be taken to comply with Sec. 45.48.500 (above).

Sec. 45.48.520 Due diligence.
Lists procedures that if performed show due diligence.

Sec. 45.48.530 Policy and procedures.
A business or governmental agency shall adopt written policies and procedures relating to records disposal.

Sec. 45.48.540 Exemptions.
Compliance to these sections is not required if a government agency or business is required by federal law to act in another way, or the business is subject to and in compliance with GLBA, or FCRA.

Sec. 45.48.550 Civil penalty.
Liability to the state by an individual, business, or governmental agency for violations of these sections.

Sec. 45.48.560 Court action.
An individual damaged by a violation of these sections may file a civil action.

Sec. 45.48.590 Definitions.
Defines the following terms: business; conducts business; possesses; dispose; governmental agency; personal information; records.

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

Sec. 45.48.600 Factual declaration of innocence after identity theft.
Describes the conditions that should exist in order for an individual to petition the superior court for a determination of innocence of a crime involving the theft of their identity.

Sec. 45.48.610 Basis for determination.
Lists the type of information that may be made part of the record for the court to make a determination of factual innocence.

Sec. 45.48.620 Criteria for determination; court order.
Sets the criteria that the court may use to determine a victim's factual innocence.

Sec. 45.48.630 Orders regarding records.
Describes what the court may order regarding the disposition of incorrect records regarding a victim of identity theft.

Sec. 45.48.640 Vacation of determination.
States that a court order may be vacated if there has been a misrepresentation of the material.

Sec. 45.48.650 Court form.
Development of a form to be used under 45.48.620

Sec. 45.48.660 Data base.
This section allows the establishment and maintenance of a data base of victims of identity theft, and who has authorization to the information.

Sec. 45.48.670 Toll-free telephone number.
Establishes a toll-free number that accesses the information in the data base established in 45.48.660.

Sec. 45.48.680 Right to file police report regarding identity theft.
Sets out rights of an individual to file a police report if they suspect they are a victim of identity theft, and the responsibility of a law enforcement agency to make the report even if they do not have jurisdiction.

Sec. 45.48.690 Definitions.
Defines the following terms: crime, department, perpetrator, and victim.

Article 6.
Truncation of Card Information

Sec. 45.48.750 Truncation of card information.
Describes limits on a business regarding the printing of credit or debit card numbers and the exceptions depending on whether the receipt is produced electronically or is handwritten or imprinted. Provides definitions and an effective date.

Article 7.
General Provisions

Sec. 45.48.990 Definitions.
Provides definitions of consumer, consumer credit reporting agency, credit report, Fair Credit Reporting Act, Gramm-Leach-Bliley Financial Modernization Act, identity theft, information system, person, and state resident.

Sec. 45.48.995 Short Title.
Alaska Personal Information Protection Act.

Section 4 AS 45.50.471(b) is amended by adding a new paragraph (53) (A) and (B).

Section 5 The uncodified law of the State of Alaska is amended by adding a new section to read: INDIRECT COURT RULE AMENDMENTS and lists out those amendments to Rule 60(b) and 82.

Section 6 The uncodified law is amended by adding a new section TRANSITION; REGULATIONS that will take effect under AS 44.62.

Section 7 Provides an effective date for AS 45.48.470 enacted by Sec. 3.

Section 8 Provides an effective date for AS 01.10.070(c) Sec. 6.

Section 9 Provides for an effective date with exceptions in Secs. 7 and 8.

U.S. Code collection

§ 6802. Obligations with respect to disclosures of personal information

(a) Notice requirements

Except as otherwise provided in this subchapter, a financial institution may not, directly or through any affiliate, disclose to a nonaffiliated third party any nonpublic personal information, unless such financial institution provides or has provided to the consumer a notice that complies with section 6803 of this title.

(b) Opt out

(1) In general

A financial institution may not disclose nonpublic personal information to a nonaffiliated third party unless—

(A) such financial institution clearly and conspicuously discloses to the consumer, in writing or in electronic form or other form permitted by the regulations prescribed under section 6804 of this title, that such information may be disclosed to such third party;

(B) the consumer is given the opportunity, before the time that such information is initially disclosed, to direct that such information not be disclosed to such third party; and

(C) the consumer is given an explanation of how the consumer can exercise that nondisclosure option.

(2) Exception

This subsection shall not prevent a financial institution from providing nonpublic personal information to a nonaffiliated third party to perform services for or functions on behalf of the financial institution, including marketing of the financial institution's own products or services, or financial products or services offered pursuant to joint agreements between two or more financial institutions that comply with the requirements imposed by the regulations prescribed under section 6804 of this title, if the financial institution fully discloses the providing of such information and enters into a contractual agreement with the third party that requires the third party to maintain the confidentiality of such information.

(c) Limits on reuse of information

Except as otherwise provided in this subchapter, a nonaffiliated third party that receives from a financial institution nonpublic personal information under this section shall not, directly or through an affiliate of such receiving third party, disclose such

information to any other person that is a nonaffiliated third party of both the financial institution and such receiving third party, unless such disclosure would be lawful if made directly to such other person by the financial institution.

(d) Limitations on the sharing of account number information for marketing purposes

A financial institution shall not disclose, other than to a consumer reporting agency, an account number or similar form of access number or access code for a credit card account, deposit account, or transaction account of a consumer to any nonaffiliated third party for use in telemarketing, direct mail marketing, or other marketing through electronic mail to the consumer.

(e) General exceptions

Subsections (a) and (b) of this section shall not prohibit the disclosure of nonpublic personal information—

(1) as necessary to effect, administer, or enforce a transaction requested or authorized by the consumer, or in connection with—

(A) servicing or processing a financial product or service requested or authorized by the consumer;

(B) maintaining or servicing the consumer's account with the financial institution, or with another entity as part of a private label credit card program or other extension of credit on behalf of such entity; or

(C) a proposed or actual securitization, secondary market sale (including sales of servicing rights), or similar transaction related to a transaction of the consumer;

(2) with the consent or at the direction of the consumer;

(3)

(A) to protect the confidentiality or security of the financial institution's records pertaining to the consumer, the service or product, or the transaction therein;

(B) to protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability;

(C) for required institutional risk control, or for resolving customer disputes or inquiries;

(D) to persons holding a legal or beneficial interest relating to the consumer; or

(E) to persons acting in a fiduciary or representative capacity on behalf of the consumer;

(4) to provide information to insurance rate advisory organizations, guaranty funds or agencies, applicable rating agencies of the financial institution, persons assessing the institution's compliance with industry standards, and the institution's attorneys, accountants, and auditors;

(5) to the extent specifically permitted or required under other provisions of law and in accordance with the Right to Financial Privacy Act of 1978 [12 U.S.C. 3401 et seq.], to law enforcement agencies (including a Federal functional regulator, the Secretary of the Treasury with respect to subchapter II of chapter 53 of title

U.S. Code collection

§ 6801. Protection of nonpublic personal information

(a) Privacy obligation policy

It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information.

(b) Financial institutions safeguards

In furtherance of the policy in subsection (a) of this section, each agency or authority described in section 6805 (a) of this title shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards—

(1) to insure the security and confidentiality of customer records and information;

(2) to protect against any anticipated threats or hazards to the security or integrity of such records; and

(3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

Is an SSN

"non public personal inf."

under fed law?

31, and chapter 2 of title I of Public Law 91-508 (12 U.S.C. 1951-1959), a State insurance authority, or the Federal Trade Commission), self-regulatory organizations, or for an investigation on a matter related to public safety;

(6)

(A) to a consumer reporting agency in accordance with the Fair Credit Reporting Act [15 U.S.C. 1681 et seq.], or

(B) from a consumer report reported by a consumer reporting agency;

(7) in connection with a proposed or actual sale, merger, transfer, or exchange of all or a portion of a business or operating unit if the disclosure of nonpublic personal information concerns solely consumers of such business or unit; or

(8) to comply with Federal, State, or local laws, rules, and other applicable legal requirements; to comply with a properly authorized civil, criminal, or regulatory investigation or subpoena or summons by Federal, State, or local authorities; or to respond to judicial process or government regulatory authorities having jurisdiction over the financial institution for examination, compliance, or other purposes as authorized by law.

U.S. Code collection

§ 6803. Disclosure of institution privacy policy

(a) Disclosure required

At the time of establishing a customer relationship with a consumer and not less than annually during the continuation of such relationship, a financial institution shall provide a clear and conspicuous disclosure to such consumer, in writing or in electronic form or other form permitted by the regulations prescribed under section 6804 of this title, of such financial institution's policies and practices with respect to—

(1) disclosing nonpublic personal information to affiliates and nonaffiliated third parties, consistent with section 6802 of this title, including the categories of information that may be disclosed;

(2) disclosing nonpublic personal information of persons who have ceased to be customers of the financial institution; and

(3) protecting the nonpublic personal information of consumers.

Such disclosures shall be made in accordance with the regulations prescribed under section 6804 of this title.

(b) Information to be included

The disclosure required by subsection (a) of this section shall include—

(1) the policies and practices of the institution with respect to disclosing nonpublic personal information to nonaffiliated third parties, other than agents of the institution, consistent with section 6802 of this title, and including—

(A) the categories of persons to whom the information is or may be disclosed, other than the persons to whom the information may be provided pursuant to section 6802 (e) of this title; and

(B) the policies and practices of the institution with respect to disclosing of nonpublic personal information of persons who have ceased to be customers of the financial institution;

(2) the categories of nonpublic personal information that are collected by the financial institution;

(3) the policies that the institution maintains to protect the confidentiality and security of nonpublic personal information in accordance with section 6801 of this title; and

(4) the disclosures required, if any, under section 1681a (d)(2)(A)(iii) of this

title.

Gramm-Leach-Bliley Act

From Wikipedia, the free encyclopedia
(Redirected from Gramm-leach-bliley)

The ***Gramm-Leach-Bliley Act***, also known as the *Gramm-Leach-Bliley Financial Services Modernization Act*, Pub. L. No. 106-102, 113 Stat. 1338 (November 12, 1999), is an Act of the United States Congress which repealed the Glass-Steagall Act, opening up competition among banks, securities companies and insurance companies. The *Glass-Steagall Act* prohibited a bank from offering investment, commercial banking, and insurance services.

The *Gramm-Leach-Bliley Act* (*GLBA*) allowed commercial and investment banks to consolidate. For example, Citibank merged with Travelers Group, an insurance company, and in 1997 formed the conglomerate Citigroup, a corporation combining banking and insurance underwriting services. Other major mergers in the financial sector had already taken place such as the Smith-Barney, Shearson, Primerica and Travelers Insurance Corporation combination in the mid-1990's. This combination, announced in 1993 and finalized in 1994, would have violated the Glass-Steagall Act and the Bank Holding Acts by combining insurance and securities companies, if not for a temporary waiver process [[1]]. The law was passed to legalize these mergers on a permanent basis. Historically, the combined industry has been known as the financial services industry.

Contents

Changes caused by the Act

Many of the largest banks, brokerages, and insurance companies desired the Act at the time. The justification was that individuals usually put more money in investments when economy is good, but they put their money into savings accounts when it turns bad. With the new Act, they would do both with the same company, so it would be doing well in all economic times.

Prior to the Act, most financial services companies were doing this anyway. On the retail/consumer side, a bank called Norwest led the charge in offering all types of financial services products in 1986. American Express attempted to own almost every field of financial business (although there was little synergy between them). Things culminated in 1997 when Travelers, a financial services company with everything but a retail/commercial bank, bought out Citibank, creating the largest and the most profitable company in the world. The move was technically illegal and provided impetus for the passage of the *Gramm-Leach-Bliley Act*.

Also prior to the passage of the Act, there were many relaxations to the *Glass-Steagall Act*. For example, a few years earlier, commercial Banks were allowed to get into investment banking, and before that banks were also allowed to get into stock and insurance brokerage. Insurance underwriting was the only main operation they weren't allowed to do, something rarely done by banks even after the passage of the Act.

Much consolidation occurred in the financial services industry since, but not at the scale some had expected. Retail banks, for example, do not tend to buy insurance underwriters, as they seek to engage in a more profitable business of insurance brokerage by selling products of other insurance companies. Other retail banks were slow to market investments and insurance products and package those products in a convincing way. Brokerage companies had a hard time getting into banking, because they do not have a large branch and backshop footprint. Banks have recently tended to buy other banks, such as the recent Bank of America and Fleet Boston merger, yet they have had less success integrating with investment and insurance companies. Many banks have expanded into investment banking, but have found it hard to package it with their banking services, without resorting to questionable tie-ins which caused scandals at Smith Barney.

Senator Phil Gramm led the Senate Banking Committee which sponsored the Act; he later joined UBS Warburg, at the time the investment banking arm of the largest Swiss bank.

Remaining Restrictions

GLBA did not remove the restrictions on banks placed by the Bank Holding Company Act of 1940 which prevented financial institutions from owning non-financial corporations. This is significant because this restriction prevents an ownership structure similar to Japan or Germany in which banks own the majority of large industrial enterprises.

Some restrictions remain to provide some amount of separation between the investment and commercial banking operations of a company. For example, licensed bankers must have separate business cards, eg. "Personal Banker, Wells Fargo Bank" and "Investment Consultant, Wells Fargo Private Client Services". Much of the debate about financial privacy is specifically centered around allowing or preventing the banking, brokerage, and insurances divisions of a company from working together.

In terms of compliance, the key rules under the Act include *The Financial Privacy Rule* which governs the collection and disclosure of customers' personal financial information by financial institutions. It also applies to companies, regardless of whether they are financial institutions, who receive such information. *The Safeguards Rule* requires all financial institutions to design, implement and maintain safeguards to protect customer information. The Safeguards Rule applies not only to financial institutions that collect information from their own customers, but also to financial institutions – such as

credit reporting agencies – that receive customer information from other financial institutions.

Privacy

- GLBA compliance is mandatory; whether a financial institution discloses nonpublic information or not, there must be a policy in place to protect the information from foreseeable threats in security and data integrity
- Major Components put into place to govern the collection, disclosure, and protection of consumers' nonpublic personal information; or personally identifiable information:
  - Financial Privacy Rule
  - Safeguards Rule
  - Pretexting Protection

Financial Privacy Rule

(Subtitle A: Disclosure of Nonpublic Personal Information, codified at 15 U.S.C. § 6801–6809)

The Financial Privacy Rule requires financial institutions to provide each consumer with a privacy notice at the time the consumer relationship is established and annually thereafter. The privacy notice must explain the information collected about the consumer, where that information is shared, how that information is used, and how that information is protected. The notice must also identify the consumer's right to opt-out of the information being shared with unaffiliated parties per the Fair Credit Reporting Act. Should the privacy policy change at any point in time, the consumer must be notified again for acceptance. Each time the privacy notice is reestablished, the consumer has the right to opt-out again. The unaffiliated parties receiving the nonpublic information are held to the acceptance terms of the consumer under the original relationship agreement. In summary, the financial privacy rule provides for a privacy policy agreement between the company and the consumer pertaining to the protection of the consumer's personal nonpublic information.

Safeguards Rule

(Subtitle A: Disclosure of Nonpublic Personal Information, codified at 15 U.S.C. § 6801–6809)

The Safeguards Rule requires financial institutions to develop a written information security plan that describes how the company is prepared for, and plans to continue to protect clients' nonpublic personal information. (The Safeguards Rule also applies to information of those no longer consumers of the financial institution.) This plan must include:

- Denoting at least one employee to manage the safeguards,
- Constructing a thorough [risk management] on each department handling the nonpublic information,
- Develop, monitor, and test a program to secure the information, and
- Change the safeguards as needed with the changes in how information is collected, stored, and used.

This rule is intended to do what most businesses should already be doing: ***protect their clients***. The Safeguards Rule forces financial institutions to take a closer look at how they manage private data and to do a risk analysis on their current processes. No process is perfect, so this has meant that every financial

institution has had to make some effort to comply with the GLBA.

Pretexting Protection

(Subtitle B: Fraudulent Access to Financial Information, codified at 15 U.S.C. § 6821–6827)

Pretexting (sometimes referred to as "social engineering") occurs when someone tries to gain access to personal nonpublic information without proper authority to do so. This may entail requesting private information while impersonating the account holder, by phone, by mail, by email, or even by "phishing" (i.e., using a "phony" website or email to collect data). The GLBA encourages the organizations covered by the GLBA to implement safeguards against pretexting. For example, a well-written plan written to meet GLBA's Safeguards Rule ("develop, monitor, and test a program to secure the information") ought to include a section on training employees to recognize and deflect inquiries made under pretext. In the United States, pretexting by individuals is punishable as a common law crime of False Pretenses.

Financial Institutions Defined

The GLBA defines "financial institutions" as: ..."companies that offer financial products or services to individuals, like loans, financial or investment advice, or insurance. The Federal Trade Commission (FTC) has jurisdiction over financial institutions similar to, and including, these:

- non-bank mortgage lenders,
- loan brokers,
- some financial or investment advisers,
- debt collectors,
- tax return preparers,
- banks, and
- real estate settlement service providers.

These companies must also be considered significantly engaged in the financial service or production that defines them as a "financial institution".

Insurance has jurisdiction first by the state, provided the state law at minimum complies with the GLBA. State law can require greater compliance, but not less than what is otherwise required by the GLBA.

Consumer vs. Customer Defined

The *Gramm-Leach-Bliley Act* defines a 'consumer' as

> "an individual who obtains, from a financial institution, financial products or services which are to be used primarily for personal, family, or household purposes, and also means the legal representative of such an individual." (See 15 U.S.C. § 6809(9).}

A 'customer' is a consumer that has developed a relationship with privacy rights protected under the *GLBA*. A 'customer' is not someone using an automated teller machine (ATM) or having a check cashed at a cash advance business. These are not ongoing relationships like a 'customer' might have; i.e. a

mortgage loan, tax advising, or credit financing. A business is not an individual with personal nonpublic information, so a business cannot be a customer under the *GLBA*. A business, however, may be liable for compliance to the *GLBA* depending upon the type of business and the activities utilizing individual's personal nonpublic information.

Consumer/Client Privacy Rights

Under the *GLBA*, financial institutions must provide their clients a privacy notice that explains what information the company gathers about the client, where this information is shared, and how the company safeguards that information. This privacy notice must be given to the client prior to entering into an agreement to do business. There are exceptions to this when the client accepts a delayed receipt of the notice in order to complete a transaction on a timely basis. This has been somewhat mitigated due to online acknowledgement agreements requiring the client to read or scroll through the notice and check a box to accept terms.

The privacy notice must also explain to the customer the opportunity to 'opt-out'. Opting out means that the client can say "no" to allowing their information to be shared with affiliated parties. The *Fair Credit Reporting Act* is responsible for the 'opt-out' opportunity, but the privacy notice must inform the customer of this right under the GLBA. The client cannot opt-out of:

- information shared with those providing priority service to the financial institution
- marketing of products or services for the financial institution
- when the information is deemed legally required.

GLBA Enforced

Violation of the *GLBA* may result in a civil action brought by the United States Attorney General. The penalties, as amended under the *Financial Institution Privacy Protection Act* of 2003 (108th CONGRESS - 1st Session - S. 1458; To amend the *Gramm-Leach-Bliley Act* to provide for enhanced protection of nonpublic personal information, including health information, and for other purposes., In The Senate of the United States, July 25 (legislative day, JULY 21), 2003)include,

- "the financial institution shall be subject to a civil penalty of not more than $100,000 for each such violation"
- "the officers and directors of the financial institution shall be subject to, and shall be personally liable for, a civil penalty of not more than $10,000 for each such violation".

Critics

Economist Robert Kuttner has criticized the repeal of the Glass-Steagall Act as contributing to the 2007 subprime mortgage financial crisis [2]. Paul Krugman of the New York Times has suggested that Sen. Gramm's advocacy of financial services deregulation is a substantial cause of the current economic downturn. [3]

External links

FYI: Websites for Compliance Information

- Disclosure of Nonpublic Personal Information
- Financial Institutions and Customer Data: Complying with the Safeguards Rule

FYI: Websites for Consumer/Client Rights Information

- Disclosure of Nonpublic Personal Information
- What Can You Do To Protect Your Privacy
- Privacy Choices for Your Personal Financial Information
- Pretexting: Your Personal Information Revealed

FYI: History of the GLBA

- History of the GLBA

References

- Financial Privacy: The Gramm-Leach Bliley Act, Federal Trade Commission, 1999
- Gramm-Leach-Bliley Act,15 USC, Subchapter I, Sec. 6801-6809, Disclosure of Nonpublic Personal Information, 1999
- Gramm-Leach-Bliley and You, Chapple, Mike, November 18, 2003
- Gramm-Leach-Bliley Act Financial Privacy Provisions:The Federal Government Imposes Broad Requirements to Address Consumer Privacy Concerns, Ledig, Robert H.
- The Gramm-Leach-Bliley Act: The Financial Privacy Rule, Federal Trade Commission
- In Brief: The Financial Privacy Requirements of the Gramm-Leach-Bliley Act, Federal Trade Commission
- The Gramm-Leach-Bliley Act — "History of the GLBA", Electronic Privacy Information Center
- Financial Institution Privacy Protection Act of 2003 — 108th CONGRESS, 1st Session, S. 1458, "To amend the Gramm-Leach-Bliley Act to provide for enhanced protection of nonpublic personal information, including health information, and for other purposes.", IN THE SENATE OF THE UNITED STATES; July 25 (legislative day, JULY 21), 2003
- Testimony of Governor Laurence H. Meyer Merchant banking

See also

- Bank regulation
- Financial regulation
- Financial institutions
- Information Technology Audit
- privacy
- Health Insurance Portability and Accountabiiity Act
- Data Loss Prevention

Cindy Smith

From: Karen Lidster
Sent: Monday, March 31, 2008 6:03 PM
To: Cindy Smith
Subject: FW:

Here you go. Sorry it took me so long. Thanks,
karen

From: Sniffen, Clyde E. (LAW) [mailto:ed.sniffen@alaska.gov]
Sent: Monday, March 31, 2008 3:28 PM
To: Karen Lidster
Cc: Sen. Lesil McGuire
Subject:

Karen:

Based on Senator McGuire's comments today, I propose the following amendment to address the "consultation with law enforcement" problem,:

AMENDMENT

Offered in the Senate Judiciary Committee to
SCS for CSHB 65 (L&C)

Page 2, lines 19 and 20
Delete text beginning with "consultation" on line 19 and ending with "enforcement" on line 20. Replace with:

"written notification to the Alaska Attorney General"

Explanation:

Since this bill targets information only on Alaska consumers, it makes since that if a company was considering NOT NOTIFYING Alaska consumers of a potential breach, that the Alaska AG should be notified as part of the company's investigation. The AG can then decide how to act on the information, including whether to forward the notification to other federal or local authorities as appropriate, or simply require the business to notify the consumer(s). This also makes it clear who a business needs to notify.

Clyde "Ed" Sniffen, Jr
Senior Assistant Attorney General
Alaska Department of Law
Commercial and Fair Business Section
1031 W. 4th Avenue #200
Anchorage, AK 99501
(907) 269-5200 (tel)
(907) 276-8554 (fax)
Ed.Sniffen@Alaska.gov

252-9191
Pat Carter

Talking points for SSN Amendments

Amendment #1

This particular amendment is needed to modify the current language, "expressly authorized," to language which better reflects the structure and language of statues governing the use of social security numbers.

The current existing federal regulatory structure that companies such as Choicepoint LexisNexis, and the credit bureaus operate under - Gramm-Leach Bliley, Fair Credit Reporting Act, Driver's Privacy Protection Act to name a few - and their state counterparts - do not "expressly authorize" the use of a social security number, or even speak directly to the legitimate business use of a social security number.

In fact, the statutes don't "expressly" refer to social security numbers. These statutes and others regulate the use of "nonpublic personal information" or "personal information" of which a social security number is included.

Additionally, these statutes do not "expressly authorize" use of the information. These statutes are "negative" statutes. They prohibit the use of such data but for certain narrow permissible purposes or other exemptions.

In short, they say 'you cannot use this data but for these permissible purposes or other allowed uses.'

The bill should reflect the language and construction of the statutes governing use of social security numbers. Without this amendment, the "expressly authorized" language cancels out the allowances for legitimate use of social security numbers made in existing law.

Amendment #2

As currently drafted, this bill requires a business to be both regulated by the federal statute (Gramm-Leach Bliley or the Fair Credit Reporting Act) AND have their use regulated by that statute for the exemption to apply.

The federal statutes are drafted in a way to restrict the uses of the information and therefore even if a particular industry isn't regulated by the statute, their use of information is restricted by it. Any misuse of the information, even by a company not regulated by the statute, falls under the prosecutorial jurisdiction of the FTC.

Without this amendment, the exemption is too narrow to allow for transactions which are occurring everyday to facilitate consumer to business transactions (such as credit) or business to business transactions (such as a bank using a SSN to verify that a customer is not a known terrorist, in compliance with the Patriot Act). These are important transactions that need to occur and already are heavily regulated.

The concern is appropriately that people handling sensitive information, like a social security number, should be held accountable for misuse. These amendments preserve that accountability but they also preserve the legitimate business uses for information that facilitate transactions for all Alaskans.

AMENDMENT (1)

OFFERED IN THE SENATE

TO: SCS CSHB 65(L&C)

Page 18, line 14, following "Act":

Insert "or to collections or requests"

Page 18, line 16, following "Act":

Insert "or to collections or requests"

Page 19, line 1, following "Act":

Insert "or"

Page 19, line 3, following "Act":

Insert "or"

Page 19, line 31:

Delete "and"

Insert "or"

Page 20, line 3:

Delete "and"

Insert "or"

L

AMENDMENT (2)

OFFERED IN THE SENATE

TO: SCS CSHB 65(L&C)

Page 18, lines 2 - 6:

Delete all material and insert:

"(1) if the person's use is ~~restricted to~~ An allowable ~~uses~~ use or purpose under local, state, or federal law, including a regulation adopted under AS 45.48.470, to

(A) demand proof of the individual's social security number;

(B) request or collect the individual's social security number; or

(C) submit the individual's social security number to the local, state, or federal government;"

Page 18, line 29:

Delete "expressly authorized by"

Insert "restricted to allowable uses or purposes under"

Page 19, line 22:

Delete "expressly authorized by"

Insert "restricted to allowable uses or purposes under"

Monday, March 31, 2008

The Honorable Hollis French
Chair, Judiciary Committee
State Capitol, Room 417
Juneau, AK 99801-1182

Dear Chairman French:

Thank you for the opportunity to testify regarding the Senate CS for CS for House Bill No. 65 (L&C), or HB0065E.

Experian is a broad-based information solutions provider, and has certain business divisions that collect and use Social Security numbers in various contexts. Essentially, Experian collects and provides Social Security numbers to qualified businesses, non-profit organizations and government agencies that have been screened to ensure that they have either a valid permissible purpose under the Fair Credit Reporting Act (FCRA) or an allowable use under Section 502(e) of the Gramm-Leach-Bliley Act (GLB) to receive Social Security number information. Experian's use and disclosure of Social Security numbers is only in a business-to-business context. No Experian entity sells, shares or disclosures Social Security numbers to the general public or to consumers, except as required by the Fair Credit Reporting Act and then only at the request of the individual consumer to whom that number pertains.

Social Security numbers are used for a variety of purposes by Experian, ranging from ensuring the accuracy of information contained in a consumer's credit report to authentication and order processing. Social Security numbers are also used for verifying or obtaining credit scores and for internal matching purposes. Other uses for Social Security numbers include: pre-employment screening for volunteer employees, locating former employees, locating beneficiaries and heirs, locating former patients, locating owners of unclaimed goods, collection of overdue payments, account tracking, audit and quality control.

As I explained during the hearing, Article 3 in HB 65 has unprecedented prohibitions against the request or collection of a Social Security number from an individual, against the sale, lease, loan, trade or rental of a Social Security number to a third party, or against the disclosure of a Social Security number to a third party. Since this provision would be enforced by a private right of action with statutory penalties, if Experian is to continue to sell our products in Alaska, the exceptions to those prohibitions must be clear . If the exemptions are not clear as we have asked, we may interpret that as an indication that the Alaska legislature intends for Experian to stop selling some or all products that include Social Security numbers.

It is critical for Experian that the exceptions include those uses authorized under the

GLBA and the FCRA because there is a body of case law and rulemaking around those statutes. An enumeration of uses permitted by FCRA and GLB would not likely provide the robust body of rulemaking and case law the defines our uses. As previously mentioned, all Experian products that include Social Security numbers are governed by GLB and FCRA. If Experian cannot rely upon exceptions for uses permitted by those laws, then we would have review all of our products to decide if we may still sell them in Alaska.

Also, while the restrictions on the uses of information regulated by GLB and FCRA remain with the products that Experian sells and are enforceable, many of our customers are not financial institutions under GLB. Therefore the current exceptions for an entity regulated by GLB or FCRA and for a use governed by the same law is inadequate. Experian would have to review our products and procedures to see how best to comply with such a law.

I would like to add that throughout this process, I am unaware of any Experian products that have been identified as objectionable and therefore worthy of prohibition. However, Experian is inclined to take Rep. Coghill at his word when he says that the bill as submitted to the committee is intended to stop at least some of the sharing of SSNs that is done legally today.

In addition, I would respectfully like to echo the concern of the Consumer Data Industry Association and others that the laws that govern the use of personal information rarely "expressly authorize" a particular use for Social Security numbers. Therefore, any exception should use language that is consistent with the type of regulation.

Please do not hesitate to contact me if there are any questions.

Sincerely,

Murray

Murray Johnston
Director, State Government Affairs
Experian
1401 K Street, NW, Suite 501
Washington, DC 20005-3417
(202) 682-4614 - office
(202) 320-7359 - mobile
murray.johnston@experian.com

AARP Alaska

March 28. 2008

The Honorable Hollis French, Chair
Senate Judiciary Committee
Alaska State Capitol, Room 417
Juneau, Alaska 99801-1182

HB 65 (Coghill and Gara)—Support

Dear Chair French:

On behalf of the members of AARP in Alaska, we urge you and your colleagues on the Senate Judiciary Committee to support HB 65, authored by Representative John Coghill and Representative Les Gara and co-sponsored by twenty-five other House members as well as Senators Therriault and Wilken. This bill builds on much of the excellent work done last session by Senators Gene Therriault and Gretchen Guess.

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

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

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

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

We also found that older users of the Internet were much less likely to participate in on-line commercial activities. Forty-three percent of our younger members, aged 50 to 64 do "not at all" trust companies providing information or services on the Internet; only nineteen percent indicated they "mostly" or "completely" trust such companies.

3601 C Street, Suite 1420 | Anchorage, AK 99503 | toll-free 866-227-7447 | 907-341-2270 fax | toll-free 877-434-7598 TTY
Marie F. Smith, President | William D Novelli, Chief Executive Officer | www.aarp.org/ak

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

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

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

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

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

Thank you for your consideration.

Sincerely,

Marie Darlin

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

CC: Vice-Chair Charlie Huggins
Senator Lesil McGuire
Senator Bill Wielechowski
Senator Gene Therriault
Representative John Coghill
Representative Les Gara

Ray Gillespie
Gillespie & Associates
Lobbying and Governmental Affairs

SESSION (January–May)
130 Seward Street #201
Juneau, Alaska 99801
Telephone: 907.463.3375
Fax: 907.463.5522
Cell: 907.230.8843

INTERIM (June–December)
1241 W. 27th Ave. #456
Anchorage, Alaska 99503
Telephone: 907.243.3125
Fax: 907.243.3125

Re: HB 65 PERSONAL INFORMATION & CONSUMER CREDIT

Senate Judiciary Committee Members,

With the amendment on Monday, March 31st deleting the words "debt collection" from page 20, subsection (6) on page lines 9 and 10, the bill now seems to prohibit a telephone company (or any other merchant who extends credit) from using a SS # to collect a debt using a collection agency.

This is a curious result because the bill permits the same company to request and collect the same SS # under subsection (6) of section 45.48.410 (page 18, line 22-24).

Subsection (6) still allows disclosure of the SS# for "background check, identity verification and fraud prevention".

It seems anomalous that a company can collect the SS # as a part of a transaction to provide services and extend credit and be subsequently prohibited from using it to collect a debt(transferring it to a collection agency) arising from the same transaction. It also seems confusing that the section seems to allow transfer of the SS # to the collection agency for "identity verification" purposes and "to avoid fraud" but not ***debt collection.***

Sincerely
Ray Gillespie
For ATT Alascom and ATT (wireless phone services)

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

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

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

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

Proposed amendments and their effect:

Article 2. Credit Report and Credit Score Security Freeze.

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

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

Sec. 45.48.130. Placement of security freeze.

(e) If a security freeze is in place, a consumer credit reporting agency may not release the credit report or credit score to a third party that intends to use the information to determine a consumer's eligibility for credit or for the opening of a new account without the prior express authorization of the consumer.

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

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

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

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

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

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

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

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

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

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

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

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

Property Casualty Insurers Association of America
Shaping the Future of American Insurance

January 23, 2008

The Hon. John Coghill
Alaska State Representative
State Capitol, Room 214
Juneau, AK 99801-1182

Dear Rep. Coghill,

In advance of today's scheduled hearing of HB 65 in the House Finance Committee, I wanted to take a moment to reacquaint you with amendments proposed to the measure in 2006 and 2007 by the Property Casualty Insurers Association of America. PCI, you will recall, is the nation's leading property-casualty trade association, representing more than 1,000 member companies nationwide.

These are issues we discussed when PCI's Alaska lobbyist, Kris Knauss, and I met with you in your office a year ago. It remains our hope that in Alaska's efforts to join the 40 states which have enacted identity theft legislation that includes a "credit freeze" option for consumers, that you will consider providing access to credit histories for non-lending purposes even where a freeze is in place – as 30 states have done in the past two years (33 of the 40 states have allowed insure access overall).

We seek this "narrow definition" of a credit freeze to speed response to consumer requests for rate quote information and to make the insurance application process as quick and "hassle-free" as possible for consumers in an age of instantaneous, 24/7 access to products and services.

PCI's approach to accessing "frozen" credit files is based on the fact that those who seek to steal personal financial information by committing identity theft crimes do not engage in this activity in order to obtain home or auto insurance. Thus, we seek to protect the ability of insurers to provide faster service to our customers while also leaving in place the peace of mind consumers may seek to protect their personal and financial information through a "credit freeze."

PCI is **not** requesting an exemption from the provisions of the credit freeze, per se. We are requesting that you define "credit information" for purposes of this legislation as consumer reports which are reviewed in consideration of the extension of credit. Our proposed language improves the measure not only for insurance consumers, agents and carriers, but also for other non-lending entities, such as employers, rental property owners and even government agencies that review consumer reports to determine eligibility for employment or housing.

I have attached for your review a summary of the proposed amendments PCI suggests adding to HB 65. We hope to have the opportunity to speak to these amendments during today's hearing, and we hope you and your colleagues will consider adding this language to improve the underlying legislation.

I have also attached the most recent information PCI has on the passage of identity theft/credit freeze measures across the nation. As I noted above 33 of the 40 states approving such bills have included language allowing insurers access to "frozen" consumer reports – including 30 of 31 states in 2006-07.

Please let me know if I may provide any additional information or answer any questions or concerns you may have. You may contact me directly, or reach me through Kris Knauss at your convenience.

Warm Regards,

Kenton Brine
NW Regional Manager

1500 Water Street SW, Ste 2 - Olympia, Washington 98501 - 360.915.6268 - kenton.brine@pciaa.net

Security (Credit) Freeze – Impact on Insurers

State	Effective date (or effective date of last amendment)	Insurer Access to Frozen Files Permitted	Specific Insurer Exemption	Applies Only to Requests Related to the Extension of Credit
Arkansas	1/1/08	yes	X	X
California	1/1/03	no		
Colorado	7/1/06	yes	X	
Connecticut	1/1/06	no		
Delaware	10/1/06	yes	X	
D.C.	7/1/06	yes	X	
Florida	7/1/06	yes	X	
Hawaii	1/1/07	yes	X	
Illinois	1/1/07	yes	X	
Indiana	9/1/07	yes	X	
Kansas	1/1/07	yes	X	
Kentucky	7/11/06	yes	X	
Louisiana	7/1/05	no		
Maine	2/1/06	no		
Maryland	7/1/08	yes	X	
Massachusetts	10/31/07	yes	X	
Minnesota	8/1/06	yes		X
Mississippi	7/1/07	yes	X	X
Montana	7/1/07	yes	X	
Nebraska	9/1/07	yes	X	X
Nevada	10/1/05	no		
New Hampshire	1/1/07	yes	X	
New Jersey	1/1/06	no		
New Mexico	7/1/07	yes	X	X
New York	11/1/06	no		
North Carolina	12/1/05	yes	X	
North Dakota	6/1/07	yes	X	
Oklahoma	1/1/07	yes	X	
Oregon	10/1/07	yes	X	X
Pennsylvania	1/1/07	yes	X	
Rhode Island	1/1/07	yes	X	X
South Dakota	7/1/06	yes	X	X
Tennessee	1/1/08	yes	X	X
Texas	9/1/03	yes		X
Utah	9/1/08	yes		X
Vermont	7/1/06	yes	X	
Washington	7/24/05/ 9/1/08	No/ yes		X (9/1/08)
Wisconsin	1/1/07	yes	X	X
West Virginia	6/8/07	yes	X	
Wyoming	7/1/07	yes		X

Security (Credit) Freeze – Impact on Insurers

Total states w/ freeze laws:	40
Insurer access permitted:	33
Total laws enacted in 2006:	17 (including amend. to existing law in IL and VT)
Allowing access to insurers:	16
Total laws enacted in 2007	14 (including amend. to existing law in HI, TX, WA)
Allowing access to insurers:	14

The various states differ in their approach to allowing a security freeze. Some states only allow victims of identity theft to freeze access to their credit information, while others allow all consumers to request a freeze. All of the states, however, provide that when a third party requests information that is "frozen," the third party may treat the application as "incomplete" if the consumer does not grant access to the requested information. All 40 states also provide access for prescreening purposes (a requirement of the FCRA that state laws may not pre-empt).

There are two ways in which the bills may continue to allow access to information for property casualty insurance companies. The first is by a specific exemption. Each state freeze bill includes a list of persons to whom a freeze does not apply. To this list of exceptions PCI seeks to add:

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

Insurers may also continue to access credit information for insurance scoring and other permissible business if the freeze is limited to requests for credit information for the purpose of extending credit - situations most vulnerable to identity theft. The preferred definition comes from the Texas law (one of the first security freeze laws enacted) and reads:

"Security freeze" means a notice placed on a consumer file that prohibits a consumer reporting agency from releasing a consumer report relating to the extension of credit involving that consumer file without the express authorization of the consumer."

This narrowed definition is also supported by the consumer reporting entities as they believe it would serve as the most effective language for fighting identity theft, while still allowing consumer reporting agencies to sell information for all other legally permissible purposes.

It is important to note that providing an exception for insurers does *not* over-ride any current limitations on the use of credit information or any current signature requirements. It simply allows insurers to continue to access credit information as currently permitted without requiring the consumer to go through the process of "lifting" the freeze to allow temporary access.

Monday, March 31, 2008

The Honorable Hollis French
Chair, Judiciary Committee
State Capitol, Room 417
Juneau, AK 99801-1182

Dear Chairman French:

Thank you for the opportunity to testify regarding the Senate CS for CS for House Bill No. 65 (L&C), or HB0065E.

Experian is a broad-based information solutions provider, and has certain business divisions that collect and use Social Security numbers in various contexts. Essentially, Experian collects and provides Social Security numbers to qualified businesses, non-profit organizations and government agencies that have been screened to ensure that they have either a valid permissible purpose under the Fair Credit Reporting Act (FCRA) or an allowable use under Section 502(e) of the Gramm-Leach-Bliley Act (GLB) to receive Social Security number information. Experian's use and disclosure of Social Security numbers is only in a business-to-business context. No Experian entity sells, shares or disclosures Social Security numbers to the general public or to consumers, except as required by the Fair Credit Reporting Act and then only at the request of the individual consumer to whom that number pertains.

Social Security numbers are used for a variety of purposes by Experian, ranging from ensuring the accuracy of information contained in a consumer's credit report to authentication and order processing. Social Security numbers are also used for verifying or obtaining credit scores and for internal matching purposes. Other uses for Social Security numbers include: pre-employment screening for volunteer employees, locating former employees, locating beneficiaries and heirs, locating former patients, locating owners of unclaimed goods, collection of overdue payments, account tracking, audit and quality control.

As I explained during the hearing, Article 3 in HB 65 has unprecedented prohibitions against the request or collection of a Social Security number from an individual, against the sale, lease, loan, trade or rental of a Social Security number to a third party, or against the disclosure of a Social Security number to a third party. Since this provision would be enforced by a private right of action with statutory penalties, if Experian is to continue to sell our products in Alaska, the exceptions to those prohibitions must be clear . If the exemptions are not clear as we have asked, we may interpret that as an indication that the Alaska legislature intends for Experian to stop selling some or all products that include Social Security numbers.

It is critical for Experian that the exceptions include those uses authorized under the

GLBA and the FCRA because there is a body of case law and rulemaking around those statutes. An enumeration of uses permitted by FCRA and GLB would not likely provide the robust body of rulemaking and case law the defines our uses. As previously mentioned, all Experian products that include Social Security numbers are governed by GLB and FCRA. If Experian cannot rely upon exceptions for uses permitted by those laws, then we would have review all of our products to decide if we may still sell them in Alaska.

Also, while the restrictions on the uses of information regulated by GLB and FCRA remain with the products that Experian sells and are enforceable, many of our customers are not financial institutions under GLB. Therefore the current exceptions for an entity regulated by GLB or FCRA and for a use governed by the same law is inadequate. Experian would have to review our products and procedures to see how best to comply with such a law.

I would like to add that throughout this process, I am unaware of any Experian products that have been identified as objectionable and therefore worthy of prohibition. However, Experian is inclined to take Rep. Coghill at his word when he says that the bill as submitted to the committee is intended to stop at least some of the sharing of SSNs that is done legally today.

In addition, I would respectfully like to echo the concern of the Consumer Data Industry Association and others that the laws that govern the use of personal information rarely "expressly authorize" a particular use for Social Security numbers. Therefore, any exception should use language that is consistent with the type of regulation.

Please do not hesitate to contact me if there are any questions.

Sincerely,

Murray

Murray Johnston
Director, State Government Affairs
Experian
1401 K Street, NW, Suite 501
Washington, DC 20005-3417
(202) 682-4614 - office
(202) 320-7359 - mobile
murray.johnston@experian.com