11481 HOUSE JUDICIARY

(127) "supermarket" means a food establishment that contains a grocery and that also contains two or more other types of operations that are subject to the permit and fee requirements of this chapter;

(128) "sushi" means an assembled food product, usually containing rice wrapped in seaweed, that may or may not contain raw seafood;

(129) "tableware" means multi-use eating and drinking utensils;

(130) "temporary food service" means a type of food service that is kept at one location for no more than 21 consecutive days in conjunction with a single event, or for no more than 28 consecutive days if an extension is granted by the department;

(131) "thermal processing" means the application of heat to render food free of microorganisms that are capable of reproducing in the food under normal nonrefrigerated conditions of storage or distribution;

(132) "traditional wild game meat" means game meat that is from wild animals commonly found in and consumed by people in this state; "traditional game meat" includes reindeer, caribou, moose, whale, beaver, muskrat, hare, squirrel, duck, and geese;

(133) "USDA" means the United States Department of Agriculture;

(134) "unpasteurized juice" means juice that has not been specifically processed to prevent, reduce, or eliminate the presence of pathogens, either through heat pasteurization or in another manner allowed under 21 C.F.R. 101.17(g)(7), adopted by reference in 18 AAC 31.011; "unpasteurized juice" includes a beverage containing juice if the juice ingredient or the beverage has not been processed as described in this paragraph;

(135) "utensil" means an implement used to eat, drink, serve, prepare, transport, or store food;

(136) "vending machine" means a self-service device that, upon insertion of a coin, paper currency, token, card, or key, dispenses a unit serving of food, whether in a package or into a container, without the necessity of replenishing the device between each vending operation; "vending machine" does not include a semi-automated espresso machine described in 18 AAC 31.630(c);

(137) "warehouse" means a type of market used exclusively to store food commodities before distribution;

(138) "water activity" means the measure of unbound, free water in a food available to support biological and chemical reactions and is the quotient of the water vapor pressure of the substance divided by the vapor pressure of pure water at the same temperature; and

(139) "wholesale" means a food establishment that manufactures, packages,

stores, repackages, or transports food to another entity for resale or redistribution;

(140) "wholesome" means in sound condition and free from spoilage, filth, and microbial or chemical contamination. (Eff.5/18/97, Register 142; am 5/23/98, Register 146; am/readopt 12/19/99, Register 152; am 6/28/2001, Register 158; am ___/___/____, Register ___)

Authority:	AS 03.05.011	AS 17.20.190	AS 17.20.346
	[AS 17.05.050]	AS 17.20.200	AS 18.35.100
	AS 17.20.005	AS 17.20.220	AS 18.35.120
	AS 17.20.010	AS 17.20.230	AS '8.35.200
	AS 17.20.020	AS 17.20.270	AS 18.35.220
	AS 17.20.040	AS 17.20.290	AS 18.25.300
	AS 17.20.070	AS 17.20.300	AS 44.46.020
	AS 17.20.072	AS 17.20.340	AS 44.46.025
	AS 17.20.180		

Editor's note: Effective 12/19/99, Register 152, the Department of Environmental Conservation readopted 18 AAC 31.990, to affirm the validity of that section following statutory amendments made in ch. 72, SLA 1998. The department also repealed 18 AAC 31.990(8), amended 18 AAC 31.990(12), (46)(F), (61), and (81) and added new paragraphs (114) – (127). Chapter 72, SLA 1998 relocated department authority to adopt regulations in 18 AAC 31 from AS 03.05 to AS 17.20.

Information about how to review or obtain a copy of a requirement referred to in 18 AAC 31.990 and adopted by reference in 18 AAC 31.011 is set out in the editor's note to 18 AAC 31.011.

Representative Jay Ramras
Co-Chair, House Resources
V-Chair, Economic Develop.
Tourism & Trade
House State Affairs
119 N. Cushman St. Suite 207
Fairbanks, Alaska 99701
Phone: (907) 452-1088
Fax: (907) 452-1146

Alaska State Legislature

While in Session
State Capitol, Room 104
Juneau, Alaska 99801-1182
(907) 465- 3004
Fax: 465-2070
Toll Free: (877) 465-3004
e-mail
Representative_Jay_Ramras
@legis.state.ak.us
House District 10

House of Representatives

MEMO

To: Representative Lesil McGuire, Chair House Judiciary Committee

Fm: Jim Pound, Chief of Staff

Cc:

Date: March 17, 2005,

Re: Request for hearing of HB 205

Please accept this Memo as a request for the House Judiciary Committee to hear HB 205, "An Act relating to review of proposed regulatory actions and regulations, fiscal effect of proposed regulatory actions, and suspension of regulations." HB 205 will assure that future regulations promulgated by the Administrative Department's meet the intent of the law and are not overly burdensome on Alaskans.

Thank you in advance for scheduling HB 205 before the House Judiciary Committee.

Attachments: Sponsor Statement, HB 205, Sectional, statutory reference, Example of memos written regarding problems with regulations

Thank you

Representative Jay Ramras
Co-Chair, House Resources
V-Chair, Economic Develop.
Tourism & Trade
House State Affairs
119 N. Cushman St. Suite 207
Fairbanks, Alaska 99701
Phone: (907) 452-1088
Fax: (907) 452-1146

Alaska State Legislature

While in Session
State Capitol, Room 104
Juneau, Alaska 99801-1182
(907) 465- 3004
Fax: 465-2070
Toll Free: (877) 465-3004

House District 10

House of Representatives

Sponsor Statement

HB 205

"An Act relating to review of proposed regulatory actions and regulations, fiscal effect of proposed regulatory actions and suspension of regulations."

Everyday Alaskans are advised that they have broken a government rule. They often come to us in the legislature and ask for help with a problem created by their government, and want to know why lawmakers would every pass such law. The fact is, lawmakers didn't.

The Alaska Administrative Code is a set of rules conceived, promulgated, and enforced by the various administration departments. When the authority was first proposed by the legislature it was aimed at allowing the government to operate with part time legislators. At that time the agencies took statutory language and clarified it for their operational needs. Today, many times regulations do not conform to statute and often project a political agenda often in sharp contrast with the legislature.

HB 205 will return the Constitutional authority of lawmaking back to the legislature. It will not stop the writing of regulations but will require that the legislature through the Administrative Regulation Review Committee, review and not prevent their approval before taking effect.

The language further requires an accounting of the costs associated with regulations before they are implemented. The estimates include the department, and probably most importantly the public. Costs include living expenses, market competition, effects on employment, and must included short and long-term benefits or damages.

HB 205 is a major step towards bringing Alaska's Regulation system back under control of elected officials.

Representative_Jay_Ramras@legis.state.ak.us

Representative Jay Ramras
Co-Chair, House Resources
V-Chair, Economic Develop. Tourism & Trade
House State Affairs
119 N. Cushman St. Suite 207
Fairbanks, Alaska 99701
Phone: (907) 452-1088
Fax: (907) 452-1146

Alaska State Legislature

While in Session
State Capitol, Room 104
Juneau, Alaska 99801-1182
(907) 465- 3004
Fax: 465-2070
Toll Free: (877) 465-3004

House District 10

House of Representatives

Sectional

HB 205

"An Act relating to review of proposed regulatory actions and regulations, fiscal effect of proposed regulatory actions, and suspension of regulations."

Section 1

The additional language assures that the Department will provide a copy of proposed regulations by electronic means to a standing committee that oversees the subject of the regulations.

Section 2

Incorporates new language into AS 24.20.445(a) and represents the action language of the bill. Once the copies are provided to the Administrative Regulations Review Committee, the Committee may hold public hearings on the proposed regulation. If the Committee disapproves of the regulation it may by a majority vote, suspend the implementation of the regulation until after the end of the Legislative Session. The Committee must submit a bill annulling or invalidating the regulation. Failure by the body to pass that bill by the end of the session will allow the regulation to take effect.

Section 3

Provides language that requires the Committee to file a suspension resolution with the Lieutenant Governor's office in order for the suspension to take effect.

Section 4

This paragraph gives the Committee the opportunity to disapprove a proposed regulation within 35 days of receipt of the new proposals. Failure by the Committee to act is interrupted to mean approval by the Committee. A disapproval, may be returned to the Department with recommendations that may allow the regulation to be reviewed again and approved. The

Committee may review the proposed regulations on several different issues listed in Paragraph (1)- (5).
Paragraph 6 adds language that authorizes the Committee to review regulatory language , introduce legislation that will suspend, nullify or amend regulations

Section 5

Paragraph 8 will require a review of regulations submitted by the Lieutenant Governor to the Committee to determine if they should be suspended.

Section 6 assures that the Administrative Regulation Review Committee receives copies of all regulations, suspensions or revisions regardless on the distribution format.

Section 6

Requires the agency to provide an actual and accurate fiscal impact note, and how it will be funded, with the proposed regulation. It further requires the agency to submit the need for the regulation to include costs and benefits and why this is the most fiscally responsible way of accomplishing a goal. The fiscal information must take into account both the costs to the state and to the private sector including the cost of doing business and or the cost of living and employment effect by specific geographical region that may be affected by the regulation(s).

In addition to costs, the agency must determine its effect on competition, the environment and public health.

ALASKA STATE LEGISLATURE

Rep. Lesil McGuire, Chair
Sen. Robin Taylor, Vice-Chair
Sen. Lyda Green
Sen. Georgianna Lincoln
Rep. Jeannette James
Rep. Joe Hayes

State Capitol, Room 116
Juneau, AK 99801-1182
(907) 465-5446 fax: 465-6592
Interim
716 W. 4th Ave. Suite 430
Anchorage, AK 99501
(907) 269-0250fax: 269-0249

Administrative Regulation Review Committee

Memo

TO: Committee Members

FM:

Cc:

Date: May 1, 2002

RE: Response to 3/19/02 Department of Law memo

This memo is in response to G. Ken Truitt's, Esq. Memorandum 663-01-0113 of March 19, 2002. Mr. Truitt addressed various aspects of the regulatory process in relationship to the review process. In every aspect he discussed and referenced the Administrative Procedures Act[1]. I can appreciate his complete explanation of how regulations are supposed to be reviewed prior to being sent to the Lieutenant Governor for her *ministerial role of filing the regulations.*[2] Unfortunately, the members of this Committee are well aware that the review process, is sometime motivated by a political agenda, resulting in regulations that violate statute.[3] It is nice to know, assuming that Mr. Truitt will be the one reviewing the regulations, that there is a willingness to consider cites during that review. Based in part on that statement, this memo includes additional cites to be considered when reviewing the 04 AAC 33.

One of the most controversial sections of 04 AAC 33.421(d) & (3) allegedly is not under review. However, by virtue of publishing this section as part of the proposed regulations, it certainly is available for change. This section deals directly with the Establishment Clause of the United States Constitution. I agree that *Allen*[4] is an older case that has more than likely been eclipsed in some earlier rulings. However, in *Mitchell*[5], *Allen* is returned as an acceptable precedent. The Court further affirmed *Witters*[6] in *Mitchell*. *Mitchell* offers and interesting observation on the current makeup of the Court and how they rule regarding the Establishment

---

[1] AS 44.62.010-.300
[2] AG Opinion 663-92-0325
[3] 12 AAC 21.990(7) & 12 AAC 39.992(b) v. AS 08.18.171(D); AS 08.40.240(3) & AS 08.40.390(A)
[4] Board of Education v. Allen, 392 U.S. 236 (1968)
[5] Mitchell et al. v. Helms et al., 530 U.S. 793 (2000)
[6] Witters v. Wash. Dept. of Services for Blind, 474 U.S. 481 (1986)

Clause. 04 AAC 33.421(d) & (3) essentially bars districts from providing funding for material that might be considered to "advocate partisan, sectarian, or denominational doctrine.

In an unnumbered Department of Education and Early Development (DEED) Memorandum from Dr. Ed McLain to Representative Fred Dyson, dated March 8, 2002, these three words are defined using Merriam Webster's 3d. Unabridged Dictionary. While the U.S. Supreme Court has, on several occasions used this source for definitions, it is interesting to note that DEED's memo uses them as a sole source for definitions in a legal sense. A more common source, one that is considered citable to define legal terms is Black's Law Dictionary. It is important to point out the definitions are similar. Black's defines the terms this way:

Partisan: An adherent to a particular party or cause as opposed to the public interest at large.

Sectarian: Denominational; devoted to, peculiar to, pertaining to, or promotive of, the interest of a sect, or sects. In a broader sense, used to describe the activities of the followers of one faith as related to those of adherents of another. The term is most comprehensive in scope.

Denominational: Of, or pertaining to, a denomination; sectarian

With that background we again return the question of not paying for materials used by parents in correspondence education. The issue falls under three aspects of the Constitution: The Establishment Clause, Discrimination and Free Speech.

The U.S. Constitution States:

Amendment I - Freedom of Religion, Press, Expression. Ratified 12/15/1791.
Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.

Amendment IX - Construction of Constitution. Ratified 12/15/1791.

The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people.

Amendment XIV - Citizenship rights. Ratified 7/9/1868. Note History

1. All persons born or naturalized in the United States, and subject to the jurisdiction thereof, are citizens of the United States and of the State wherein they reside. No State shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws.

Likewise, Alaska's Constitution has similar language.

Section 1.1 - Inherent Rights.

This constitution is dedicated to the principles that all persons have a natural right to life, liberty, the pursuit of happiness, and the enjoyment of the rewards of their own industry; that all persons are equal and entitled to equal rights, opportunities, and protection under the law; and that all persons have corresponding obligations to the people and to the State.

Section 1.3 - Civil Rights.

No person is to be denied the enjoyment of any civil or political right because of race, color, creed, sex, or national origin. The legislature shall implement this section. [Amendment effective October 14, 1972]

Section 1.4 - Freedom of Religion.

No law shall be made respecting an establishment of religion, or prohibiting the free exercise thereof.

Section 1.5 - Freedom of Speech.

Every person may freely speak, write, and publish on all subjects, being responsible for the abuse of that right.

In *Good News Club*[7] The U.S. Supreme Court dealt with the use of a public school by a religious organization. The Court stated the two primary issues:

> This case presents two questions. The first question is whether Milford Central School violated the free speech rights of the Good News Club when it excluded the Club from meeting after hours at the school. The second question is whether any such violation is justified by Milfords concern that permitting the Clubs activities would violate the Establishment Clause. **We conclude that Milfords restriction violates the Clubs free speech rights and that no Establishment Clause concern justifies that violation.** (emphasis added)

The Court cited two other cases in the issue of free speech:

> ...we first address whether the exclusion constituted viewpoint discrimination. We are guided in our analysis by two of our prior opinions, *Lambs Chapel*[8] and *Rosenberger*[9]. In *Lambs Chapel*, we held

[7] Good News Club et al. v. Milford Central School et al., 531 U.S. 923 (2000)
[8] Lambs Chapel v. Center Moriches Union Free School Dist., 508 U.S. 384, 401 (1993)
[9] Rosenberger v. Rector and Visitors of Univ. of Va., 515 U.S. 819 (1995)

> that a school district violated the Free Speech Clause of the First Amendment when it excluded a private group from presenting films at the school based solely on the films discussions of family values from a religious perspective. Likewise, in *Rosenberger*, we held that a university's refusal to fund a student publication because the publication addressed issues from a religious perspective violated the Free Speech Clause. Concluding that Milfords exclusion of the Good News Club based on its religious nature is indistinguishable from the exclusions in these cases, we hold that the exclusion constitutes viewpoint discrimination.
>
> In *Rosenberger*, a student organization at the University of Virginia was denied funding for printing expenses because its publication, Wide Awake, offered a Christian viewpoint. Just as the Club emphasizes the role of Christianity in students morals and character, Wide Awake challenge[d] Christians to live, in word and deed, according to the faith they proclaim and encourage[d] students to consider what a personal relationship with Jesus Christ means. 515 U.S., at 826. Because the university select[ed] for disfavored treatment those student journalistic efforts with religious editorial viewpoints, we held that the denial of funding was unconstitutional. *Id.*, at 831.

In what is Known as the *Lemon*[10] Test The Supreme Court asks whether a statute (1) has a secular purpose, (2) has a primary effect of advancing or inhibiting religion, or (3) creates an excessive entanglement between government and religion.

Lemon can be applied to both the State and Federal Constitutions. It is also applicable to 04 AAC 33.421(d) which reads: *Certified Staff shall not advocate partisan, sectarian, or denominational doctrine as part of their instruction or duties as certified staff in the correspondence program.* This by itself is not a problem since the certified staff is only there to review what lessons are being learned in the required basics. However, the paragraph continues: *Nothing in this section prevents a parent from providing instruction to their child using materials of their choice, **provided such material was not purchased with program funds***. This sentence meets the first and the third questions in the *Lemon* test by preventing a secular purpose and excessive entanglement. On the other hand, it fails the second part of the test because it essentially inhibits religion. This same point could also be an issue under Section 1.4 - Freedom of Religion, Alaska State Constitution and the First Amendment of the U.S. Constitution. Both use the same language **"...prohibiting the free exercise thereof...."** (emphasis added) Paragraph (3) also fails the same test.

One of the issues presented to the Committee by the Department on March 1, was that distant school districts were receiving funds and then not using the full amount for the correspondent student, therefore diverting that money somewhere else within the local district. While the DEED considers this a problem, they freely allow it to happen by restricting that money discriminately to parents who chose to teach moral values and character. *Good News Club*,

[10] Lemon v. Kurtzman, 403 U.S. 602 (1971); 411 U.S. 192 (1973)

"([W]hen the subject matter is morals and character, it is quixotic to attempt a distinction between religious viewpoints and religious subject matters)...."

In *Mitchell* the court states:

> "In distinguishing between indoctrination that is attributable to the State and indoctrination that is not, we have consistently turned to the principle of neutrality, upholding aid that is offered to a broad range of groups or persons without regard to their religion. If the religious, irreligious, and a religious are all alike eligible for governmental aid, no one would conclude that any indoctrination that any particular recipient conducts has been done at the behest of the government. For attribution of indoctrination is a relative question. If the government is offering assistance to recipients who provide, so to speak, a broad range of indoctrination, the government itself is not thought responsible for any particular indoctrination. To put the point differently, if the government, seeking to further some legitimate secular purpose, offers aid on the same terms, without regard to religion, to all who adequately further that purpose, see *Allen*, 392 U. S., at 245-247 (discussing dual secular and religious purposes of religious schools), then it is fair to say that any aid going to a religious recipient only has the effect of furthering that secular purpose. The government, in crafting such an aid program, has had to conclude that a given level of aid is necessary to further that purpose among secular recipients and has provided no more than that same level to religious recipients."

It should be pointed out at that *Allen*, is the same case referenced in the first Committee memo and referenced by Mr. Truitt. Essentially, Section 4 AAC 431(d) & (3) restricts one group from receiving funds, to pay for a curriculum that in addition to teaching the Basics, enhances the child's growing and learning experience by teaching moral values and character.

Justice Scalia in *Good News Club* adds:

> I have previously written that [r]eligious expression cannot violate the Establishment Clause where it (1) is purely private.
>
> In *Rosenberger v. Rector* and *Visitors of Univ. of Va.*, 515 U.S. 819 (1995), we struck down a similar viewpoint restriction. There, a private student newspaper sought funding from a student-activity fund on the same basis as its secular counterparts. And though the paper printed such directly religious material as exhortations to belief, see *id.*, at 826 (quoting the papers self-described mission to encourage students to consider what a personal relationship with Jesus Christ means); *id.*, at 865 (Souter, J., dissenting) (The only way to salvation through Him is by confessing and repenting of sin. It is the Christians duty to make sinners aware of their need for salvation

> (quoting the paper)); see also *id.*, at 865867 (quoting other examples), we held that refusing to provide the funds discriminated on the basis of viewpoint, because the religious speech had been used to provid[e] a specific premise from which a variety of subjects may be discussed and considered, *id.*, at 831 (opinion of the Court). The right to present a viewpoint based on a religion premise carried with it the right to defend the premise.

In Conclusion:

The cases cited in this memo are only the tip of the iceberg. In February, The U.S. Supreme Court heard and is reviewing *Zelman et al. v. Simmons-Harris*, No. 00-1751, 1777, 1779. This will present a new review of the Establishment Clause. While I have not had time to completely read the 71 pages, the makeup of this Court has not changed since any of the cases cited here. Barring any surprise decision from the Court it appears that the cases referenced in this memo establish grounds to require the Department of Education to pass funding on to individual correspondence parents, to purchase educational material, even if those materials have some religious overtones. This is not to say that the State should be purchasing the Koran or Bible for these students. However, more than one parent in the correspondence program has pointed out that there are a lot of excellent curriculums from religious sources. I continue to feel that 04 AAC 421(d) and 04 AAC 421(3) makes it difficult if not impossible for some parents involved in the program to have the ability to chose an education tool that meets the needs of the family by virtue of the fact that the regulations as written forbid it.

If the Department resists, then the question must be asked about funding for the curriculum that is being used. Does it present a partisan position? We have all heard about schoolbooks with an agenda. To allow the State to pay for a partisan curriculum is just as bad, but that does not appear to be a problem.

The Department and the Board both need to review their policy and ask these questions:

Does it discriminate?
Currently it does, based on inhibiting religion and therefore discriminating against it.

Does it prevent Free Speech?
Currently it does, because a parent has made a choice to teach their children in a manner that includes family values, morals and character. This is as basic a right under free speech as any.

Does violate the Establishment Clause?
Yes. It violates the Clause by specifically restricting religious activities and education.

Based on these and other points to numerous to list in a memo I believe changes need to be made to the regulations:

04 AAC 33.405 (2) should read: students enrolled in such programs are public school students; **but because of the unique nature of their educational environment AS 14.03.090 may not apply.**

I also believe that paragraph (c),(d) and (3) need to be amended:

Paragraph c should read: The program must use curriculum materials, including textbooks and other instructional aids that have been reviewed [and selected] by the district school board,... And are in compliance with [AS 14.03.090 and] AS 14.18.060.

Sentence 2 of (d) should read: Nothing in this section prevents a parent from providing instruction to their child using materials of their choice. [provided such material was not purchased with program funds.]

Paragraph 3 should be deleted.

ALASKA STATE LEGISLATURE

Rep. Lesil McGuire, Chair
Sen. Robin Taylor, Vice Chair
Sen. Lyda Green
Sen. Georgianna Lincoln
Rep. Jeannette James
Rep. Joe Hayes

State Capitol, Room 116
Juneau, AK 99801-1182
(907) 465-5446 fax: 465-6592
Interim
716 W. 4th Ave. Suite 430
Anchorage, AK 99501
(907) 269-0250fax: 269-0249

Administrative Regulation Review Committee

Memo

To:

Fm:

Date: January 25, 2002

Re: Background, Mechanical Code

Since statehood the fire Marshall has traditionally used the Uniform Mechanical Code (U) (AS 18.70.080)1

The legislative process began on December 15, 1999, with the submission of the Governor's proposed budget with the Public Safety line item. That line item made it through the 2000 Legislative session and was signed in June or 2000.

Using those funds the Department of Public Safety moved forward to adopt the International Mechanical Codes (I). This involved coordination with local fire marshals so that the effort was generally organized.

Ross Fosberg was hired as a consultant in July, 2000

Public notices and public comments were sent out in November, 2000 with the comment period ending on January 31, 2001. Because of concerns from the Mechanical Contractors of Alaska, the Department reopened public comment from May 5 through June 8, 2001. As a result of comments some changes were made and the regulations took effect on September 15, 2001. All actions by the Department of Public Safety met and exceeded the requirements of statute.

The mechanical contractors filed suite against Commissioner Godfrey (PS) and Sedwick (DCED) on September 6, 2001. On November 23, 2001, The Contractors filed an application seeking a preliminary injunction to prevent the regulations from being implemented until the case was resolved.

The parties met before Judge Elaine Andrews, Superior Court on December 17, 2001, and the injunction motion was denied.

In late December the State moved for Summary Judgment seeking Dismissal. In mid January, the Contractors responded opposing and cross-moved for Summary Judgment challenging the Department's authority to adopt regulations. That is where the case stands today as the State is still within its timeline for response to the court.

Even with the court proceedings underway, in October, the Department of Commerce and Economic Development gave public notice that it intended to adopt the "I" code for the purposes of testing. This is where the department interpreted "Uniform Mechanical Code" to mean any code adopted by the Department of Public Safety. DCED cited AS 08.18.171, AS 08.40.230, .240, .270, .490, as the source of the decision.

Following the proper procedures the Department went through the public process (no public hearing) with written comments submitted by November 23, 2001.

The regulations were adopted on November 27, 2001 with an effective date of January 19, 2002.

Ballentines Legal Dictionary defines **Uniform** as an adjective meaning: consistent in pattern; unchanging; without variation, conforming to a standard. It goes on to include: compatible, habitual, homogeneous, equal, even, identical, constant, undeviating, conventional.

While this definition certainly gives the Department the ability to interpret the individual word generically, their decision does not take into account that the statute does not take Uniform as an individual word. Both the "Uniform Mechanical Code and the "International Mechanical Code" are propriety documents. I do not have copies in front of me, I am sure they are both copyrighted and suspect the names are registered.

My Conclusion and opinion: (I realize this may sound a little dramatic)

First I should point out, I do not believe this was the intent of the Department of Public Safety.****

The Administration, through DCED is making a stand against the Legislature using Separation of Powers. This vehicle is its best choice, because, the majority of the Department's decisions are made by boards, not under our control. A victory in this arena will ultimately mean that any word or group of words in statute means nothing more than what an attorney in a department says it means. Additionally, if we attack it using the appropriations process, the Knowles media will accuse the legislature of being anti-economic development. This puts the Legislature in a position of having to pass a repeal bill. It has never been successful before, but this may actually have the most potential, since it the most blatant case of interpretation I have seen.

As for the court case, based on the earlier decision in Anchorage, I do not think the contractors will prevail. The case is against both Departments and Public Safety is legal. I also believe the State can argue that the codes are similar enough that the Judge will rule in favor of the state. I do not believe she will rule on the Statute v. Regulation interpretation of Uniform as that is traditionally left to the Supremes. The Contractors will more than likely, not appeal.

THE HEARTLAND INSTITUTE
19 South LaSalle Street #903
Chicago, IL 60603
phone 312/377-4000 · fax 312/377-5000
http://www.heartland.org

Regulations Hamper Private Schooling Efforts in California

Author: Kate McGreevy
Published: The Heartland Institute 03/01/2005

California school choice advocates should consider shifting some of their resources away from the voucher movement to contest cumbersome regulations that affect the supply of private schooling in the Golden State, according to a recent report from the Reason Foundation. Even if demand-side reforms occurred and voucher programs were made operational, the low supply of private schools "would prevent those reforms from succeeding," the report concludes.

While demand for better schools--private, charter, and public--has been increasing, the supply has not kept up because of state-level regulatory barriers. The report posits current regulations "shift back the supply curve, keeping potential entrepreneurs out of the market, reducing the amount of new school capacity, and raising its price."

The December 2004 report, "Addition and Subtraction: State and Local Regulatory Obstacles to Opening a New Private School," provides an analysis of California's main regulatory hurdles and recommendations for improvement. The report was written by Bahaa Seireg, a George Mason University Ph.D. candidate.

Excessive Regulation Noted

The report provides compelling, if anecdotal, evidence in the form of three case studies.

In one example, Michael Leahy, founder of the Alsion Montessori Middle/High School, estimated the cost of his building should have been $400,000, but the total came to nearly $1.2 million because of several state regulations, "like the one requiring that he install a red tile roof."

"Children and parents want and need real educational choices," said Lisa Snell, the study's project director and director of education at the Reason Foundation. "But we aren't seeing more private schools because the government buries anyone interested in building a school under a mountain of needless regulations. The resulting lack of competition among private schools is fueling increases in private school tuition."

Reason's report identifies four main sources of regulation faced by those trying to open new schools:

- the State Environmental Quality Act (SEQA), which imposes barriers to land acquisition and modifications of structures on schools' land;
- city zoning requirements, which impose restrictions on where schools can be located;
- city parking requirements; and,
- state and local building codes, which impose restrictions on design and construction of school buildings.

Time, Money Wasted

According to Seireg, each regulation is potentially time-consuming, expensive, process-intensive, and "predicated on the city planner's belief that there is one best answer to all decisions about building."

SEQA, for example, requires a particularly lengthy process involving several land studies, all shouldered financially by the landowner, and an eventual public notice posting of a detailed Environmental Impact Report. Zoning regulations and enforcement processes are often prolonged, as well.

"The basic purpose of zoning regulations is to protect neighboring properties and owners from potentially adverse impacts of certain uses," says Geoffrey Goodfellow, planning director for Santa Clara, California. He adds the local public school district makes available closed school sites to private schools, and Santa Clara does not require a city review for the private use of these public buildings.

Even after years of working through the process, however, a permit application can be rejected because of the influence of a few local voices of opposition on decision-makers at a lead agency. This, says Seireg, makes the purchase of land for a private school "very risky."

Improvements Proposed

Seireg maintains that a performance planning approach to building regulation would improve the situation for private schooling. That approach, he said, gives landowners more flexibility to "use the land as they see fit," while remaining accountable for damages to the property.

"A performance planning approach focuses on end results rather than prescriptive policies," Seireg writes. He notes performance-based planning approaches have succeeded elsewhere.

"Performance standards that deal directly with actual and measurable impacts on the specific area would result in fewer regulations, less paperwork, a much simpler approval process, and ultimately, more schools," Snell stated.

Kate McGreevy (**mcgreevy@gmail.com**) *is a freelance education writer from Indiana. She formerly worked with the Cesar Chavez Public Charter High School for Public Policy in Washington, DC.*

For more information ...

The December 2004 report, "Addition and Subtraction: State and Local Regulatory Obstacles to Opening a New Private School," is available online at **http://www.rppi.org/ps329.pdf**.

FISCAL NOTE

STATE OF ALASKA
2005 LEGISLATIVE SESSION

Fiscal Note Number:
Bill Version: HB 205
() Publish Date:

Revision Date/Time (Note if correction):
Dept. Affected:
Title: Review and Suspension of Regulations
BRU: Alaska Court System
Component: Trial Courts
Sponsor: Representative Ramras
Requester:
Component No.: 768

Expenditures/Revenues (Thousands of Dollars)

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

OPERATING EXPENDITURES	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
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 (FY2005) 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)*
The court system does not anticipate any fiscal impact from the passage of HB 205.

Prepared by: Douglas Wooliver, Administrative Attorney — Phone 463-4750
Division: Alaska Court System — Date/Time 4/1/05 9:01 AM
Approved by: Doug Wooliver for Stephanie Cole, Administrative Director — Date 4/1/2005
Agency: Alaska Court System

(Revised 9/2002 OMB)

HB

210

HOUSE COMMITTEE REPORT

(7)
Date Referred to Committee: March 7, 2005 — FURTHER REFERRALS: Finance

Date of Committee Action: March 30, 2005

The JUDICIARY Committee considered: HB 210

HOUSE BILL NO. 210 — BLOODBORNE PATHOGEN TESTING

"An Act relating to blood testing of certain persons alleged to have committed certain offenses directed toward peace officers or emergency workers."

Recommends it be replaced with [ ] HCS *or* [X] CS for HB 210 (JUD)
For Senate Bills with new title: [ ] Technical Title [ ] New Title: HCR_____ [X] Same Title [ ] New Title

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

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

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

PREVIOUS FISCAL NOTES				
List by Dept(s):	FN#	Fiscal	Indet.	Zero

Signing with recommendations	Printed Last Name	DP	DNP	NR	AM
	Kott	–			
	Anderson	X			
		X			
	Gara	✓			
	Gruenberg	–			
Chair:	McGuire	X			
Chair:					

circumstances that are inconsistent with the intent required under (a) of this secti remain a resident of this state. (§ 1 ch 67 SLA 1983)

NOTES TO DECISIONS

Jurisdiction over divorce action. — This section does not affect the common-law rule that Alaska courts have jurisdiction over a divorce action wh... one of the parties is domiciled in Alaska, where "domicile" is defined as physical presence plus an intent to remain permanently. Perito v. Perito, 756 P.2d 895 (Alaska 1988).

Quoted in E.H. v. State, 23 P.3d 1186 (... 2001).

Stated in State v. Andrade, 23 P.3d 58 (... 2001).

Sec. 01.10.060. Definitions. (a) In the laws of the state, unless the context othe requires,

(1) "action" includes any matter or proceeding in a court, civil or criminal;

(2) "daytime" means the period between sunrise and sunset;

(3) "month" means a calendar month unless otherwise expressed;

(4) "municipality" means a political subdivision incorporated under the laws o state that is a home rule or general law city, a home rule or general law borough, unified municipality;

(5) "nighttime" means the period between sunset and sunrise;

(6) "oath" includes affirmation or declaration;

(7) "peace officer" means

(A) an officer of the state troopers;

(B) a member of the police force of a municipality;

(C) a village public safety officer;

(D) a regional public safety officer;

(E) a United States marshal or deputy marshal; and

(F) an officer whose duty it is to enforce and preserve the public peace;

(8) "person" includes a corporation, company, partnership, firm, association, orga tion, business trust, or society, as well as a natural person;

(9) "personal property" includes money, goods, chattels, things in action, and evide of debt;

(10) "property" includes real and personal property;

(11) "real property" is coextensive with land, tenements, and hereditaments;

(12) "signature" or "subscription" includes the mark of a person who cannot write, the name of that person written near the mark by a witness who writes the witness's name near the name of the person who cannot write; but a signature or subscriptio mark can be acknowledged or can serve as a signature or subscription to a sw statement only when two witnesses so sign their own names to the sworn statemen

(13) "state" means the State of Alaska unless applied to the different parts of United States and in the latter case it includes the District of Columbia and territories;

(14) "writing" includes printing.

(b) In the laws of the state, "lewd conduct," "lewd touching," "immoral condu "indecent conduct," and similar terms do not include the act of a woman breast-feedi child in a public or private location where the woman and child are otherwise authori to be. Nothing in this subsection may be construed to authorize an act that is an offe under AS 11.61.123. (§ 4 ch 62 SLA 1962; am § 2 ch 66 SLA 1965; am § 10 ch 117 S 1968; am § 19 ch 74 SLA 1985; am § 1 ch 60 SLA 1990; am § 2 ch 78 SLA 1998; am ch 97 SLA 2001)

Revisor's notes. — Reorganized in 1985 to alphabetize the defined terms.

Cross references. — For additional definition of "peace officer", see AS 11.81.900(b); for listing of p officers for purposes of the Fish and Game Code, AS 16.05.150; for a definition of "police officer", see

ALASKA STATE LEGISLATURE

Session
State Capitol Building, Room 118
Juneau, Alaska 99801-1182
Phone (907) 465-2995
Fax (907) 465-6592

Interim
716 West Fourth Avenue, Suite 430
Anchorage, Alaska 99501
Phone (907) 269-0250
Fax (907) 269-0249

REPRESENTATIVE LESIL MCGUIRE
HOUSE DISTRICT 28

Chair
Judiciary Committee

Member
House Leadership
Rules Committee
Health, Education & Social Services Committee
Oil & Gas Committee
Military & Veterans' Affairs Committee

SPONSOR STATEMENT
HB 210

"An Act relating to blood testing of certain persons alleged to have committed certain offenses directed toward peace officers or emergency workers."

HB 210 takes policies and procedures for testing for blood born pathogen exposure to correctional officers that were passed by the 23rd Alaskan Legislature and expands them to include peace officers, firefighters, emergency medical technicians and mobile paramedics.

The bill first sets out procedures for determining if the first responders were exposed to blood born pathogens in the course of their work. Once it is reasonably concluded that such exposure has occurred, the bill then sets our procedures for obtaining the consent of the person who exposed the first responder to have his or her blood tested. These procedures protect the identity of the person tested and pass on only the results of the test to the first responder exposed to the blood born pathogens. The results of the test are also passed on to the person tested.

The bill also provides procedures for court ordered testing of the person who exposed the first responder to blood born pathogens if that person refuses to be tested. The bill does not enact any new policies or procedures for blood born pathogen testing, it simply extends the policies and procedures enacted by the 23rd Alaskan Legislature for correctional officers to the other first responders mentioned above.

FISCAL NOTE

STATE OF ALASKA
2004 LEGISLATIVE SESSION

Fiscal Note Number:
Bill Version: HB 210
() Publish Date:

Revision Date/Time (Note if correction):
Dept. Affected: Corrections
Title "An act relating to blood testing of certain persons alleged to have committed certain offenses directed ...."
RDU: Administration & Operations
Component: Inmate Health Care
Sponsor: Representative McGuire
Requester: Judiciary, Finance
Component No.: 705

Expenditures/Revenues (Thousands of Dollars)

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

OPERATING EXPENDITURES	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010
Personal Services	0.0	0.0	0.0	0.0	0.0	0.0
Travel	0.0	0.0	0.0	0.0	0.0	0.0
Contractual	0.0	0.0	0.0	0.0	0.0	0.0
Supplies	0.0	0.0	0.0	0.0	0.0	0.0
Equipment	0.0	0.0	0.0	0.0	0.0	0.0
Land & Structures	0.0	0.0	0.0	0.0	0.0	0.0
Grants & Claims	0.0	0.0	0.0	0.0	0.0	0.0
Miscellaneous	0.0	0.0	0.0	0.0	0.0	0.0
TOTAL OPERATING	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**
CAPITAL EXPENDITURES	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**
CHANGE IN REVENUES ( )	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**

FUND SOURCE (Thousands of Dollars)

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

Estimate of any current year (FY2004) cost: 0.0
Mark this box (X) if funding for this bill is included in the Governor's FY 2005 budget proposal:

POSITIONS

Full-time	0	0	0	0	0	0
Part-time	0	0	0	0	0	0
Temporary	0	0	0	0	0	0

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

This legislation expands Ch 142, SLA 04, HCS CSSB 309 (JUD) to include other "public safety officers from other public safety agencies and exposure from juvenile offenders".

The Department of Corrections does not anticipate a significant fiscal impact with the passage of this legislation.

Prepared by: Sharleen Griffin, Acting Director
Phone: (907) 465-4647
Division: Administrative Services
Date/Time: 3/28/05 9:39 AM
Approved by: Portia C. K. Parker, Deputy Commissioner
Date: 3/28/2005
Agency: Department of Corrections

(Revised 9/2003 OMB)

FISCAL NOTE

STATE OF ALASKA
2005 LEGISLATIVE SESSION

Fiscal Note Number:
Bill Version: HB 210
() Publish Date:

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

Title: Bloodborne Pathogen Testing
BRU: Alaska Court System
Component: Trial Courts

Sponsor: McGuire
Requester:
Component No.: 768

Expenditures/Revenues (Thousands of Dollars)

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

OPERATING EXPENDITURES	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
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 (FY2005) 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)*

The court system does not anticipate any fiscal impact from the passage of HB 210.

Prepared by: Douglas Wooliver, Administrative Attorney
Phone: 463-4750
Division: Alaska Court System
Date/Time: 3/24/05 9:12 AM

Approved by: Doug Wooliver for Stephanie Cole, Administrative Director
Date: 3/24/2005
Agency: Alaska Court System

(Revised 9/2002 OMB)

FISCAL NOTE

STATE OF ALASKA
2005 LEGISLATIVE SESSION

Fiscal Note Number:
Bill Version: HB210-LAW-CDCO-3-29
() Publish Date:

Revision Date/Time (Note if correction):
Dept. Affected: LAW
Title "An Act relating to blood testing of certain persons alleged to have committed certain offenses..."
RDU CRIMINAL
Component Criminal Justice Litigation
Sponsor Representative McGuire
Requester House Judiciary
Component No.

Expenditures/Revenues (Thousands of Dollars)

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

OPERATING EXPENDITURES	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
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 (FY2005) 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)*

This bill amends AS 18.15.400 (Health, Safety, and Housing - Disease Control - Blood Testing of Prisoners for Bloodborne Pathogens) by broadening it to include all peace officers and emergency workers who may have exposure to offenders with blood borne pathogens. The current statute protects correctional officers from exposure to prisoners. This bill would also extend beyond prisoners, to any adult or juvenile offender whether incarcerated or not. The bill seeks to acknowledge that the risk of exposure to blood born pathogens is significant for all peace officers and the ability to test blood to identify where and when medical treatment might be needed is an important protection measure.

Passage of this legislation will have no fiscal impact on the Department of Law.

Prepared by: Kathryn Daughhetee, Director
Phone 465-3673
Division Administrative Services Division
Date/Time 3/29/05 4:18 PM
Approved by: K. Daughhetee for Scott Nordstrand, Acting Attorney General
Date 3/29/2005
Agency Department of Law

FISCAL NOTE

STATE OF ALASKA
2005 LEGISLATIVE SESSION

Fiscal Note Number:
Bill Version: HB210-DPS-ASTD-3-30-05
() Publish Date:

Revision Date/Time (Note if correction):
Dept. Affected: Public Safety
Title: "An Act relating to blood testing of certain persons alleged to have committed cerain offenses."
RDU: Alaska State Troopers
Component: AST Detachments
Sponsor: Rep. McGuire
Requester: House Judiciary
Component No: 2325

Expenditures/Revenues (Thousands of Dollars)

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

OPERATING EXPENDITURES	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
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 (FY2005) 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)*

This bill amends AS 18.15.400 -18.15.450. Peace officers, fire fighters, emergency medical technicians, mobile intensive care paramedics employed or volunteering for the state or municipality, a volunteer department or emergency medical service provider will be able to request bloodborne pathogen testing when they have been exposed to blood or body fluids during the performance of their duties. The bill will now allow bloodborne testing of certain adult or juvenile offenders in addition to prisoners. The "employing agency" is responsible for insuring the testing procedures are followed correctly. Passage of this bill will have no immediate fiscal impact on the Department of Public Safety, and simply outlines the proper course of action when personnel are exposed to blood or body fluids. DPS has a policy for reporting this kind of exposure.

Prepared by: Lieutenant Todd Sharp
Phone: 907-465-3423
Division: Alaska State Troopers
Date/Time: 3/30/05 12 01 PM
Approved by: Commissioner William Tandeske
Date: 3/30/2005
Agency: Department of Public Safety

HB

219

HOUSE COMMITTEE REPO T

(7)
Date Referred to Committee: March 15, 2005 **FURTHER REFERRALS: Finance**

Date of Committee Action: March 23, 2005

The JUDICIARY Committee considered: **HB 219**

HOUSE BILL NO. 219 **STRANGULATION CRIMES**

"An Act relating to crimes and dangerous instruments."

Recommends it be replaced with [ ] HCS *or* [ ] CS *for* _____(_____)
For Senate Bills with new title: [ ] Technical Title [ ] New Title: HCR_____ **[ ] Same Title [ ] New Title**

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

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

NEW FISCAL NOTES
*Assigned by Chief Clerk's Office

List by Dept(s):	*FN#	Fiscal	Indet.	Zero
CRT				✓
LAW				✓
DPS				✓
ADM			✓	

PREVIOUS FISCAL NOTES

List by Dept(s):	FN#	Fiscal	Indet.	Zero

Signing with recommendations	Printed Last Name	DP	DNP	NR	AM
	Gruenberg	–			
	Scott	–			
	Gara	–			
	Dahlstrom	X			
Chair:	McGuire	✓			
Chair:					

24-LS0582\G.1
Luckhaupt
3/21/05

not offered

AMENDMENT

OFFERED IN THE HOUSE BY REPRESENTATIVE

TO: HB 219

Page 1, line 1:

Delete "**crimes and dangerous instruments**"

Insert "**the definition of 'dangerous instrument' as applied within the criminal code**"

Municipality of Anchorage

4501 Brigaw Street • Anchorage, Alaska 99507-1599 • Telephone (907) 786-8500 • http://www.muni.org

Mayor Mark Begich

Anchorage Police Department

March 17, 2005

Representative Mike Hawker
State Capitol, Room 434
Juneau, AK 99801-1182

Dear Representative Hawker,

I understand that a bill regarding strangulation has been introduced to the House of Representatives. Several of our Department members have been conferring with Tara Henry about what is being proposed. I would like to provide support for the passing of this bill.

The State of Alaska faces multiple challenges in combating the elevated rate of crimes involving sexual assault and domestic violence. All too often, we learn that some form of strangulation occurred during the commission of these crimes. Individuals who perpetrate this type of violence against another person are using it as the ultimate form of control. Through the use of one's hands or another object to impede normal breathing or circulation, they are sending a message to the victim that they control their life.

In recent years, we are becoming more aware of the prevalence of strangulation as well as the extreme danger associated. The Anchorage Police Department has proactively responded to this information by educating all of our officers about how to recognize and respond to these incidents. An imperative part of this response package involves the prosecution of those who perpetrate these crimes. The proposed change in statute regarding the definition of dangerous instrument would add greatly to the ease of both charging and prosecuting these suspects.

I appreciate your willingness to carry this through. If you require any assistance from the Anchorage Police Department, please don't hesitate to call me personally.

Sincerely,

Walt Monegan
Chief of Police

WM/ga

From: lisa rea [lisadrew@alaska.com]
Sent: Tuesday, March 22, 2005 7:54 AM
To: Juli Lucky
Subject: Strangulation bill

Representative Hawker,

As a resident of Anchorage, a Public Health Nurse and a Sexual Assault Nurse Examiner I want to thank you for your support of house bill 219, strengthening the statutes to increase strangulation from a misdemeanor to a felony. This bill is an opportunity to recognize the seriousness of strangulation. If you have any questions about why I support this I can be reached at 349-9941.

Thank you
Lisa Rea, RN

Forensic Nurses Association of Alaska
PO Box 771633
Eagle River, Alaska 99577

February 4, 2005

To Whom It May Concern:

The Forensic Nurses Association of Alaska supports the proposed statutory changes to include strangulation as a felony assault. Strangulation is a very serious, sometimes fatal physical assault that is commonly seen in domestic violence and sexual assault cases. When a person is being strangled, they are at a substantial risk for death. The victim becomes unconscious within seconds and death can occur within minutes.

It is well documented in the latest research that strangulation is one of the top five risk factors for a domestic violence homicide. Women who are strangled by an intimate partner are at a 9.9 times higher risk for being murdered by their partner than other women.

The State of Alaska leads the nation in the number of domestic violence homicides per capita. The proposed statutory changes that will include strangulation as a felony assault is a proactive approach to preventing domestic violence homicides, and is desperately needed in our state. In addition, the proposed changes will finally address this life threatening assault at the level of seriousness that it is.

The Forensic Nurses Association of Alaska fully supports and encourages this statutory change.

Sincerely,

Carol Odinzoff RN

Carol Odinzoff, RN
President
Forensic Nurses Association of Alaska

Representing Alaska's Finest
Alaska State Troopers, State Fire Marshals, Court Service Officers, Airport Police and Fire Officers, Juneau Police, Unalaska Police, Sitka Police, Fairbanks Police, Ketchikan Police, and the Soldotna Police

Political Action Committee

March 16, 2005

Representative Mike Hawker
State Capitol, Room 502
Juneau, AK 99801-1182

Re: HB 219

Dear Representative Hawker,

On behalf of the members of PSEA, I would like to thank for introducing HB 219. We believe HB 219 brings about a much-needed amendment to better define the criteria of what is a "dangerous instrument".

As a representative of Alaska's law enforcement officers, it is imperative that we have the necessary tools to ensure that Alaska's citizens are adequately protected. HB 219 will better assist law enforcement with the prosecution for those individuals who have committed such a horrendous assault.

PSEA hopes that the legislature will act swiftly on this matter and pass HB 219.

Sincerely,

Maurice I. Hughes Jr.
PSEA Vice President

4300 Boniface Parkway, Suite 116, Anchorage, Alaska 99504
Phone (907) 337-1979 Fax (907) 337-1753

Anchorage Police Department Employees Association

Phone (907) 561-7500
P.O. Box 230330
Anchorage, Alaska 99523
500 West International Airport Road
Anchorage, Alaska
www.apdea.org

March 17, 2005

Re: HB 219

Dear Legislative Body:

The Anchorage Police Department Employees Association represents rank-and-file police employees in the Anchorage Police Department. I am writing to express the APDEA's full support for HB 219. There is presently an ambiguity in the law that has led to uncertainty by prosecutors as to how to charge the crime of strangulation. Unfortunately, this ambiguity has led to some of those who have committed this potentially life-threatening crime to receive lesser sentences than would otherwise be appropriate. HB 219 brings much needed clarity to this area.

I look forward to answering any questions you may have about HB 219.

Sincerely,

Michael Coutu[illegible]
APDEA Vice President

Juli Lucky

From: Natasha Norris [Natasha_Norris@law.state.ak.us]
Sent: Monday, March 21, 2005 11:17 AM
To: Juli Lucky
Subject: Strangulation bill

Ms. Lucky:

I am writing this email in support of House Bill No. 219. I have been a proscutor for almost four years in the State of Alaska. I worked in Sitka, Alaska as the only State prosecutor, for two and half years.
While at the Sitka post, I dealt with several strangulation cases.
There are a couple of things regarding strangulation that are striking.
First, strangulation occurs in many domestic violence situations.
Often, when speaking to a victim of domestic violence, they disclose that although strangulation may not have occurred the incident leading to arrest, they have at one point or another, suffered strangulation at the hands of their boyfriend or husband. Second, because of the lethality of strangulation, ANYTIME a defendant uses their hands to block normal breathing causes a substantial risk of death or serious physical injury. The law now requires that before hands can be a "dangerous instrument", an expert needs to testify that the hands were used in a way that caused a substantial risk of death or serious physical injury. Given what we know about domestic violence and the lethality of strangulation, the definition of dangerous instrument should include the use of hands or other objects to strangle without the need for experts to testify to the lethality of strangulation. For the sake of victims, I hope House Bill No. 219 passes.

Sincerely,
Natasha Norris

Representative Mike Hawker
Alaska State Legislature

Session:
State Capitol
Juneau, AK 99801
907 465-4949 direct
800 478-4950 toll free
907 465-4979 fax

Interim
716 W 4th Avenue
Anchorage, AK 99501
907 269-0244 office
907 269-0248 fax

Member:
House Finance Committee
Legislative Budget
& Audit Committee

House District 32
Eagle River
Anchorage
Rainbow
Indian
Bird
Girdwood
Portage
Whittier
Sunrise
Hope

To: Representative Lesil McGuire
Chairman, House Judiciary Committee

From: Representative Mike Hawker

Date: March 15, 2005

Re: House Bill 219

I request that HB 219, which would specifically permit felony prosecution for an assault involving strangulation or suffocation, be scheduled for the House Judiciary Committee at your earliest possible convenience.

Strangulation can cause life-threatening injuries without obvious external marks that can be presented to a jury as evidence of "serious physical injury." Without visible injuries, many cases are tried as misdemeanors, even if the victim was minutes from death. HB 219 would ensure that these cases can be prosecuted as felonies.

HB 219 is supported by the Office of Victims' Rights, Forensic Nurses' Association of Alaska, Public Safety Employees' Association, and the Anchorage Police Department Employees' Association. The Department of Law has seen and approved the proposed statutory change.

Please feel free to contact me if you need any additional information. You may also contact my legislative aide, Juli Lucky.

Representative Mike Hawker
Alaska State Legislature

Session
State Capitol
Juneau, AK 99801
907 465-4949 direct
800 478-4950 toll free
907 465-4979 fax

Interim
716 W 4th Avenue
Anchorage, AK 99501
907 269-0244 office
907 269-0248 fax

Member
House Finance Committee
Legislative Budget
& Audit Committee

House District 32
Eagle River
Anchorage
Rainbow
Indian
Bird
Girdwood
Portage
Whittier
Sunrise
Hope

House Bill 219
Sponsor Statement

"An Act relating to crimes and dangerous instruments."

House Bill 219 specifically permits felony prosecution for an assault involving strangulation or suffocation. Strangulation is one of the top five risk factors for domestic violence homicide and is the cause of ten percent of homicide deaths in the United States. Yet, many cases have not been prosecuted as felonies due to physical evidence requirements that may not be relevant in strangulation assaults.

Strangulation can cause life-threatening injuries without obvious external marks that can be photographed and presented to a jury as evidence of "serious physical injury," which is required by current statute for felony assault. Forensic science proves that even in some fatal cases of strangulation there is no external evidence of injury. The cause of death was determined during autopsy, when the chance to photograph and collect untainted evidence had passed.

Without visible injuries, many cases are tried as misdemeanors even though the victim was minutes from death. Unconsciousness can occur within ten seconds, followed closely by irreversible brain damage and death within five minutes. Lack of oxygen can also cause internal injuries, including brain damage, which can lead to death hours, days or even weeks after the crime.

When strangulation occurs in a domestic relationship, it is indicative of a high level of violence within the relationship. In recent years, strangulation has been identified as one of the most lethal forms of domestic violence – a domestic violence victim who has been strangled is nine times more likely to be killed than one who has not.

This bill recognizes strangulation as a serious life threatening assault warranting felony prosecution. I urge your support.

Columbus Dispatch (Ohio)

August 14, 2004 Saturday

Strangulation Cases; Seminar Explores Details Overlooked in Investigations

By Alayna DeMartini, *Columbus Dispatch*

The man called 911 with an odd complaint.

"She won't die," he told the dispatcher. "I've tried to kill her four different ways. She won't die."

But when medics arrived at the couple's home they found that the man had succeeded in strangling his wife.

The call to a 911 operator in Las Vegas was played yesterday for central Ohio police officers, prosecutors and emergency personnel during a training session on recognizing and prosecuting strangulation and attempted strangulation cases.

Too often the assailant walks away with little or no punishment because there aren't always marks left on the victim, said Gael B. Strack, a San Diego city attorney who led yesterday's seminar at the Franklin County Courthouse.

The victim may have serious injuries that aren't always apparent, such as internal fractures in the throat, Strack said.

"We understand when someone's stabbed, when their lip is cut, because we can see the signs," Strack said. "With strangulation, most victims will have internal injuries. It's easy to overlook, minimize or trivialize."

A study by the San Diego city attorney's office of police reports showed that if there was no visible sign of attempted strangulation, the assailant wasn't charged with a serious crime.

"We didn't understand what we had in front of us," Strack said.

The study, conducted in the late 1990s, showed that police often neglected to clearly document what symptoms victims were experiencing, Strack said. Cases that were prosecuted were charged as misdemeanors when many could have been felonies, Strack said.

Franklin County prosecutors estimate that 30 percent to 40 percent of the annual 6,000 domestic-violence cases in the county involve choking or strangulation, said Leslie Ashworth, director of the Columbus city attorney's domestic-violence unit.

Typically, victims of attempted strangulation will have red marks on the neck and a raspy voice, Ashworth said.

However, victims sometimes refuse to be treated at a hospital because they can't afford it, Ashworth said.

"Then you lose the evidence," Ashworth said.

Even when victims go to hospitals, they often minimize their injuries and do not blame them on others.

"The important thing is for everyone to realize that it's a potentially life-threatening matter and not say 'Oh, they were just choked,'" Ashworth said.

In Ohio, someone who tries to strangle a mate could be charged with domestic violence, which is a misdemeanor, or a felony such as felonious assault.

Some states have recently stepped up their domestic-violence laws and the penalties for strangulation attempts.

On Thursday, North Carolina Gov. Mike Easley signed legislation, "assault inflicting serious physical injury by (attempted) strangulation," a felony punishable by up to two years in prison.

An Oklahoma law that goes into effect in November makes it a felony to commit attempted strangulation on a domestic partner.

ademartini@dispatch.com

OPDV Bulletin:
Strangulation in Domestic Violence and Sexual Assault

"He choked me– but there are no marks."

In 1999, the Clinton County District Attorney's Office and the New York Prosecutors Training Institute (NYPTI) hosted the nation's leading experts in the prosecution and investigation of strangulation cases. Assistant District Attorney Gael Strack and George M. Clane, MD, both from San Diego, California, presented their findings at the three-day conference, "Detection and Prosecution of Strangulation in Domestic Violence and Sexual Assault Cases," funded by the US Department of Justice Violence Against Women Grants Office and the New York State Division of Criminal Justice Services. The following is adapted from a condensed portion of their presentation.

"He choked me - but there are no marks." Strangulation has only recently been identified as one of the most lethal forms of domestic violence. When perpetrators use strangulation to silence their victims, this is a form of power and control that has a devastating psychological effect on victims and a potentially fatal outcome. Historically, "choking" was rarely prosecuted as a serious offense because victims minimize the level of violence and police and medical personnel fail to recognize it.

Strangulation is defined as a form of asphyxia and is characterized by closure of the blood vessels and/or air passages of the neck as a result of external pressure on the neck. It is often incorrectly referred to as choking which involves blocking, or obstructing the windpipe. Ten percent of violent deaths in the US each year are due to strangulation, with six female victims to every male.

Strangulation by ligature is done with a cord like object that could include anything from a telephone cord to articles of clothing. Manual strangulation is done with the hands, forearms (as in the classic chokehold), or standing or kneeling on the victim's throat.

Clinically, a victim who is being strangled first experiences severe pain, followed by unconsciousness, and then brain death. The victim will lose consciousness by any one or more of the following: blocking of the carotid arteries (depriving the brain of oxygen), blocking of the jugular veins (preventing deoxygenated blood from exiting the brain), and/or closing off the airway, causing the victim to be unable to breathe. Only eleven pounds of pressure placed upon both carotid arteries for ten seconds is necessary to cause unconsciousness. If pressure is released immediately, consciousness will be regained within ten seconds. After 50 seconds of continuous oxygen deprivation the victim rarely recovers. To completely close off the trachea, three times as much pressure (33 lbs.) is required. For comparison purposes, it only takes 8 lbs. of pressure to pull a trigger on a gun.

Fifty percent of victims report symptomatic voice changes which may be as mild as simple hoarseness or a complete loss of voice. Many victims also report that it is difficult or painful to swallow. This is due to injury of the larynx cartilage and/or hyoid bone, a small horseshoe shaped bone in the neck. Difficulty getting a breath may be due to the hyperventilation that normally accompanies a terrifying event, but more importantly may be secondary to underlying neck injury. It is critical to know that breathing changes may initially appear to be mild, yet underlying injuries may kill the victim hours or days later due to decompensation of the injured structures. Involuntary urination and defecation often occurs. Officers

should inquire about such because victims may be embarrassed and reluctant to disclose these facts unless asked.

Visible injuries to the neck may include scratches, abrasions, and scrapes. Redness on the neck may be fleeting, but may demonstrate a detectable pattern. These marks may or may not darken to become a bruise. Bruises may not appear for hours or even days. Chin abrasions are also common, as are tiny red spots called petechiae. These are caused by ruptured capillaries and may be found around the eyes, under the eyelids, anywhere on the face, and on the neck above the area of constriction. Blood red eyes are due to capillary rupture in the white portion of the eyes. This phenomenon suggests a particularly vigorous struggle between the victim and assailant.

In 70 to 80 percent of all domestic violence cases, the victim will recant. Therefore law enforcement should anticipate this and plan on prosecution based on the evidence, just like in a murder case. Efforts should be made to investigate the cases like an attempted homicide case. It is important to ask as many questions as possible at the earliest time possible. For specific questions and checklists to assist in detecting and investigating strangulation cases, go to http://www.correctionhistory.org/northcountry/html/knowlaw/strangulationinvestigation3.htm.

Condensed by NYPTI, (518) 432-1100, the Continuing Legal Education and Mutual Assistance Division of the New York State District Attorneys Association. The points of view or opinions stated in this article are those of the particular author and do not represent the official position of the NYS Division of Criminal Justice Services. Information dealing with a specific legal matter should be researched in original and current sources of authority.

Note to Officers and Prosecutors: Treat Your Strangulation Cases Seriously

Start by using the word "strangle" as opposed to the word "choke." Strangle means to obstruct seriously or fatally the normal breathing of a person. Choke means having the windpipe blocked entirely or partly by some foreign object like food.

"How to Improve Your Investigation and Prosecution of Strangulation Cases" by Gael B. Strack, San Diego Assistant City Attorney and Dr. George McClane, Emergency Physician, October 1998, updated May 1999 is an excellent article. It can be obtained by request from Gael B. Strack at: Gael B. Strack at

Know the Law: Resource Materials on Strangulation

Strangulation Conference

On September 28-30, 1999, the Clinton County District Attorney's Office and the New York Prosecutor's Training Institute sponsored a conference on **Detection and Prosecution of Strangulation in Domestic Violence and Sexual Assault Cases.** Funding was provided by the United States Department of Justice Violence Against Women Grants Office and the New York State Division of Criminal Justice Services.

The leading experts on this subject, Assistant City Attorney Gael Strack of the San Diego City Attorney's Office and George E. McClane, M.D., Emergency Physician at Sharp Health Care in San Diego, came to Plattsburgh and conducted three days of training for more than 350 physicians, nurses, emergency responders, law enforcement, prosecutors, case workers and others

"Strangulation" refers to the behavior of one person placing one or two hands around the neck of another person and squeezing or applying other pressure. This can kill.

We presented training on detecting and prosecuting strangulation because, in reviewing the Domestic Incident Reports (DIRs) filed by the police and interviewing victims, we repeatedly came across descriptions of the incident that included the complainant being choked - hands put on her throat, sometimes until she passed out! There might have been other physical violence, as well, sometimes not.

In examining this more closely, we found that in about 10% of the DIRs, choking was part of the specific incident. Reports made to the STOP Domestic Violence program by women, about 40% described "choking" as part of the abusive conduct at one or more points in their relationship.

Despite this frequency, rarely was there an arrest for the choking behavior. Seldom were there any marks or visible injuries seen by the police, and the victims themselves often described the choking aspect as minor in relation to the other violence used against them.

In New York, a person cannot be charged with criminal assault unless "physical injury" is actually caused. That is defined in the Penal Law as "impairment of physical condition or substantial pain." The choking cases did not really seem to meet this standard; it was understandable that the police did not make an arrest.

But, we wondered whether there were internal injuries caused by being choked - strangled - that did not leave outward visible signs. Or maybe the signs were there, but we did not know what to look for.

In our search for more information, we found some people around the state asking the same things, but no real answers. Eventually, through an internet search, we made progress. When the key word was "choking," it brought articles about medical conditions or choking on food. "Strangulation" first led to some guy's personal web page that suggested the sexual benefits of that conduct!

In refining the search to "manual strangulation," we came up with articles by pathologists, describing the evidence of strangulation found during autopsies. Hoping for someone who could identify such signs in living people who had been strangled, we pressed on and learned of Gael Strack and Dr. George McClane in San Diego.

We learned that they struggled with the same kinds of problems a couple of years earlier in S n Diego, in cases that started with what looked like minor abuse, including choking, and led to homicide. As a consequence, they taught themselves and other law enforcement and medical personnel what to look for to detect whether injury was caused.

As a prosecutor, I know that I can only be effective if there is a good investigation. I depend upon the police, the EMTs, the nurses and doctors for the evidence I use in court.

We now realize that we may be overlooking serious crimes, because we did not know what to look for. The frequency with which manual strangulation is used in domestic violence incidents is surprising: in San Diego, in Plattsburgh, and very likely, everywhere else.

Because we all see it but have not known how to deal with it, we brought the experts from San Diego to train us. We want to learn how to better do our jobs; how to better protect our community.

The three days of training were outstanding - all we hoped for and more. The presentations of Gael Strack and Dr. Geroge McClane are summarized in the New York Prosecutors Training Institute Newsletter which follows.

FISCAL NOTE

STATE OF ALASKA
2005 LEGISLATIVE SESSION

Fiscal Note Number:
Bill Version: HB 219
() Publish Date:

Revision Date/Time (Note if correction):
Dept. Affected:
Title: Strangulation Crimes
BRU: Alaska Court System
Component: Trial Courts
Sponsor: Representative Hawker
Requester:
Component No: 768

Expenditures/Revenues (Thousands of Dollars)

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

OPERATING EXPENDITURES	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
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 (FY2005) 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)*

The court system does not anticipate any fiscal impact from the passage of HB 219

Prepared by: Douglas Wooliver, Administrative Attorney
Phone: 463-4750
Division: Alaska Court System
Date/Time: 3/17/05 3:12 PM
Approved by: Doug Wooliver for Stephanie Cole, Administrative Director
Date: 3/17/2005
Agency: Alaska Court System

(Revised 9/2002 OMB)

FISCAL NOTE

STATE OF ALASKA
2005 LEGISLATIVE SESSION

Fiscal Note Number:
Bill Version: HB219-DPS-ASTD-3-18-05
() Publish Date:

Revision Date/Time (Note if correction):
Dept Affected: Public Safety
Title: "An Act relating to crimes and dagerous instuments."
RDU: Alaska State Troopers
Component: AST Detachments
Sponsor: Rep. Hawker
Requester: House Judiciary
Component No.: 2325

Expenditures/Revenues (Thousands of Dollars)

Note: Amounts do not include inflation unless otherwise noted below

OPERATING EXPENDITURES	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
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 (FY2005) 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)*

This bill amends AS 11.81.900(b)(15) which is the criminal definition for "dangerous instrument." It adds "hands or other objects when used to impede normal breathing or circulation of blood by applying pressure on the throat or neck or obstructing the nose or mouth" to the definition.

This additional language adds clarity and will aide us when we have assault cases that involve strangulation and/or choking of victims.

Passage of this bill will have no fiscal impact on the Department of Public Safety.

Prepared by: Lieutenant Todd Sharp
Phone: 907-465-3223
Division: Alaska State Troopers
Date/Time: 3/18/05 4:14 PM
Approved by: Commissioner William Tandeske
Date: 3/18/2005
Agency: Department of Public Safety

(Revised 9/23/2004 OMB)

FISCAL NOTE

STATE OF ALASKA
2005 LEGISLATIVE SESSION

Fiscal Note Number:
Bill Version: HB 219
() Publish Date:

Revision Date/Time (Note if correction):
Dept. Affected: Administration
Title: An Act relating to crimes and dangerous instruments.
RDU: Legal and Advocacy Services
Component: Public Defender Agency
Sponsor: Rep. Hawker
Requester: House Judiciary
Component No.: 1631

Expenditures/Revenues (Thousands of Dollars)

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

OPERATING EXPENDITURES	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
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 (FY2005) 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)*

This bill broadens the definition of "dangerous instrument" in the criminal code to include hands or other objects when used for strangulation or suffocation. Using or threatening the use of a "dangerous instrument" in the commission of an offense generally raises the level of the offense to a felony, or aggravates the offense. Including hands within the definition of "dangerous instruments" will increase the level of offenses currently charged where hands are used or threatened to be used in such a manner. The number of these impacted offenses cannot be determined with any certainty. This bill, if enacted, will have a fiscal impact on the operations of the Agency, but it is not possible to predict with any certainty what that impact will be. Therefore an indeterminate fiscal note is submitted.

Prepared by: Linda K. Wilson, Deputy Director
Phone: (907)334-4416
Division: Public Defender Agency
Date/Time: 3/21/05 8:42 AM
Approved by: Michael Tibbles, Deputy Commissioner
Date: 3/21/2005
Agency: Department of Administration

(Revised 9/23/2004 OMB)

FISCAL NOTE

STATE OF ALASKA
2005 LEGISLATIVE SESSION

Fiscal Note Number:
Bill Version: HB219-LAW-CDCO-3-21
() Publish Date:

Revision Date/Time (Note if correction):
Dept. Affected: LAW
Title "An Act relating to crimes and dangerous instruments."
RDU: CRIMINAL
Component: Criminal Justice Litigation
Sponsor Representative Hawker
Requester House Judiciary
Component No.

Expenditures/Revenues (Thousands of Dollars)

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

OPERATING EXPENDITURES	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
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 (FY2005) 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)*

This bill amends Title 11 Criminal Law AS 11.81.900 (General Provisions - Definitions) by adding a new subsection under (b)(15) defining hands or other objects used in strangulation as "dangerous instruments".

Passage of this legislation will have fiscal impact on the Department of Law.

Prepared by: Kathryn Daughhetee, Director
Phone 465-3673
Division Administrative Services Division
Date/Time 3/22/05 2:45 PM
Approved by: K. Daughhetee for Scott Nordstrand, Acting Attorney General
Date 3/22/2005
Agency Department of Law

(Revised 9/23/2004 OMB)

HB

226

HOUSE COMMITTEE REPORT

(7)
Date Referred to Committee: April 22, 2005 **FURTHER REFERRALS: Finance**

Date of Committee Action: 02/10/06

The JUDICIARY Committee considered: **HB 226**

HOUSE BILL NO. 226 **PERSONAL INFORMATION BREACH**

"An Act relating to breaches of security involving personal information; and relating to credit report security freezes."

Recommends it be replaced with [ ] HCS *or* [X] CS for HB 226 (JUD)
For Senate Bills with new title: [ ] Technical Title [ ] New Title: HCR_____ [ ] Same Title [ ] New Title

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

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

NEW FISCAL NOTES *Assigned by Chief Clerk's Office

List by Dept(s):	*FN#	Fiscal	Indet.	Zero
LAW				X

PREVIOUS FISCAL NOTES

List by Dept(s):	FN#	Fiscal	Indet.	Zero

Signing with recommendations	Printed Last Name	DP	DNP	NR	AM
	Gara	✓			
	Coghill			✓	
	WILSON	✓			
	Gruenberg	✓			
	ANDERSON				X
	KOTT			✓	
Chair:	McGuire	✓			
Chair:					

FISCAL NOTE

STATE OF ALASKA
2006 LEGISLATIVE SESSION

Fiscal Note Number:
Bill Version: HB226-LAW-C&FB-2-9-0
() Publish Date:

Revision Date/Time ("Note if correction):
Dept. Affected: LAW
Title "An Act relating to breaches of security involving personal information; and relating to credit report..."
RDU CIVIL
Component Commercial & Fair Business
Sponsor Representative Gara
Requester House Judiciary
Component No.

Expenditures/Revenues (Thousands of Dollars)

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

OPERATING EXPENDITURES	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
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 (FY2005) 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)*

This bill ads a chapter to AS 45 that imposes disclosure requirements on businesses that collect and store personal information if there is a security breach of the businesses' information system. In the event of a security breach, notice of the breach must be made to consumers by either written or electronic means, with some exceptions if the notice will cost more than $250,000, or the number of affected consumers exceeds 500,000. Consumers can bring a court action for violations of this law to recover damages and injunctive relief.

The bill also ads a section that allows consumers to place a security freeze on his or her credit report. When a security freeze is in place, a credit reporting agency may not release information from the consumer's credit report to third parties unless requested by the consumer. There are several exemptions for access required to correct technical information, and for some agencies like the child

Prepared by: Kathryn Daughhetee, Director
Phone 465-3673
Division Administrative Services Division
Date/Time 2/9/06 4:33 PM
Approved by: Kathryn Daughhetee for David Márquez, Attorney General
Date 2/9/2006
Agency Department of Law

STATE OF ALASKA **BILL NO.** _____
2005 LEGISLATIVE SESSION

ANALYSIS CONTINUATION

support enforcement agency, Department of Health and Social Services, and Department of Revenue. Court action can be brought by consumers to enforce this law. Remedies include injunctive relief, damages (including lost wages and pain and suffering), and punitive damages up to $5000.

Violations of the provisions of this bill are not automatically violations of Alaska's Consumer Protection Act. Consumers will likely be left to their own enforcement efforts for violations of this Act except in the most agregious cases where the State may bring an action. I do not believe there will be any significant fiscal impact to the Department of Law from this bill.

ALASKA STATE LEGISLATURE

REPRESENTATIVE LES GARA REPRESENTATIVE JOHN COGHILL

CSHB 226 (L&C): Personal Information Breach / Security Freeze

Sponsor Statement

In February ChoicePoint, Inc., a Georgia-based financial database company admitted personal information affecting almost 150,000 consumers had been stolen from its company. Recently the company admitted it knew of this breach since the fall and had delayed letting consumers, including 251 Alaskans, know about the breach until last month. HB 226 is based on two provisions in California law.

This bill requires that any business or governmental entity that collects this personal customer information as part of their business must notify consumers if the security of that information is compromised. California is currently the only state to mandate consumer notification and this bill is modeled after the California law.

Once an individual learns or believes their personal information has been compromised, that person should be able to block access to credit reports and credit scores. Blocking access to a credit report prevents an identity thief from fraudulently opening new lines of credit in his or her name.

The second section of the bill contains this "security freeze" provision. There are three companies in the country (Experian, Equifax and TransUnion) which act as consumer financial information clearinghouses, and that provide consumer data to banks, credit card, insurance, and other companies. The security freeze provision allows consumers to prevent the clearinghouses from sharing their information. The provision will allow a consumer to regulate who will receive a copy of their credit report. Under the security freeze provision the consumer is required to give the credit reporting agency an access code to release their report to a company wishing to extend a line of credit.

Many businesses like ChoicePoint make money by selling consumer information. Alaskans value their privacy. Companies that profit from trading financial and personal information need to protect that information.

Representative Les Gara
State Capitol, Room 418
Juneau, AK 99801
(907) 465-2647

Representative John Coghill
State Capitol, Room 204
Juneau, AK 99801
(907) 465-3719

ALASKA STATE LEGISLATURE

REPRESENTATIVE LES GARA

SECTIONAL ANALYSIS

CSHB 226 (L&C) – Personal Information Breach / Security Freeze

---

Section 1 Establishes *Chapter 48 – Information Security* under AS 45.

Article 1. Breach of Security Involving Personal Information.

- **Sec. 45.48.010.** A business or governmental agency must notify Alaskans of any breach of security that compromises their personal information.

- **Sec. 45.48.020 – 45.48.060.** The business or governmental agency may notify people of a breach by email or written documentation. These disclosures may be delayed if it would compromise a Dept. of Law investigation. An exception is made for employees or agents of a business who view personal information if they do not use that information for purposes unrelated to the business. An exception is also made if the business or governmental agency already has a policy in place that complies.

- **Sec. 45.48.070.** A person has the right to civil legal action if any part of AS 45.48.010 - 45.48.090 is violated.

- **Sec. 48.45.090.** Definitions.

Article 2. Security Freeze.

- **Sec. 45.48.100.** A consumer may freeze part or all of their credit report information.

- **Sec. 45.48.110 – 45.48.120.** To place a security freeze a person must notify credit reporting agencies by certified mail. The reporting agency is then required to place the freeze within 5 days after receiving the request and send a written confirmation of the security freeze within 10 days. A personal identification number or password must accompany this written confirmation for the consumer to use when authorizing the release of their credit report.

- **Sec. 45.48.130.** Once a security freeze is in place a consumer may contact a credit reporting agency to release their credit information to a specific third party. The consumer must provide proper identification, the password or number provided under the previous section, and information to identify the party to allow access to. The reporting agency must comply with a consumer's request within 3

days. Once a security freeze is in place, a credit reporting agency may not release a credit report without prior authorization.

- **Sec. 45.48.140 – 45.48.150.** If a consumer requests a security freeze, the credit reporting agency must disclose the process to the consumer. A credit reporting agency must remove a security freeze within 3 days if the consumer requests it.

- **Sec. 45.48.160.** Credit reporting agencies may not charge more than $10 to place or remove a security freeze or more than $12 to allow access for a specific person. They may not charge a fee if the person has had personal information stolen.

- **Sec. 45.48.170 – 45.48.180.** A credit reporting agency may require additional information from the consumer only when needed to reasonably identify the consumer. During a security freeze a credit reporting agency may not change information in a consumer's file without sending confirmation to the consumer.

- **Sec. 45.48.190.** A person who suffers damages as a result of AS 45.48.100 – 45.48.290 may bring about a court action and recover damages. A person who knowingly violates these sections is also liable in a class action suit.

- **Sec. 45.48.270.** Certain reports are not covered by AS 45.48.100 – 45.48.290. These reports include:
  - Reports that contain only information about transactions between the consumer and the person making the report.
  - Reports that are internal communications within the organization that is making the report as long as the consumer is informed that this information may be communicated.
  - Reports of an authorization or approval of a specific extension of credit.
  - Reports that contain only information about a person's decision whether to extend credit if the person is informed where
  - Reports that contain only general information such as character, reputation, personal characteristics gained from personal interviews.
  - Reports that contain credit information to be used only for a commercial purpose.

- **Sec. 45.48.280.** Certain uses of credit reports are exempted from the provisions of AS.45.48.100 – 45.48.290. These include use by the Dept of Health and Social Services when investigating fraud, use by the Dept. of Revenue when investigating or collecting delinquent taxes, and use by a state or municipal agency that establishes and enforces child support obligations.

- **Sec. 45.48.290.** Definitions.

Article 3. General Provisions.

- **Sec. 45.48.300.** If any provision of AS 45.48 conflicts with federal law, the provision does not apply to the extent of the conflict.

- **Sec. 45.48.390.** Definitions.

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.

Victims of ID theft fight for years to repair sprawling mess

IDENTITY: "You're guilty until proven innocent," says woman who was hurt by a criminal.

By JAMES JAMES
Chicago Tribune

WASHINGTON — Since falling victim to identity theft four years ago, John Harrison has learned the hard way that the crime is like a chronic disease that goes into remission, only to flare up again when least expected.

"I dealt with my latest debt collector just a week ago," the 44-year-old salesman for a firearms maker said.

"And the Army actually just garnisheed my retirement pay for the third time," said Harrison, a retired infantry captain who lives in Connecticut.

The man who misused Harrison's personal information not only obtained credit using Harrison's name but also opened checking accounts and wrote more than 126 bad checks as Harrison, some of them on government installations.

"The ones that were written on military bases become government debt," Harrison said. "And because I'm retired and get a government paycheck, when those things start to, I just get a government letter in the mail saying, 'We're taking your money.'"

The Federal Trade Commission estimated 10 million people were victimized by the crime in 2002, the most recent year for which it has data.

Recent disclosures by consumer-data collection companies including ChoicePoint, LexisNexis and Bank of America that sensitive information about millions of consumers was compromised have fueled concerns that many more people could be victimized like Harrison.

If those failures to protect consumers' personal data lead to more identity theft, the victims would be added to what experts consider the fastest-growing financial crime in the United States.

The Federal Trade Commission estimated 10 million people were victimized by the crime in 2002, the most recent year for which it has data.

No credible expert believes that number has fallen. Identity theft costs the U.S. economy billions of dollars annually.

See Page A-5, IDENTITY

John Harrison says it has taken him years to straighten out the mess caused when he became a victim of identity fraud.

Anchorage Daily News 4/3/05

IDENTITY: *As credit industry, politicians debate costs, victims struggle*

Continued from A-1

While federal and state governments and businesses that extend credit have made progress in helping victims regain their financial footing, the experience of victims shows much more is left to be done.

COUNTERMEASURES

In January, for example, a Springfield, Ill., police officer made a routine traffic stop of a 78-year-old woman, an identity-theft victim, according to Illinois Attorney General Lisa Madigan.

The officer ran the motorist's name through the state's criminal database, which turned up a warrant for writing bad checks. It was the identity thief, however, who wrote the checks.

Nevertheless, "the poor, little old lady was hauled off to the police station," Madigan said. That occurred even though the identity theft took place in 1998 and she had reported it to state law-enforcement officials.

The arrest also happened even though the attorney general two years ago had pushed legislation through the Illinois General Assembly meant to prevent that kind of humiliation.

Such an arrest might have been avoided if there had been a statewide database of identity-theft victims, something Madigan is trying to implement.

The financial services industry has raised concerns about such databases, fearing that unscrupulous borrowers could falsely claim to be identity-theft victims to avoid paying debts.

Something that could help victims and nonvictims alike would be to give them the ability to deny prospective credit providers access to credit bureau files for the purpose of issuing new credit. That could stop identity thieves.

Victim advocates say a federal law to that effect would help greatly. So far, only California and Texas allow victims to place security freezes on their files maintained by the three largest national credit bureaus.

But a dozen states are considering following suit, said Gail Hillebrand, a senior attorney with Consumers Union, an advocacy group.

Banks, car dealers and other businesses have opposed such legislation, however, raising doubts about such laws' effectiveness.

And such freezes could deny consumers the instant gratification of walking into stores, getting rapid credit approvals and leaving with cars, televisions or refrigerators.

CRITICAL STAGE

"The problem is, let's say mortgage interest rates dropped and I wanted to refinance," said Kirsten Fedda, senior federal counsel at the American Bankers Association.

"It's going to be an impediment. It's an unnecessary cost. It would probably end up frustrating more customers than helping them," Fedda said.

Creditors say they have taken steps to fight identity theft. Using advanced computer technology, companies can often spot fraud by detecting unusual spending patterns, for instance.

But victim advocates say the financial-services industry isn't moving aggressively enough, in part because they say the industry can pass along the costs of identity theft to other customers through fees and additional charges.

Identity-theft experts add that while the financial industry often advises consumers to protect themselves from the crime by shredding credit-card statements and the like, consumers are helpless in most cases of identity theft since lax security at companies or unscrupulous employees are often to blame.

Identity-theft victims and their advocates acknowledge the situation has improved in recent years for many victims, who sometimes include children whose Social Security numbers are misused by dishonest parents to obtain credit. They ruin the children's credit, making it hard for them to get loans later.

The improvement started with increased sensitivity to the victims among many law-enforcement officials, government policy makers and financial industry executives who once appeared to operate as though identity theft were a victimless crime.

A 2003 federal law resulted in changes phased in over the past year requiring businesses taken in by identity thieves to provide victims with the fraudulent credit applications. Before, victims routinely were denied such information.

California has a security-breach law in which consumer-data companies must notify consumers when security around sensitive consumer information has been compromised.

It was that law that required ChoicePoint to go public with its problem. About 20 states are considering similar laws.

Some states also have passed laws requiring police departments to take crime reports from identity-theft victims. Illinois allows victims to go to court to obtain a factual declaration of innocence.

Still, numerous proposals that would have helped identity-theft victims have been rebuffed in Congress and state legislatures.

'YOU'RE GUILTY'

During the recent Senate debate over legislation to tighten bankruptcy rules, Sen. Ben Nelson, D-Neb., tried to pass an amendment exempting debtors who could prove their financial problems were caused by identity theft. He failed.

Meanwhile, Linda Foley, executive director of the Identity Theft Resource Center and herself a victim of identity theft, asked, "Why don't we have all states requiring that victims of identity theft are allowed to have police reports taken, that the police must take police reports in the jurisdiction where the victim lives?"

She said even more understanding is needed of the "secondary wounding" that occurs after someone is targeted.

She blames the collection agencies, credit issuers and credit bureaus — as well as law enforcement — for requiring victims to provide copious documentation, which can be time consuming and expensive.

"It's frustrating," Foley said. "You're guilty until proven innocent."

Harrison, the firearms company salesman, said he stopped keeping track of the time he spent trying to clear his name after he hit 2,000 hours in early 2003, more than a year after he learned his identity was stolen in November 2001.

He blames losing an earlier sales job to the theft when his productivity dropped from having to field calls from collection agents at work.

He suffered from depression and anxiety.

His consumer debt interest rates tripled, and insurance premiums soared inexplicably.

"It's a difficult thing to explain," Harrison said. "I've always been a real strong person. I was a company commander in the 82nd Airborne. I actually kind of thrived in stressful situations.

"But this is (a) different deal because you really don't have any control over what these other people do or don't do," he said. "With identity theft you're not bleeding ... you haven't lost an arm or a leg. It's real difficult for people to see your loss or your damage."

Harrison had trouble finding another job; potential employers were scared off after conducting the standard credit checks. His solace was that the identity thief was caught and served 38 months in prison.

But the thief was released Dec. 15, giving Harrison pause.

"He could still have my Social Security number right in his wallet," he said.

InformationWeek
BUSINESS INNOVATION POWERED BY TECHNOLOGY

Law Requires ChoicePoint To Disclose Fraud

An identity-theft ring gained access to 145,000 consumer records held by ChoicePoint, which later notified consumers as required under California law SB-1386.

By Thomas Claburn, InformationWeek
Feb. 17, 2005
URL: http://www.informationweek.com/story/showArticle.jhtml?articleID=60401882

In its privacy statement, data-aggregation company ChoicePoint Inc. says that it is "dedicated to protecting the privacy of individuals," which includes "strict standards regarding the use and dissemination of personal informa ion."

Yet such dedication is only exceeded by the determination of identity thieves who, by setting up some 50 fictitious businesses, duped the company into granting them access to 145,000 consumer-data profiles it maintains among its store of roughly19 billion public records.

In Los Angeles County Superior Court last week, a Nigerian national who participated in the identity-theft scheme was sentenced to 16 months in state prison. ChoicePoint was alerted of the breach last October. But some 35,000 California consumers didn't realize they were potential victims until they received a letter about the breach from ChoicePoint last week, per California law.

Disclosure of the incident was required under California's SB-1386, which took effect July 1, 2003. According to the law, any state agency, person, or business that does business in California and owns or licenses electronic data that includes personal information, is required to disclose any data security breach to California residents whose unencrypted personal information may have been accessed by an unauthorized person.

While the extent of the fraud arising from the incident may not be known for months, ChoicePoint said it would send out 110,000 more notifications to individuals outside California.

"That's certainly good practice and most responsible companies are going to do that, if no other reason than of mitigating any damages that might result," says Kevin Lyles, partner in the privacy practice at law firm Jones Day. Lyles says another privacy-related law, the Health Insurance Portability and Accountability Act, requires organizations to mitigate any damages as a result of security breaches, and there are similar provisions in the Gramm-Leach-Bliley law.

Gail Hillebrand, senior attorney for Consumers Union, a nonprofit testing and information organization that publishes *Consumer Reports*, suggests such provisions aren't enough. "This is a reminder to all consumers how insecure our personal financial information is when it's held by someone else who makes their own decisions about how much to spend on security," she says. "It highlights the need for consumers to have additional rights to protect themselves, particularly the need for state security freeze laws."

A security freeze lets a consumer prevent people or businesses from accessing a credit reports for the purpose of granting credit. In turn, it prevents identity thieves from accessing a credit report.

Currently, Hillebrand says, freeze laws are being considered in 11 states: Colorado, Connecticut, Hawaii, Illinois, Indiana, Maine, Maryland, Massachusetts, Oregon, Utah, and Washington. California, Louisiana, Texas, and Vermont already have passed some form of freeze law.

Consumers Union is pushing for federal laws th.. would require all companies to inform customers nationwide of data breaches. "We think that will help consumers to protect themselves but also will create a business environment that encourages more investment in security," says Hillebrand. Massachusetts already has a disclosure provision similar to California's, and Illinois may be next.

Yet many oppose a legislative approach to the problem. California state Sen. Debra Bowen's effort last year to expand the data-breach notification requirement to cover disclosures of data in any form, not just electronic data, was voted down amid lobbying by business groups such as the California Chamber of Commerce and the American Electronics Association.

Quinn Jalli, director of privacy and Internet service provider relations at E-marketing company Digital Impact Inc., says that that while data breaches often lead to calls for federal legislation, companies such as ChoicePoint already have a strong incentive to protect their data. "As we saw with spam, legislation is not going to solve the problem," Jalli says.

"This obviously means companies need to do a better job with their information security," Lyles says. "But having a law that says to do that doesn't really help. The problem is technology, and the ability of hackers is moving faster than some companies can move to keep information secure."

Laws don't dictate what companies need to do from a security standpoint, Lyles says. "Almost all the laws that I've seen just say you'll take reasonable security precautions," he explains. "It very well could be that ChoicePoint was using reasonable precautions and that wasn't good enough. The real key is what you do after it. And I think the lesson here for companies is if you have a breach you know about, whether you have a [disclosure] law in the state or not, you ought to let individuals know."

ChoicePoint could not be reached for comment regarding the data breach.

Last year, according to the Federal Trade Commission, consumers reported fraud losses of more than $547 million. Internet-related fraud accounted for 53% of all reported fraud complaints. According to the Better Business Bureau, 9.3 million Americans were victims of identity-theft fraud in 2004.

The New York Times
nytimes.com

March 9, 2005

LexisNexis Says Thieves May Have Taken Data on Consumers

By TOM ZELLER Jr.

In yet another apparent theft of consumers' personal data, the LexisNexis Group, a major compiler of legal and consumer information, said today that about 30,000 of its records - including names, addresses and Social Security numbers of individuals - may have fallen into the hands of thieves.

The announcement follows the recent disclosure several other cases of the loss or theft of consumer data. ChoicePoint, another leading data broker, said last month that it had inadvertently sold the records of more than 140,000 individuals to con artists. And Bank of America said more recently that backup computer tapes containing information on more than a million of its customers had been lost.

The Federal Bureau of Investigation and the Treasury Department are investigating the LexisNexis incident, people close to the inquiry said. The concern in such cases is that criminals can use the information to open credit card accounts in other people's names or engage in various other forms of so-called identity theft.

The LexisNexis breach is almost certain to accelerate calls from privacy advocates and state and federal officials for greater scrutiny of the companies that buy, store and sell consumer data. The issue will be taken up on Thursday in a hearing before the Senate Banking, Housing and Urban Affairs Committee, and next Tuesday at a similar hearing before the House Energy and Commerce Committee.

"I personally see no socially redeeming value in anyone having the right to give away and sell my personal information unless I approve it," the chairman of the House Energy and Commerce Committee, Representative Joe Barton, Republican of Texas, said today.

"Under current law these companies have a legal right to package it and do almost anything they want to do with it," Mr. Barton said. "I just think that's fundamentally wrong. And in the Internet age, it's dangerous."

Some other lawmakers expressed similar sentiments.

"We need to think proactively and treat these data troves with the same level of care and protection that we would any other valuables," Senator Patrick Leahy, Democrat of Vermont, wrote in an e-mail statement. On behalf of the Senate Judiciary Committee, Mr. Leahy is scheduled to testify before the Senate Banking Committee hearing this afternoon. "Our peace of mind, our economy and even our nation's security depend on it," he wrote. The Judiciary Committee also plans to conduct hearings on the issue soon.

As it is, the industry is governed by a hodgepodge of state and federal laws. Critics have argued that because those laws are often at odds and sufficiently ill-defined, the rules permit companies like ChoicePoint and LexisNexis to police themselves as they market consumer data to insurance agencies, background screeners, private detectives, law firms and even the federal government.

Some control is provided by the federal Gramm-Leach-Bliley Act of 1999, which governs the use of personal information maintained by financial institutions. And the Fair Credit Reporting Act of 1970, along with its 2003 amended version, the Fair and Accurate Credit Transactions Act, establishes rules for gaining access to and disseminating consumer reports.

But it has been a matter of debate over how those rules apply to vast information warehouses like ChoicePoint and LexisNexis, which provide a blend of both public and private information, only some of which is of interest to identity thieves. The information services industry has lobbied hard in the past to stall legislation that would put curbs on the kinds of information that can be peddled and to whom. But the succession of large-scale breaches, and the sheer number of consumers being affected by each new incident, will make it harder for the industry to resist some sort of legislative yoke.

"This is going to be hotly fought by people who are gathering and packaging this information," Mr. Barton said. "But I don't see why you have to have Social Security numbers available that are really extraneous to the product at hand."

Several new bills have been introduced in Congress to address the growing problem of consumer privacy, including three submitted in January by Senator Dianne Feinstein, Democrat of California. Mr. Barton has said that he and colleagues from both sides of the aisle have been discussing possible legislative approaches. Senator Charles E. Schumer, Democrat of New York, who chastised another data compiler, WestLaw, in February for making sensitive information like Social Security numbers to easily available, said he plans to introduce legislation next week.

"If we do nothing, identity theft is going to go through the roof," Mr. Schumer said today. "It really means we should get on the stick and do something here. We're in the wild west where companies can do anything they want."

LexisNexis and its parent company in London, the publishing and information services giant Reed Elsevier, said the recent breach involved databases acquired last July through the $775 million purchase of Seisint, a Florida-based compiler of consumer background and asset information.

Seisint has two main products: Accurint, a service for locating people and determining their financial assets, and Securint, a background screening service. LexisNexis has been in the process of folding those Seisint databases into its fleet of legal, news and consumer data archives.

Exactly how thieves gained access to the Seisint databases remains murky. LexisNexis said that the breach was discovered as part of "an ongoing extensive review of the verification, authorization and security procedures and policies" and that it appeared to have occurred well after the Seisint acquisition. The company also said it has been asked by law enforcement officials investigating the matter not to reveal too many details of the crime.

But Kurt Sanford, the chief executive for corporate and federal markets at LexisNexis, which is based in Dayton, Ohio, emphasized that the company's own computer systems did not appear to have been broken into by hackers. Instead, Mr. Sanford said, it appeared that thieves were able to gain access to the log-in names and passwords used by what he described as a handful of legitimate subscribers to the Seisint databases.

Mr. Sanford would not comment on whether the passwords were somehow stolen by hackers breaking into those customers' computers or compromised by less technical means. But once they logged in, the thieves were able to sift through a trove of consumer data without being detected until the legitimate subscribers were billed for their monthly activity.

In early February, Mr. Sanford said, those customers notified LexisNexis of odd activity on their bills. The company took about two weeks to investigate the billing questions, Mr. Sanford said, and then notified law enforcement officials when it became clear that a breach had been made. Reed Elsevier disclosed the breach in a public announcement this morning in London.

The timing is of particular interest in the wake of the breach at ChoicePoint, which has been criticized for delaying notification of the 145,000 affected consumers for more than five months. In that case, the company learned that it had been fooled by thieves posing as legitimate subscribers to its service in late September of last

year. Law enforcement officials were notified, and they asked the company to delay a public announcement until Jan. 1. But ChoicePoint did not publicly disclose the breach until mid-February.

LexisNexis says it plans to begin sending letters to the 30,000 affected consumers in the next few days, similar to the notification process that ChoicePoint recently completed. More than one-third of the people whose data was compromised in the LexisNexis case appear to reside in California, according to a state-by-state breakdown provided by the company. Massachusetts, New York, Florida and Texas were also heavily hit.

All 30,000 consumers will be offered free credit monitoring for one year, according to Mr. Sanford. ChoicePoint made a similar gesture in notification letters that it mailed out in the wake of the security breach there.

But privacy advocates argue that such gestures are not commensurate with the damage such security breaches can bring to consumers' lives.

"Thieves will just put this stuff on the shelf until the heat is off," said Beth Givens, the director of the Privacy Rights Clearinghouse, a consumer advocacy group in San Diego. "They know that there is increased scrutiny of these individuals at this time, and if they read the newspapers, they know that ChoicePoint and Lexis have purchased credit monitoring for one year," Ms. Givens said.

"They need to tell these individuals that they need to be monitoring their credit for the rest of their lives."

LexisNexis Data on 300,000 People Feared Stolen

By Jonathan Krim
Washington Post Staff Writer
Tuesday, April 12, 2005; 12:22 PM

Information broker giant LexisNexis announced today that previously announced security breaches at the company could affect roughly 300,000 consumers, making it one of the largest potential identity theft incidents on record.

When the company announced last month that its Seisint unit had been compromised by identity thieves in a series of incidents, it estimated that Social Security numbers, drivers' license numbers, names and addresses of 32,000 consumers were exposed.

The new figure, the company said yesterday, reflects internal investigations that analyzed data over the past two years and found that identity thieves used IDs and passwords of legitimate Seisint customers to purchase the information.

Last year LexisNexis bought Florida-based Seisint Inc., which sells data gathered from extensive searches of public records to businesses, law-enforcement agencies, private investigators and others.

"We regret that consumers, who traditionally are the primary beneficiaries of our risk management products and services, may have been affected by these events," Kurt Sanford, head of the company's corporate and federal markets group, said in a statement. "We have taken a number of significant actions in recent weeks to further guard against these types of fraudulent intrusions at our customer sites and to enhance our security procedures and policies overall."

The company said that affected consumers would be offered a free credit report and monitoring for a year.

The announcement is yet another blow to the largely unregulated marketplace of sensitive personal information that involves mega-brokers such as LexisNexis, ChoicePoint and Acxiom to smaller re-sellers, some private investigators and others. Each of the three large brokers has announced at last one major breach, as have universities, banks and other organizations that store consumer data.

More than two dozen states are now examining identity theft legislation, while several members of Congress have introduced legislation or are preparing to do so.

washingtonpost.com

Data Brokers Vow to Protect Personal Information

By Jonathan Krim
Washington Post Staff Writer
Wednesday, March 16, 2005; Page E01

Two captains of the information-broker industry told a congressional panel yesterday that they would support new regulations to better protect sensitive personal data that they collect and sell on virtually every adult American.

But the executives balked at what appears to be a growing bipartisan consensus among key House and Senate members that the sale of Social Security numbers for commercial purposes should be banned unless individuals give their permission.

"When my [Social Security] number and my information is routinely given out without my permission, it's just wrong," said Rep. Joe Barton (R-Tex.), who heads the House Energy and Commerce Committee. "And in the Internet age, it's dangerous."

Barton said Congress would probably consider a measure to require permission for the trading or sale of such data except to law enforcement agencies, in addition to other steps to increase oversight of the largely unregulated data-broker industry that has been rocked by a series of security breaches.

Last month, ChoicePoint Inc., one of the nation's largest brokers, announced that personal information on at least 145,000 consumers was bought from the company by thieves who masqueraded as legitimate business people.

Last week, LexisNexis Group, another big broker that specializes in business and legal data, announced that its systems had been penetrated by thieves who obtained data on 32,000 consumers.

Kurt Sanford, chief executive of LexisNexis Corporate and Federal Markets, endorsed a proposal by the head of the Federal Trade Commission, Deborah Platt Majoras, that would extend the same security guidelines to data brokers that financial institutions must follow.

Sanford also agreed with calls for a federal law requiring notification of consumers if their personal information has been obtained by thieves. Only California has such a law.

But Sanford said banning all sales of Social Security numbers would be a mistake, because "there are circumstances where the sale is in the consumers' best interests." For example, he said, independent investigative agencies might need such data to help fight identity fraud. Businesses, he added, need it to help collect unpaid debts.

Derek V. Smith, chief executive of ChoicePoint, agreed.

"I believe that only by adding a more formal structure to the current scheme of information use will we realize the value of technology-based tools to society," Smith said. Both he and Sanford used the hearing as a platform to apologize to consumers whose data have been compromised, and to assure Congress that they have tightened their systems to try to prevent such fraud.

But several members of the House subcommittee on commerce, trade and consumer protection were unimpressed by the companies' efforts.

Raising his voice in a series of rapid-fire questions, Rep. Edward J. Markey (D-Mass.) pressed Smith on whether he would lengthen the credit-alert monitoring period that ChoicePoint has offered to consumers whose information was stolen.

"What about lifetime monitoring?" Markey asked. "One year is not enough. What about five years? Can you guarantee that?" He said thieves might simply lie low for a year before trying to access consumers' accounts.

Smith, appearing rattled, said he would consider extending the service but refused to commit.

AARP Alaska

April 13, 2005

The Honorable Tom Anderson, Chair
House Labor and Commerce Committee
Alaska State Capitol, Room 408
Juneau, AK 99801-1182

RE: HB 226 (Gara)--Support

Dear Chair Anderson:

On behalf of the members of AARP in Alaska, we encourage you and your colleagues on the House Labor and Commerce Committee to support HB 226, authored by Representative Les Gara and co-sponsored by Majority Leader Coghill and Representatives McGuire and Kerttula.

As you know, earlier this year ChoicePoint admitted that it had lost personal information affecting 150,000 customers, including some Alaskans. Although the information was illegally stolen from the company, the company failed to notify their customers at the time they first discovered the information was taken last fall.

HB 226 will mandate that any company that has had its customer financial information stolen must notify those customers that they could be victimized.

HB 226 also requires the three companies that have credit information on all of us to offer security freeze protection. Security freeze protections allow the consumer to determine which companies will be allowed credit information which can be used for lines of credit. This will provide an effective tool to prevent false applications for credit because of stolen information/identity theft.

While your Committee is hearing this bill today, the United States Senate is conducting hearings on the millions of Americans who are victims of identity theft and the billions of dollar they have lost.

This issue needs to be addressed and HB 226 is one good way to help Alaskans.

We urge an "AYE" vote on HB 226.

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 Pete Kott
Representative Gabrielle LeDoux
Representative Bob Lynn
Representative Norman Rokeberg
Representative Harry Crawford
Representative David Guttenberg
Representative Les Gara

AKPIRG
ALASKA PUBLIC INTEREST RESEARCH GROUP WWW.AKPIRG.ORG
PO Box 101093 • Anchorage, Alaska 99510-1093 • Ph: (907) 278-3661 • Fax: (907) 278-9300 • email: akpirg@akpirg.org

April 4th, 2005

AkPIRG Statement of Support for:

HB 226 / SB 148: Personal Information Breach / Security Freeze

The Alaska Public Interest Research Group (AkPIRG), an Alaska membership organization dedicated to protecting consumers, urges quick passage of HB 226 / SB 148. These bills are an appropriate response to the ChoicePoint Inc. security breach that occurred in February. Consumers across the nation were alarmed to find out that nearly 150,000 people across the nation had their personal information stolen and were at high risk for identity theft. Yet only California had laws on the books that mandated ChoicePoint Inc. to notify those who fell victim.

The total included some 251 Alaskans. This bill will help better protect those individuals and all Alaskans if and when a similar security breach occurs in the future

HB 226 / SB 148 are based on two provisions in California law.

First, the bills require that any business that collects this personal customer information as part of their business must notify consumers if the security of that information is compromised. This common sense step will make sure that companies like Choicepoint Inc. will disclose when consumers are at risk

When a consumer's personal information has been compromised, that person should be able to block access to credit reports and credit scores. Blocking access to a credit report prevents an identity thief from fraudulently opening new lines of credit in his or her name, one of the many dangers of identity theft.

The second section of the bills contains this "security freeze" provision. The three credit reporting agencies - Experian, Equifax and TransUnion - act as consumer financial information clearinghouses The security freeze provision allows consumers to prevent the clearinghouses from sharing their information. Without access to a consumer's credit report, an identity thief will not be able to open a new account. The provision will allow a consumer to regulate who will receive a copy of their credit report. The security freeze provision allows consumers to use an access code to release their report to a company wishing to extend a line of credit.

Any company that makes a profit from trading financial and personal information has the responsibility to protect that information. HB 226 / SB 148 have strong measures that the Alaska Legislature can enact to better protect consumers. We urge you to pass HB 226 / SB 148

Sincerely,

Steve Cleary, AkPIRG Executive Director

NATIONAL ASSOCIATION OF
State PIRGs

Kerry Smith
Senior Consumer Attorney
National Association of
State PIRGs
1334 Walnut St, 8th Floor
Philadelphia, PA 19107
Phone: (215) 732-3747
Fax: (215) 732-3747
ksmith@pirg.org

March 3, 2005

Representative Les Gara
State Capitol, Room 418
Juneau, AK 99801-1182
Fax: 907-465-3518

Dear Representative Gara:

This letter is in response to your inquiry about state level consumer protections against identity theft.

In December 2003, Congress passed the Fair and Accurate Credit Transactions Act (FACT Act). With the FACT Act, Congress significantly amended the Fair Credit Reporting Act (FCRA), which provides consumer protections regarding the use, accuracy, and privacy of consumer credit reports. Through its passage, the financial industry won its primary goal: permanent preemption of stronger state credit and privacy laws in several, but importantly, not all, areas.

In the wake of the ChoicePoint Inc. security breach, mandatory notification is an available and advisable step for states to take to protect consumers. A state law requiring companies to notify consumers about a security breach should not be preempted by the federal Fair Credit Reporting Act. Currently, California is the only state with mandatory notification, but several other states are considering legislation including Connecticut, Georgia, Illinois, Massachusetts, and Texas.

It is imperative that consumers' personal, sensitive information be protected and we urge you to enact mandatory notification. There are many other important consumer protections set forth in: *The Clean Credit and Identity Theft Protection Act: Model State Laws*, which we produced along with Consumers Union. I would be happy to provide you with a copy of those model laws if AkPIRG has not already done so.

I would be happy to answer any questions that you and your colleagues in the Alaska Legislature may have. Thank you for your time and interest in this matter.

Sincerely,

Kerry C. Smith

Kerry Smith
Senior Consumer Attorney

Consumers Union

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

April 7, 2005

Representative Les Gara
State Capitol
Room 418
Juneau, AK 99801-1182
907-465-3518 (fax)

Re: Support for HB 226, Breaches of Security and Security Freeze for Credit Reports

Dear Representative Gara:

Consumers Union, the independent, nonprofit publisher of *Consumer Reports*, supports HB 226, 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 ward 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

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

State Security Freeze Laws are Not Preempted by the Federal FCRA

Assertions by the opponents of state security freeze legislation that it is preempted by federal Fair Credit Reporting Act are wrong. Congress amended FCRA section 625, codified at 15 U.S.C. sec. 1681t, to specifically include identity theft prevention and mitigation in the listing of categories of state laws *not* preempted. Section 1681t(a), the general rule against preemption, preserves state law, except to the extent this rule is modified by (b) and (c). The general rule of section 1681(t)(a), preserves "the laws of any State with respect to the collection, distribution, or use of any information on consumers, or for the prevention or mitigation of identity theft, except to the extent that those laws are inconsistent with any provision of this title, and then only to the extent of the inconsistency." (emphasis added)

Consumer reporting agencies have claimed in some states that a state security freeze law would be preempted by FCRA's provisions on fraud alerts or trade line blocking. This is wrong. Fraud alerts and trade line blocking, Sec. 605A and 605B, are listed in sec. 625(b)(5)(B) and (C), and preempt state law only "with respect to the conduct required by the specific provisions of" 605A and 605B. See 625(b)(5), codified at 15 U.S.C. sec. 168t(b)(5). In other words, the fraud alert and trade line blocking sections preempt states from imposing other fraud alert and other trade line blocking requirements on the same entities reached by the federal statute. However, the preemption extends ONLY to the conduct required by these specific sections. Other "conduct," including a state-created obligation to freeze access to a credit record, falls under the general preservation of state laws in 1681t(a).

The Federal Trade Commission and the Federal Reserve Board, in a regulatory preamble, have emphasized the narrowness of the "conduct required" type of preemption, which is the type that applies to fraud alerts and to trade line blocking, in a regulation relating to the effective date of "conduct required" preemption under section 1681t(b)(5).

In the Joint Final Rule on Effective Dates, 12C.F.R. sec 222; 16 C.F.R. sec. 602, the introductory material emphasizes that FACTA preemption under the "conduct required" formula in section 1681t(b)(5) is narrow. The FTC and Federal Reserve Board state:

> The Agencies note that section 711(2) of the FACTA Act adds a new provision to the FCRA that bars any requirement or prohibition under any state laws "with respect to the conduct required by the specific provisions" of the FCRA, as amended by the FACTA Act. The joint final rules are based on the Agencies' view that the specific protections afforded under the FCRA override state laws only when the referenced federal provisions that require conduct by the affected persons are in effect because that is the time when conduct is required by those provisions of the FCRA.

This analysis was made in connection with the issue of the effective date of conduct required preemption. Read in conjunction with the addition of ID theft to the general no-preemption except for inconsistency rule, it strongly supports the position that if FACTA does not require

conduct in an area related to ID theft, then states remain free to require conduct in that area. This is precisely the case with a security freeze law, a subject simply unaddressed by FACTA.

An extensive legal analysis of the various types of preemption under FACTA, and how those provisions do, and do not, apply to various state legislative measures, by Consumers Union attorney Gail Hillebrand is posted at
http://www.consumersunion.org/creditmatters/creditmattersupdates/001640.html
and printed in: After the FACTA: State Power to Prevent Identity Theft, 17 Loyola Consumer Law Review 53 (2004).

G:\Groups\Credit & Finance\Gr ii\Wallet\2005\noFCRApreemption.doc

LEGISLATIVE RESEARCH REPORT

MARCH 11, 2005

REPORT NUMBER 05.196

CHOICEPOINT AND SECURITY BREACHES OF PERSONAL INFORMATION

PREPARED FOR REPRESENTATIVE LES GARA

BY CHERIE NIENHUIS, LEGISLATIVE ANALYST

You asked about security breaches of personal information. You inquired specifically about the recent security breach involving ChoicePoint, Incorporated.

In February 2005, newspapers around the country reported that ChoicePoint, Inc., an "information clearinghouse," had sent letters to thousands of Californians informing them that their personal information may have been compromised in a fraud scheme. According to ChoicePoint, the scammers posed as legitimate businesses, and acquired the names, Social Security numbers, driver's license numbers, and credit reports of close to 145,000 people nationwide. To date, at least 750 people have been defrauded as a result of the scheme, which the company knew about since the fall of 2004.[1]

CHOICEPOINT, INCORPORATED

ChoicePoint, Inc. is one of several businesses that make money from selling consumer information. Such enterprises generally have no transactions with consumers directly. Rather, they gather data on individuals, from otherwise public records such as home purchases, bankruptcy filings, criminal convictions, and professional licensing boards, for the purpose of brokering the information to other businesses. Other businesses interested in this information include lending companies, insurance agencies, and corporations conducting pre-employment background checks. According to one news source, data brokers like ChoicePoint do not need permission from members of the public to collect and sell their personal information. Further, the

[1] "Response to Customer Fraud Litigation," from the ChoicePoint website, *http://www.choicepoint.com/news/statement_0205_1.html.*

they bypass the rules of the Fair Credit Reporting Act (FCRA)—a law intended to give consumers more control over who can view information that credit agencies collect about them and the right to examine and dispute such information.[2]

Various products sold by ChoicePoint, however, appear to fit the criteria for inclusion under the FCRA, and indeed, ChoicePoint claims they are "FCRA-compliant." The Electronic Privacy Information Center (EPIC), a public interest research center that informs the public about civil liberty, privacy, and constitutional issues, believes that other data products sold by ChoicePoint should be included under the FCRA. In a letter to the Federal Trade Commission dated December 2004 (prior to the public disclosure of the ChoicePoint security breach) the EPIC urged the FTC to investigate two products for inclusion under the federal law, arguing that they meet the criteria of "consumer reports" specified by the FCRA.[3] We include the EPIC's letter, describing products sold by ChoicePoint as Attachment A.

Filings with the Securities and Exchange Commission indicate that among the products ChoicePoint sells are claims history data, motor vehicle records, police records, and credit information. They also provide services related to employment background screenings, drug testing administration, public record searches, vital record services, credential verification, due diligence information, Uniform Commercial Code searches and filings, DNA identification services, authentication services and people and shareholder locator information searches. In addition to private businesses, ChoicePoint has provided personal information to law enforcement agencies and other government entities.[4]

The March 2005 issue of the *Privacy Journal*, a monthly publication that covers legislation and public attitudes affecting the confidentiality of personal information, reports that ChoicePoint is a spin-off of Equifax, one of the nation's three major credit reporting agencies. Chronicles of Equifax, and, indirectly, ChoicePoint, detailed in the article, show that Equifax has on more than one occasion faced charges by the Federal Trade Commission of violating the Fair Credit Reporting Act. We include the *Privacy Journal* article as Attachment B.

CONSUMERS AFFECTED BY CHOICEPOINT SECURITY BREACH

ChoicePoint estimates that the personal information of up to 145,000 consumers could have been compromised by the recently announced security breach. The company also provides information about how many individuals by state may have been affected by the incident. According to the ChoicePoint website, information about 251 Alaskans may have been compromised in the fraud scheme.

Although California is currently the only state that requires companies to notify persons whose information may have been stolen in a security breach, officials with ChoicePoint indicate that

[2] Kim Zetter, "California Woman Sues ChoicePoint," *Wired News*, February 24, 2005, available on the Internet at *http://www.wired.com/news/privacy/0,1848,66710,00.html*

[3] Letter, Chris Jay Hoofnagle and Daniel J. Solove, EPIC, to the Federal Trade Commission, December 16, 2004, as posted at the EPIC website, *http://www.epic.org/privacy/choicepoint/fcraltr12.16.04.html*.

[4] ChoicePoint Inc., "Notes to the Consolidated Financial Statements," September 30, 2004, available online at *http://www.sec.gov/Archives/edgar/data/1040596/000095014404010687/g91731e10vq.htm*.

they sent out letters to all 145,000 consumers they believe may have been affected. This action may have been prompted by a letter from 19 state attorneys general to ChoicePoint, requesting that the company disclose additional information about the incident. Alaska's attorney general was one of the signers of the letter.[5] We include information about ChoicePoint's actions, including a list showing the number of consumers affected by state, as Attachment C.

BREACH OF INFORMATION LEGISLATION

The National Conference of State Legislatures (NCSL) reports that as of early March 2005, legislators in 20 states are considering legislation pertaining to the breach of personal information. One common provision in the recently-introduced legislation is the reporting of security breaches to affected persons. According to NCSL, these provisions are being considered in Arizona, Colorado, Georgia, Idaho, Illinois, Indiana, Minnesota, Missouri, Montana, New Jersey, New York, Ohio, Oregon, Rhode Island, Tennessee, Texas Virginia, Washington, and West Virginia.[6] We provide a copy of NCSL's compilation of breach of information legislation as Attachment D.

I hope you find this information to be useful. Please do not hesitate to contact us if you have questions or need additional information.

---

[5] Todd R. Weiss, "State Officials Push ChoicePoint on ID Theft Notifications," *Computerworld*, February 18, 2005, available on the Internet at *http://www.computerworld.com/printthis/2005/0,4814,99886,00.html*.

[6] California, which already has provisions for notification of affected persons, is considering additional breach of personal information legislation.

Attachment A

Letter, Chris Jay Hoofnagle and
Daniel J. Solove, EPIC, to the
Federal Trade Commission,
December 16, 2004

ELECTRONIC PRIVACY INFORMATION CENTER

December 16, 2004

Federal Trade Commission
600 Pennsylvania Ave. NW
Washington, DC 20580

Re: Request for investigation into data broker products for compliance with the Fair Credit Reporting Act

Dear Commissioners,

In recent years, there has been an explosion in the creation and use of dossiers of personal information to evaluate individuals. Some of these dossiers, known as "data products," in the information brokerage industry, are designed to be sold so that they avoid triggering the provisions of Fair Credit Reporting Act of 1970 (FCRA), a landmark law that ensures that compilations of personal information used for many different purposes are accurate, correctable, fairly collected. Additionally, the FCRA mandates that information collectors be accountable for their practices.

Commercial data broker ChoicePoint, for instance, is selling data products that are used by law enforcement, government, and the private sector to make important decisions about people. ChoicePoint, [1] one of the largest data aggregation companies, became independent from Equifax, a leading U.S. credit rating agency, in 1997.[2] ChoicePoint has bought more than 40 companies and competitors, and obtains 40,000 new public records daily for its database of more than 19 billion records.[3] Choicepoint contracts with about 35 federal agencies to supply data.[4]The company's slogan is "Smarter Decisions. Safer World." However, decisions cannot be smarter, and we cannot be safer, if these new data products are not subject to the basic fairness requirements incorporated in the FCRA.

In 1970, Congress passed the FCRA in response to a litany of problems and complaints about credit reporting agencies.[5] The opening of the FCRA states:

> The Congress makes the following findings:
>
> (1) The banking system is dependent upon fair and accurate credit reporting. Inaccurate credit reports directly impair the efficiency of the banking system, and unfair credit reporting methods undermine the public confidence which is essential to the continued functioning of the banking system.
>
> (2) An elaborate mechanism has been developed for investigating and evaluating the credit worthiness, credit standing, credit capacity, character, and general reputation of consumers.
>
> (3) Consumer reporting agencies have assumed a vital role in assembling and evaluating consumer credit and other information on consumers.
>
> (4) There is a need to insure that consumer reporting agencies exercise their grave responsibilities with fairness, impartiality, and a respect for the consumer's right to privacy.
>
> 15 U.S.C. § 1681(a) (1970).

Americans face a return to the pre-FCRA era if companies like ChoicePoint can amass dossiers on

Americans without compliance with any regime of Fair Information Practices. That era was marked by unaccountable data companies that reported inaccurate, falsified, and irrelevant information on Americans, sometimes deliberately to drive up the prices of insurance or credit.[6] To some extent, this pre-FCRA area has returned. For instance, erroneous ChoicePoint data sold without the FCRA's protections were relied upon in Florida to cleanse voting registration rolls of felons prior to the 2000 election, resulting in the disenfranchisement of thousands of eligible voters.[7]

In an appendix to this letter, we explain ChoicePoint's business activities.[8] ChoicePoint sells a number of FCRA products in the employment screening, tenant screening, and criminal background check fields. But the company also sells two products, "AutoTrackXP" and "Customer Identification Programs" outside of the FCRA's protections. AutoTrackXP is a database of 17 billion records that includes Social Security Number, addresses, property and vehicle information, and other information.[9] The company's anti-fraud "Customer Identification Programs" are a suite of data products that have been created in order to verify the identity and perform background checks on individuals who open new financial services accounts. [10] From its description, Customer Identification Programs appears to be an AutoTrackXP report with additional identity verification services.

These two products are sold to financial institutions, members of the public (private investigators, law firms, etc.) and to law enforcement agencies. These are the same institutions which rely on credit reports and investigative consumer reports, but these new products are sold outside the protections of the FCRA, yet are often used for related (and sometimes identical) purposes.

It is difficult to determine what sources ChoicePoint used to create AutoTrackXP and Customer Identification Programs. However, both of these non-FCRA products have similar data elements and descriptions as ChoicePoint's FCRA products. The similarities between the information in an AutoTrackXP report and the company's FCRA products is striking; it suggests that AutoTrackXP was generated from FCRA sources.[11]

Under a well-developed line of cases, courts interpreting the FCRA have held that if a data product originates from a consumer report database, the product remains protected by the FCRA. For instance, the D.C. Circuit held in *Trans Union v. FTC* that marketing lists drawn from a credit reporting agency's master databases were "credit reports" for purposes of the FCRA.[12]

If ChoicePoint had created AutoTrackXP or its Customer Identification Programs from FCRA sources, the products should be considered "consumer reports" for purposes of the FCRA. Consumers could exercise a series of important rights with respect to their ChoicePoint reports that are not currently available. Only the FTC can determine the "information flows" or sources of data used by ChoicePoint, and whether the company has leaked data from the FCRA products to AutoTrackXP and Customer Identification Programs. We urge the Commission to engage in this inquiry.

Even if these products are not consumer reports for purposes of the FCRA, it is incumbent on the FTC to analyze them and make recommendations to Congress concerning possible expansion of the FCRA. If these products are found not to be within the FCRA, the FTC should recommend to Congress to expand the scope of the Act.

Many of the public policy purposes underlying the FCRA are being circumvented by data brokers who have artfully constructed databases to avoid the Act's provisions. For instance, the use of data products for voter registration list cleansing implicates the most important right in a democracy—access to the polls. If such a use is not covered by the FCRA, this creates an absurd consequence. Someone denied access to a credit card would enjoy access, correction, and other FCRA rights, while another person denied access to the voting polls would have no federal information privacy rights.

Other absurd consequences emerge from this end-run around the protections of the FCRA. Although the