

RESNALES ISLATIONS OFFIILES, 2005 2000/2

11912 SENATE LABOR & COMMERCE

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

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

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

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

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

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

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

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

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

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

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

Identity crisis?

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

- A recent change in federal laws requires that each of the major credit reporting bureaus provide free of charge one credit report per year to any consumer who asks for it. They're available at www.annualcreditreport.com, or by phone, toll-free, at 1-877-322-8228.
- A quick review of your credit report will enable you to detect fraudulent credit-card accounts and loans taken out by identity thieves. If you find something amiss on any one of the three reports, contact the credit reporting bureau and place a security alert on your file. That will warn the bureaus to look for fraudulent credit applications submitted in your name and require lenders to contact you personally before extending any credit.

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

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

This [Federal Trade Commission](#) page has more advice for consumers looking to avoid identity theft

Print Page

Close Window

Copyright © 2005 The Anchorage Daily News (www.adn.com)



[Homepage](#) | [Alaska News](#) | [Alaska Weather](#) | [Alaska Sports](#) | [Alaska Videos](#) | [Alaska Real Estate](#) | [Home Improvement](#) | [A](#)
[Your Health](#) | [2 on Your Side](#) | [Assignment Alaska](#) | [The Bottom Line](#) | [Market View](#) | [Spirit of Youth](#) | [What's Cookin'?](#)

ChoicePoint says 251 Alaskans at risk of identity theft

Tuesday, February 22, 2005 - by Jeffrey Hope

Search

Anchorage, Alaska - Alaskans who may be at risk for identity theft will be getting a letter from the company that caused the problem.

The Georgia company ChoicePoint says it will send letters to 251 Alaskan customers, warning them of potential problems. The move comes after ChoicePoint says someone forged documents to gain access to thousands of customers' names, Social Security numbers and credit reports.

The company first learned of the problem in October. However, it wasn't until last month that officials began telling their customers. Now ChoicePoint says it will lead the industry in combating identify fraud.

"We've stepped up and said we think the industry needs to change," said ChoicePoint CEO Derek Smith. "We're going to lead the way, regardless of whether the rest of the industry follows -- we hope they will -- because it's in the consumer's best interest that we all do that."

Last week, Alaska's attorney general's office joined 17 other states asking ChoicePoint to notify any customers who may be at risk. Alaska is now considering writing a law that would force companies to notify customers in the event of a security breach.

EMAIL ARTICLE PRINT ARTICLE

Related articles:



Copyright © 2004 Channel 2 Broadcasting Inc. 701 East Tudor Road, Suite# 220, Anchorage, AK, 99503-7488 Phone: (907) 762-9202 Fax: (907) 561-0

Mor
Ear
dam
islar
Sno
wor
city
APD
roac
dow
Stop
conl
colli
Was
Corr

H
H



Identity Theft Victim Complaint Data

*Figures and Trends
In Alaska*

January 1- December 31, 2003

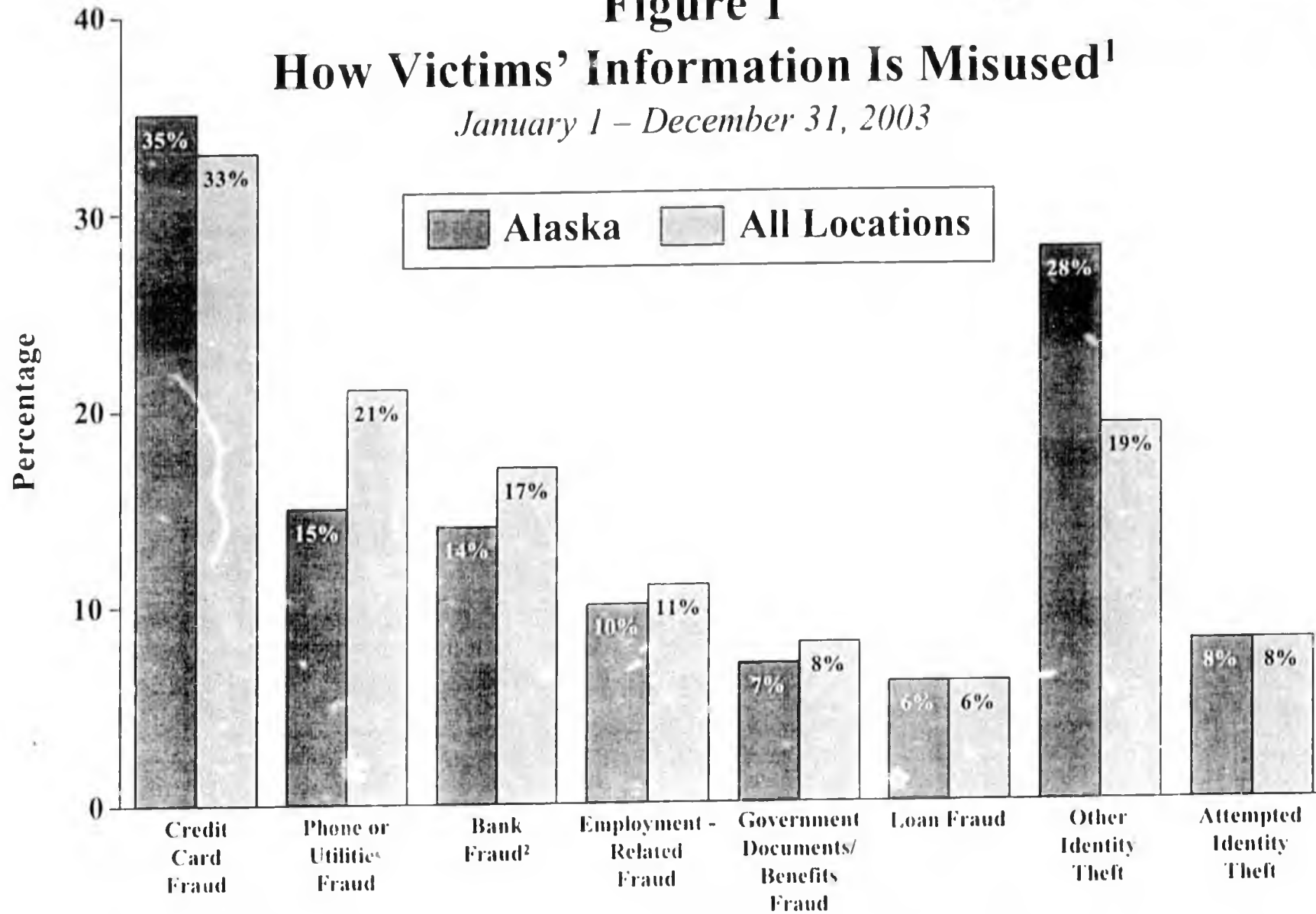


*Federal Trade Commission
Washington, DC*



Figure 1 How Victims' Information Is Misused¹

January 1 – December 31, 2003



¹Percentages are based on the total number of victims reporting 231 from Alaska and 214,905 from all locations. Percentages add to more than 100 because approximately 17% of victims from Alaska and 19% of victims from all locations reported experiencing more than one type of identity theft. All victims reported experiencing at least one type of identity theft.

²Includes fraud involving checking and saving accounts and electronic fund transfers.

Figure 2



How Victims' Information Is Misused¹

January 1 – December 31, 2003

Total Number of Identity Theft Victims:

Alaska = 231

All Locations = 214,905

Credit Card Fraud

<i>Theft Subtypes</i>	<i>Alaska</i>	<i>All Locations</i>
New Accounts	19.0%	19.2%
Existing Accounts	14.3	12.0
Unspecified	1.3	1.4
Total	35%	33%

Phone or Utilities Fraud

<i>Theft Subtypes</i>	<i>Alaska</i>	<i>All Locations</i>
Wireless - New	5.6%	10.4%
Telephone New	6.1	5.6
Utilities - New	2.6	3.8
Unauthorized Charges to Existing Accounts	0.9	0.6
Unspecified	0.0	0.8
Total	15%	21%

Bank Fraud²

<i>Theft Subtypes</i>	<i>Alaska</i>	<i>All Locations</i>
Existing Accounts	6.5%	8.2%
Electronic Fund Transfer	4.8	4.8
New Accounts	2.2	3.8
Unspecified	0.4	0.5
Total	14%	17%

Employment-Related Fraud

<i>Theft Subtype</i>	<i>Alaska</i>	<i>All Locations</i>
Employment-Related Fraud	10.0%	11.1%

Government Documents or Benefits Fraud

<i>Theft Subtypes</i>	<i>Alaska</i>	<i>All Locations</i>
Fraudulent Tax Return	2.6%	3.7%
Driver's License Issued / Forged	3.9	2.3
Gov't Benefits Applied For / Received	0.9	1.3
Social Security Card Issued / Forged	0.0	0.4
Other Gov't Documents Issued / Forged	0.0	0.4
Unspecified	0.0	<0.1
Total	7%	8%

Loan Fraud

<i>Theft Subtypes</i>	<i>Alaska</i>	<i>All Locations</i>
Business / Personal / Student Loan	2.1%	2.3%
Auto Loan / Lease	1.7	2.0
Real Estate Loan	2.6	1.0
Unspecified	0.0	0.3
Total	6%	6%

Other Identity Theft

<i>Theft Subtypes</i>	<i>Alaska</i>	<i>All Locations</i>
Other	18.6%	11.6%
Illegal / Criminal	2.6	2.1
Medical	0.9	1.8
Internet / E-Mail	2.2	1.7
Apartment / House Rented	0.4	0.9
Bankruptcy	1.3	0.3
Insurance	0.4	0.3
Property Rental Fraud	0.0	0.2
Child Support	0.4	0.2
Securities / Other investments	0.4	0.2
Magazines	0.4	0.1
Total	28%	19%

Attempted Identity Theft

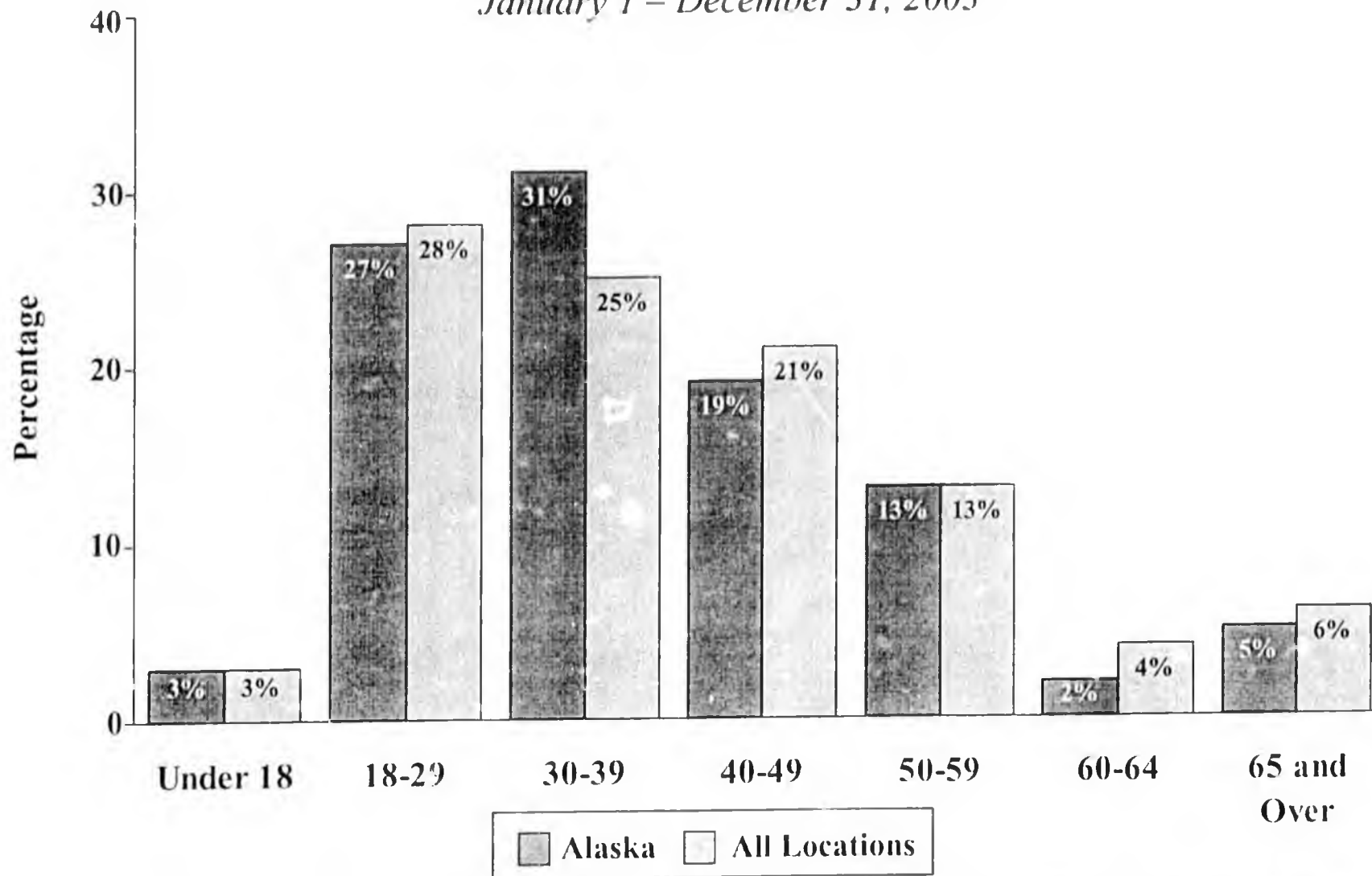
<i>Theft Subtype</i>	<i>Alaska</i>	<i>All Locations</i>
Attempted Identity Theft	7.8%	8.0%

¹Percentages are based on the total number of victims reporting: 231 from Alaska and 214,905 from all locations. Percentages add to more than 100 because approximately 17% of victims from Alaska and 19% of victims from all locations reported experiencing more than one type of identity theft. All victims reported experiencing at least one type of identity theft.

²Includes fraud involving checking and saving accounts and electronic fund transfers.



Figure 3
Complaints by Victim Age¹
January 1 – December 31, 2003



¹Percentages are based on the number of victims who provided their age: 231 from Alaska and 197,475 from all locations. This chart represents 96% of victims reporting from Alaska and 95% of victims reporting from all locations who contacted the Federal Trade Commission directly.

Figure 4a



Identity Theft Victims by State (Per 100,000 Population)¹

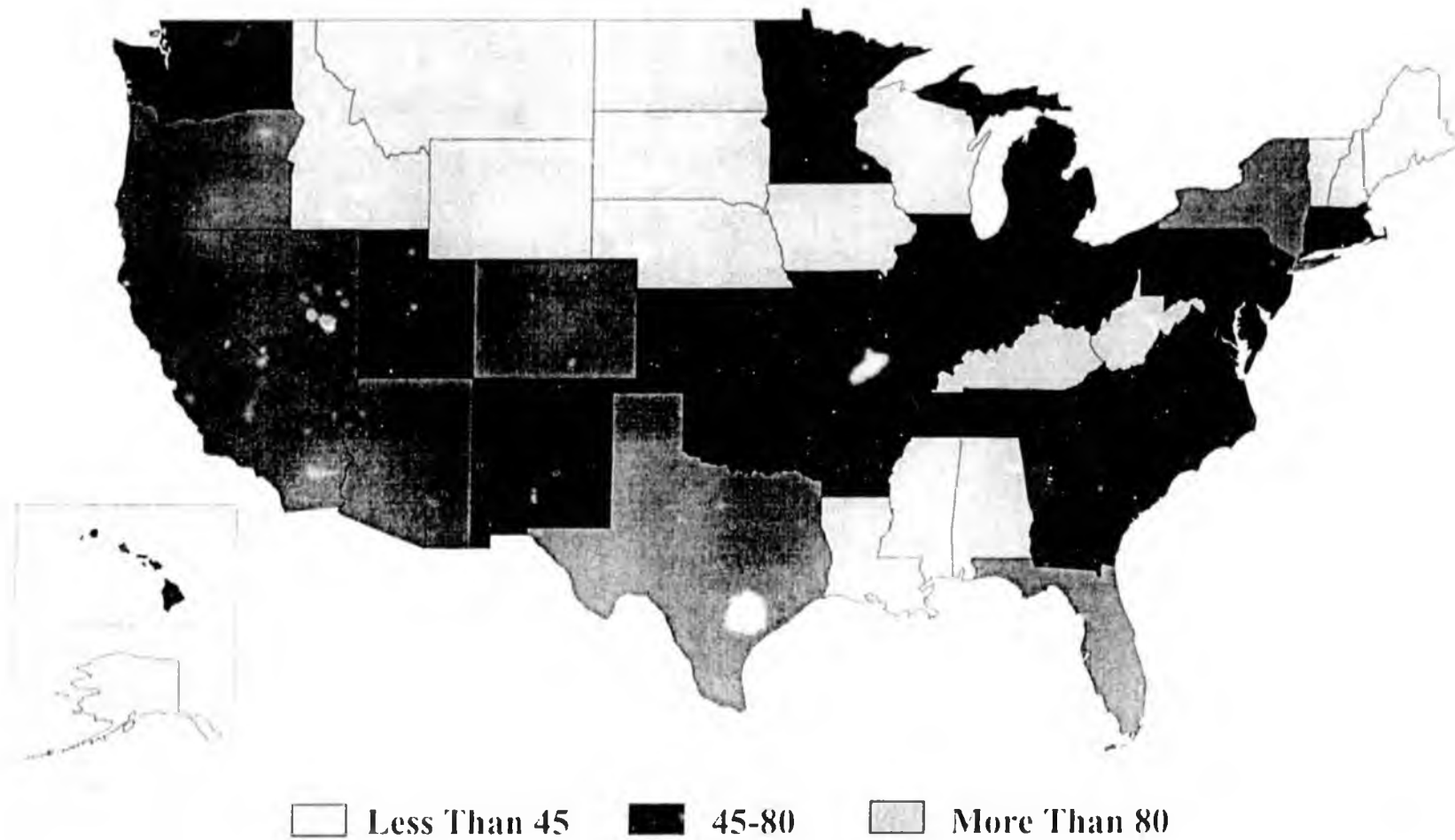
January 1 – December 31, 2003

Rank	Victim State	Victims Per 100,000 Population	Number of Victims	Rank	Victim State	Victims Per 100,000 Population	Number of Victims
1	Arizona	122.4	6,832	26	Kansas	50.6	1,378
2	Nevada	113.4	2,541	27	Rhode Island	49.9	537
3	California	111.2	39,452	28	Minnesota	49.7	2,517
4	Texas	93.3	20,634	29	Oklahoma	48.1	1,689
5	Florida	83.0	14,119	30	Ohio	48.0	5,494
6	New York	82.4	15,821	31	Tennessee	47.6	2,782
7	Oregon	81.7	2,909	32	Arkansas	47.5	1,294
8	Colorado	81.3	3,698	33	South Carolina	45.7	1,895
9	Illinois	77.4	9,792	34	Nebraska	44.9	781
10	Washington	77.3	4,741	35	Wisconsin	42.5	2,325
11	Maryland	74.9	4,124	36	Louisiana	41.7	1,875
12	Georgia	70.5	6,127	37	Alabama	40.5	1,823
13	New Mexico	70.3	1,317	38	New Hampshire	38.8	500
14	New Jersey	68.9	5,948	39	Mississippi	37.6	1,084
15	North Carolina	65.9	5,537	40	Idaho	36.1	493
16	Michigan	65.1	6,566	41	Alaska	35.6	231
17	Missouri	61.3	3,496	42	Wyoming	34.3	172
18	Indiana	59.1	3,660	43	Kentucky	32.3	1,332
19	Virginia	58.2	4,297	44	Montana	30.7	282
20	Delaware	57.7	472	45	Iowa	30.6	900
21	Massachusetts	56.5	3,634	46	West Virginia	28.1	05
22	Utah	56.4	1,326	47	Maine	27.0	153
23	Connecticut	54.9	1,913	48	Vermont	26.7	39
24	Pennsylvania	52.9	6,545	49	South Dakota	20.0	101
25	Hawaii	51.6	649	50	North Dakota	19.6	150

¹Per 100,000 unit of population estimates are based on the 2003 U.S. Census population estimates (Table NST-EST2003-01 - Annual Estimates of the Population for the United States and States, and for Puerto Rico, April 1, 2000 to July 1, 2003). Numbers for the District of Columbia are: 917 victims and 162.8 victims per 100,000 population. 97% of the 214,965 total victims reporting indicated their state of residence.



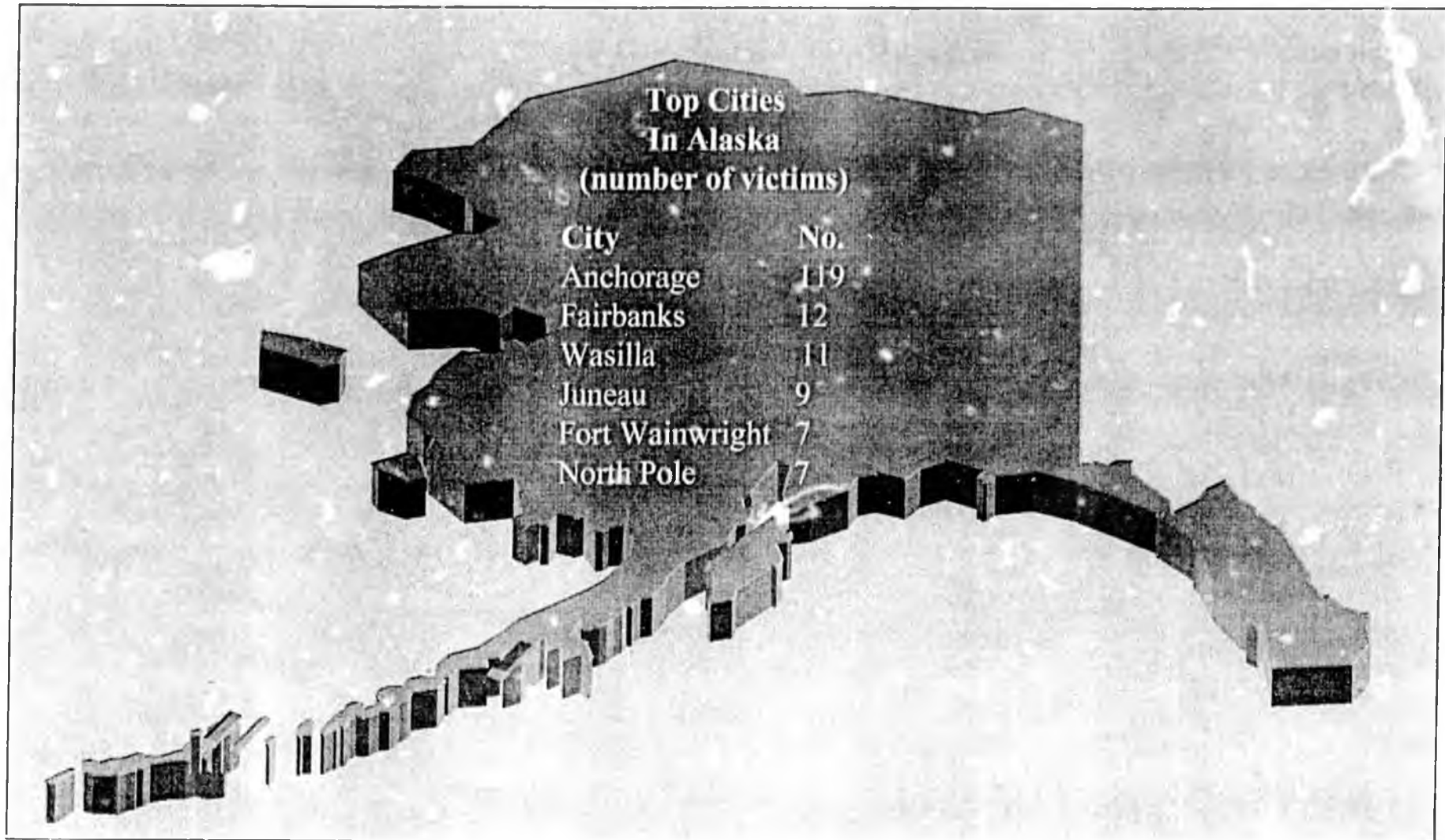
Figure 4b
Identity Theft Victims by State (Per 100,000 Population)¹
January 1 – December 31, 2003



¹Per 100,000 unit of population estimates are based on the 2003 U.S. Census population estimates (Table NST-EST2003-01 - Annual Estimates of the Population for the United States and States, and for Puerto Rico - April 1, 2000 to July 1, 2003). Numbers for the District of Columbia are: 917 victims and 162.8 victims per 100,000 population. 97% of the 214,905 total victims reporting indicated their state of residence.



Figure 5
Top Cities in Alaska¹
January 1 – December 31, 2003



¹99.1% of the 231 victims reporting from Alaska indicated their city of residence

ALASKA
Consumer Sentinel Complaint Statistics and Trends
January 1 - December 31, 2002

Total Number of Fraud and Identity Theft Complaints from Alaska Consumers = 1,121

Consumer Sentinel

Fraud Complaints from Alaska Consumers = 873

Top Fraud Complaint Categories for Alaska Consumers

Rank	Top Categories	Complaints	Percentage ¹
1	Internet Auctions	229	26%
2	Advance-Fee Loans and Credit Protection/Repair	136	16%
3	Shop-at-Home/Catalog Sales	75	9%
4	Foreign Money Offers	74	8%
5	Internet Services and Computer Complaints	72	8%

¹Percentages are based on the total number of fraud complaints from Alaska consumers (873).

Amount Paid Reported by Alaska Consumers

Total No. of Complaints	Total Amount Paid Reported	Total Complaints Reporting Amt Pd	Percentage of Complaints Reporting Amount Paid	Average Amount Paid ²
873	\$647,187	707	81%	\$915

²Average amount paid is based on the total number of fraud complaints where amount paid was reported by Alaska consumers (707)

Top Alaska Consumer Locations for Fraud Complaints

Consumer City	No. of Complaints
Anchorage	319
Fairbanks	59
Wasilla	35
Juneau	33
Eagle River	26
North Pole	26

IDENTITY THEFT
Data Clearinghouse

Identity Theft Complaints from Alaska Victims = 248

Identity Theft Types Reported by Alaska Victims

Rank	Identity Theft Type	No. of Victims	Percentage ¹
1	Credit Card Fraud	123	50%
2	Phone or Utilities Fraud	49	20%
3	Bank Fraud	37	15%
4	Loan Fraud	21	8%
5	Government Documents or Benefits Fraud	13	5%
6	Employment-Related Fraud	12	5%
	Other	46	19%
	Attempted Identity Theft	18	7%

¹Percentages are based on the 248 victims reporting from Alaska. Percentages add to more than 100 because approximately 24% of victims from Alaska reported experiencing more than one type of identity theft

Top Alaska Identity Theft Victim Locations

Victim City	No. of Victims
Anchorage	77
Fairbanks	19
Juneau	14
Eagle River	10
Wasilla	8



ALASKA PUBLIC INTEREST RESEARCH GROUP

WWW.AKPIRG.ORG

PO Box 101093 • Anchorage, Alaska 99510-1093 • Ph: (907) 278-3861 • Fax: (907) 278-9300 • email: akpirg@akpirg.org

April 4th, 2005

AkPIRG Statement of Support for:**SB 149: Identity Theft Protections**

The Alaska Public Interest Research Group (AkPIRG), an Alaska membership organization dedicated to protecting consumers, urges quick passage of SB 149. This bill is an appropriate response to the ChoicePoint Inc. security breach that occurred in February, and will greatly enhance consumer protection in regard to Identity Theft. Consumers 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 even 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, and it will protect Alaskans from the increasing array of sophisticated identity thieves.

The bill requires 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.

The bill also contains a "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.

SB 149 provides for consumer driven credit monitoring allowing consumers monthly access to their credit reports for a fee of two dollars per month, additional reports would cost eight dollars. It also requires bureaus to provide reports to consumers within twenty-four hours of receiving a request.

The bill will assure better protection of consumers' Social Security Numbers (SSN), which are the gateway to many financial accounts and private information. The widespread use of the SSN's as an identifier makes it relatively easy for thieves to fraudulently use consumers' SSNs to assume their identities and gain access to financial accounts and other sensitive information.

In addition, the bill requires businesses to take reasonable measures to protect against unauthorized access to or use of records containing personal information when disposing of them. In addition, it extends this requirement to any third-party vendors engaged to dispose of such records.

When a consumer has been a victim of an identity theft, he or she is at increased risk for further misuse of his personal information for unlawful purposes. Criminal identity theft occurs when a suspect in a criminal investigation identifies himself or herself using the identity of another, innocent person. As a result, a criminal record is created in the name of an innocent person. In such circumstances, a victim of identity theft must have the right to obtain a factual declaration of innocence from the courts in his or her state, and such declaration should be available through a statewide database that can be used to show others that the victim was not responsible for the crime. This bill provides for that.

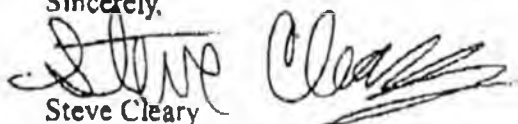
The unrestricted use and sharing of credit header information can put consumers at serious risks if identity theft as well as other harms. This bill closes credit header loopholes by limiting the release of this data only to those individuals who would have a permissible purpose to obtain a consumer's credit report under the federal Fair Credit Reporting Act.

When a consumer suspects that he or she has been the victim of identity theft, his or her most obvious recourse is the local police department. Consumers in Alaska have been frustrated by local law enforcement agents who do not know how to respond to identity theft. Whether the theft has occurred at home or in another community, a consumer should be entitled to file a police report in his or her home jurisdiction and this bill provides for that.

Any company that makes a profit from trading financial and personal information has the responsibility to protect that information. This bill will go a long way to insuring that while also giving Alaskan consumers other needed protections.

SB 149 has strong measures that the Alaska Legislature can enact to better protect consumers. We urge you to pass SB 149.

Sincerely,



Steve Cleary

AKPIRG Executive Director



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

April 1, 2005

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

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

Dear Senator Guess:

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

Security freeze

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

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

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

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

Federal law is inadequate to prevent identity theft

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

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

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

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

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

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

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

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

Notice of security breach

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

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

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

Very truly yours,



Gail Hillebrand

VIDEO Professor

March 28, 2005

Rep. John Coghill
Alaska State Legislature

Dear Rep. John Coghill,

We read with great interest of, and support your efforts to fight Identity Theft. Our own CEO and founder, John Scherer "The Video Professor" was himself a victim of Identity Theft.

As a result, we've launched a special section on our own website at www.videoprofessor.com with lots of free information about ID Theft for consumers.

But based on our experience with John's case, one can wonder what is worse. The crime itself, or the struggle to fight back with an often-chaotic legal system.


Too often we heard in court, "It's not a violent crime." Violent? No. Vile? Yes!

We applaud your efforts and encourage stronger laws, and even tougher enforcement of these laws.

Identity thieves are predators of the worst kind.

If we can be of assistance to you in our efforts, please do not hesitate to call on us.

Yours truly,

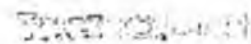


Brian Olson
Director-Marketing Communication
VIDEO PROFESSOR Inc
303-232-1244 Ext 380
bolson@videoprofessor.com



Web

CNN Money



- Home
- News
- Markets
- Technology
- Commentary
- Personal Finance
- Autos
- Real Estate

TECHNOLOGY > Personal Tech

SAVE | EMAIL | PRINT | SUBSCRIBE TO MONEY

LexisNexis acknowledges more ID theft

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

April 12, 2005 4:49 PM EDT

By Caleb Silver, CNN Business News Producer

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

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

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

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

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

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

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

Top Stories

[Investors too eager?](#)

[Markets fly post-Fed](#)

[Superfast downloaders sued](#)

[Mission: Security](#)

[Ventas to buy Provident for \\$1.2 billion](#)

— ADVERTISEMENT —

YOUR E-MAIL ALERTS

Identity Theft

LexisNexis

Activate or
CREATE YOUR OWN

[Manage alerts](#) | [What is this?](#)

Related stories

- [Fund clients vulnerable to ID theft?](#)
- [ID theft: The real risk](#)
- [Damage control for identity theft](#)
- [ChoicePoint: More ID theft warnings](#)

Video

[More video](#)



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

[Play video](#)

— advertiser links —

[what's this?](#)

MyCashNow - \$100 - \$1,000 Overnight

Payday Loan Cash goes in your account overnight. Very low fees. Fast decisions....
www.mycashnow.com

been fraudulently breached 59 times using stolen passwords.

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

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

How safe is your computer? [Click here](#) to find out.

If you think you are a victim, [click here](#).

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

The Hot List

[Tax-friendly places '05](#)

[5 island hideaways off the beaten path](#)

[In King Bruce's mines at Lazard](#)

More Personal Tech

[Apple's Tiger software out April 29](#)

[HP unveils iPod models](#)

[LexisNexis acknowledges more ID theft](#)

Money TRY AN ISSUE OF MONEY MAGAZINE FREE



Name State/Pr [Privacy Policy](#)

Address Zip/Postal

City E-mail

[contact us](#) | [magazine customer service](#) | [site map](#) | [glossary](#) | [RSS](#) | [press room](#)

OTHER NEWS: [CNN](#) | [SI](#) | [Fortune](#) | [Business2.0](#)

♣ = Money subscribers ♦ = Premium content

Disclaimer

© 2005 Cable News Network LP, LLLP, A Time Warner Company ALL RIGHTS RESERVED
Terms under which this service is provided to you. [privacy policy](#) [Reprints](#) of site stories are available.



Powered by Clickability

Anatomy of an ID theft

After Heather Harding's identity was stolen, she worked full time to reclaim her good name.

November 18, 2004: 3:24 PM EST

By Joan Caplin, MONEY Magazine

NEW YORK (MONEY Magazine) - The first warning sign came last December, although at the time Heather Harding didn't recognize it as such. Instead, when the letter arrived from Capital One asking if she'd requested a credit application, Harding assumed a simple mistake had been made.

Five months rolled by without incident, but then the red flags popped up in rapid succession. A call from her bank, Wells Fargo, inquiring about her application for a line of credit. The same question from Chase, where she had no accounts. Then a message from a local Ford dealer, who said he hoped to see her later that day with the additional paperwork they had discussed.

Harding knew nothing about these transactions. Instead, she realized, she had become a victim of one of the fastest-growing crimes in the U.S.: identity theft.

The credit inquiries, it turned out, were just the beginning. As Harding would find out over the following months, the thief had also rented a luxury apartment with a pool, a fitness center and views of the Pacific Ocean. She signed up for utilities, cell phones, Internet service and cable. She opened multiple financial accounts and ran up nearly \$10,000 in bills.

Yet, though the police are virtually certain they know the thief's true identity, she has not been arrested and probably never will be.

This nightmare, unfortunately, is all too common. Harding, 34, is one of 7 million people who were victims of identity theft in 2003, an increase of 80 percent from the previous 12 months.

At the Federal Trade Commission, identity theft is now the No. 1 consumer complaint. Only a tiny fraction of the perpetrators are prosecuted -- often, as in the case of Harding's alleged thief, because there are no witnesses who actually see the suspect filling out the credit application.

No one knows for sure how the criminal gained access to Harding's Social Security number, which opened the door to the thievery that followed.

What is more important, though, is the decisive action that Harding took afterward on her own behalf -- steps that ultimately restored her good name and absolved her of any financial responsibility.

Stage 1: Damage control.

Harding took the first crucial steps in wresting back her identity even before she understood properly that she'd been the victim of a crime. At the suggestion of a representative from Capital One, the first lender to

contact her last December, Harding notified the police and the three major credit reporting agencies (CRAs) that a false credit application had been made in her name.

She also asked the agencies to place a fraud alert on her credit reports. That would supposedly prompt lenders to inform her of any new requests for credit in her name. In practice, however, it often doesn't work.

In this case, though, Harding received a flurry of unsolicited calls from lenders in May, enough to make her realize that someone was using her identity.

She kicked her damage-control campaign into high gear. She visited the Ford dealer who had left the mysterious phone message about the need for additional paperwork. There, sales manager Othman Ghneim explained that the fraud alert on Harding's credit report had popped up when he ran a check on the young woman who had claimed to be Harding.

His suspicions grew when he perused the report. He says, "I saw some credit there that I didn't think this girl could have. It went back too far -- she would have been about 10 years old."

As she listened to Ghneim describe his encounter with her Doppelganger, Harding got chills.

"She knew everything about me," Harding says. "She knew I was married, where I lived, that I drove a Mercedes. And she had a story for everything."

When Ghneim found no record of Harding having owned the Ford Taurus that the imposter wanted to trade in, for instance, she explained that her husband got the Mercedes in their divorce. The real Harding has been happily married for six years.

But it wasn't until later in the day, when police paid a visit to the impersonator and found out that she lived only 20 minutes away, that Harding (whose home is in a gated community in Orange County, Calif.) got truly scared.

Until that moment, Harding says, she'd been in denial. Now she realized her security was threatened. "She could do something to my house, to my family."

Stage 2: Reality sets in.

Harding quickly put a number of safety measures in place.

She placed passwords on her legitimate financial accounts. She filed a complaint with the FTC, which provides law enforcement officials with information that will help stop perpetrators.

Harding also recontacted the police, and called the CRAs to reactivate her fraud alerts, which can expire in as little as 90 days. (For more ways to protect yourself, [click here](#)).

Filing a fraud alert with one CRA is supposed to automatically trigger all three agencies to send copies of your credit report so you can detect and fix errors.

Harding took no chances and made three separate requests for copies. She received them within a week. The one from Experian, however, was blank. It took several weeks and considerable hounding before the corrected report resurfaced.

Stage 3: Grunt work.

Victims of identity theft can spend anywhere from 30 to 600 hours recovering from the crime. Harding's experience was at the upper end of the spectrum. As is typical, most of Harding's time was spent on phone-hold or in repeated attempts to correct or make headway in matters she thought she'd already corrected or explained.

Overwhelmed by the task at hand, Harding began taking time off from her part-time job as the director of marketing for a special-events firm. A month into her ordeal, she decided to quit for good. Reclaiming her good name had turned into a full-time career.

To stay on top of the job, Harding began keeping a log of action she took to set her credit record straight.

"I've worked in the special-events industry for about 15 years," she explains, "and I know details are extremely important."

Harding's records cover 10 single-spaced pages and a spreadsheet with headings such as "date," "company contact," "time spent" and "response."

Harding sent all her correspondence by certified mail, return receipt requested. Credit agencies, she learned, are required by law to respond within 30 days. If she had her letters time-stamped, in effect, she'd improve her chance of a quick response.

You need to try to control the situation as much as possible," explains Harding.

Under the circumstances, Harding's quest for control was certainly understandable. In a 2003 study by the Identity Theft Resource Center, 76 percent of the respondents said they experienced "a sense of powerlessness or helplessness." Even more universal was the feeling of rage: 89 percent said they had it, as did Harding.

She began to have trouble sleeping and felt constant anxiety, "One minute, I'd be extremely angry and the next I'd be crying." In time, she even stopped socializing. "People try to understand," she says, "but it's very difficult unless you've been through it."

Creditors began hounding her, demanding payment for goods and services she'd never ordered. Getting out of town with her husband Wes became one of her few pleasures because Harding knew that then she couldn't get any phone calls.

"I was afraid to go to the mailbox or answer the phone," she explains. "I didn't know who'd be threatening me next."

Stage 4: Righting the wrongs.

Over the next four months, Harding vigilantly contacted every company that wrongly appeared on her credit report. She'd call, e-mail or send certified letters -- repeatedly -- until the false information was dropped.

She always identified herself as a victim of identity theft, then supplied the company with a notarized ID Theft Affidavit of the crime (available at ftc.gov).

"I asked as many questions as I could, to try and piece together what [the thief] had done," she says. "I was a

real reporter."

The most stressful moment: visiting the apartment complex where the suspect lived, after the manager insisted on a face-to-face meeting.

"I was terrified I'd bump into her," Harding recalls. "I was afraid [the manager] would call her down and confront her." Her worries, though, were unfounded. The imposter never appeared.

Stage 5: Recovery.

One year after Harding first became a victim of identity theft, she has finally managed to clear her name. The fraudulent accounts are closed, the black marks have been erased from her credit record, and some equilibrium has returned to her life.

Charles Juntikka, a New York attorney who specializes in credit report litigation, is impressed with what Harding has accomplished in a short time, but warns that negative data sometimes creep back into the credit reports.

Stay vigilant, Juntikka cautions, and "don't assume that once the problem is fixed, it's fixed for good."

Harding may be in a better position to prevent a recurrence than many other victims because of where she lives. California is one of just two states (Texas is the other) that allow identity-theft victims to put a freeze on their credit reports.

Now the only way a bank or other creditor can run a check on Harding is if she gives her permission via a PIN. Under state law, Harding is also entitled to review her credit reports for free every month for a full year to make sure there is no improper activity.

In the coming year, all consumers will be the beneficiaries of greater protections against identity theft. A nationwide system of fraud detection and alerts that is supposed to take effect Dec. 1 creates procedural standards that CRAs must follow to ensure that future requests for credit are legitimate.

It also allows victims to report the crime with a single call. In addition, between now and September 2005, everyone will be able to begin checking their credit report once a year for free.

Harding will certainly be checking hers. She never wants to feel as out of control as she has this past year; she compares the emotional impact of identity theft to battered person syndrome.

While she hopes her nightmare has ended, she concedes, "Once you've been through an experience like this, I don't think you ever really know if it's over for good." ■

Find this article at:

http://money.cnn.com/2004/11/18/pt/security_IDrecovery_0412/index.htm

Check the box to include the list of links referenced in the article.

AMENDMENT

OFFERED IN THE SENATE
TO: SSSB 149

BY SENATOR GUESS

1 Page 5, line 1:

2 Delete "or (2)"

3

4 Page 5, lines 1 - 2:

5 Delete "within three business days after receiving a request under (a)(3) of this
6 section"

7 Insert "immediately after receiving a request under (a)(2) or (3) of this section"

8

9 Page 5, lines 28 - 29:

10 Delete "within three business days after receiving the request"

11 Insert "immediately after receiving the request by telephone or electronic mail or
12 within three business days after receiving the request by certified mail"

13

14 Page 6, line 31, through page 7, line 1:

15 Delete "within three business days"

16 Insert "immediately"

17

18 Page 8, line 18 - 19:

19 Delete "not later than three business days after receiving your request"

20 Insert "immediately after receiving your request if you make the request by telephone
21 or electronic mail, or within three business days after receiving your request if you make the
22 request by certified mail"

LEGAL SERVICES

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

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

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

MEMORANDUM

April 19, 2005

SUBJECT: SSSB 149 relating to personal information
(Work Order No. 24-LS0809\Y)

TO: Senator Gretchen Guess
Attn: Meagan

FROM: Theresa Bannister
Legislative Counsel

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

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

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

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

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

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

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

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

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

Sectional Analysis

Senator Gretchen Guess

April 19, 2005

Page 2

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

Sec. 45.48.090 defines terms for Article 1.

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

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

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

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

Sec. 45.48.130 requires, if a consumer requests it, that a consumer reporting agency allow access by a third party to a consumer's report or information during a security freeze. Describes how the consumer is to make the request and states when the consumer reporting agency is required to comply. Prohibits an agency from releasing a report or information to a third party during a freeze without the consumer's prior express authorization. Requires an agency to notify a consumer if a third party has attempted to access the consumer's report or information during a security freeze and the purpose is not solely for account review. States that this section does not prevent an agency from telling a third party requesting access that a security freeze is in effect.

Sec. 45.48.140 prohibits a consumer reporting agency from removing a security freeze except under certain identified conditions.

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

Sec. 45.48.160 prohibits a consumer reporting agency from charging a consumer for taking an action related to the placement of, removal of, or allowing access to a report on which a freeze has been placed. Makes an exception for repeated loss of personal identification numbers or passwords by the consumer.

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

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

Sec. 45.48.190 establishes the remedies and penalties available for an agency's violation of a security freeze.

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

Sec. 45.48.210 establishes certain exemptions for Article 2.

Sec. 45.48.290 defines terms for Article 2.

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

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

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

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

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

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

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

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

Sec. 45.48.410 establishes certain penalties for knowingly violating sec. 45.48.400.

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

Senator Gretchen Guess

April 19, 2005

Page 4

Sec. 45.48.500 requires a business, when (and after) disposing of records containing personal information, to take reasonable measures necessary to protect against unauthorized access to or use of the records.

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

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

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

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

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

Sec. 45.48.590 defines terms for Article 5.

Article 6. Factual Declaration of Innocence after Identity Theft (secs. 45.48.600 - 45.48.690).

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

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

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

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

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

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

Senator Gretchen Guess

April 19, 2005

Page 5

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

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

Sec. 45.48.690 defines terms for Article 6.

Article 7. Miscellaneous Provisions (secs. 45.48.800 - 45.48.810).

Sec. 45.48.800 prohibits a consumer reporting agency from furnishing a consumer's credit header information to a person unless the person has a permissible purpose under 15 U.S.C. 1681b (Fair Credit Protection Act) to obtain the report. Defines "credit header information."

Sec. 45.48.810 requires a local law enforcement agency with jurisdiction over the individual's actual place of residence to make a report of an individual's identify theft allegations and to provide the individual with a copy.

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

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

Sec. 45.48.990 defines terms for this chapter.

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

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

Section 3. Adds a transition provision for Article 4.

If I may be of further assistance, please advise.

TLB:med

05-272.med



April 12, 2005

The Honorable Con Bunde
Chair, Senate Labor and Commerce Committee
Alaska Senate
State Capitol, Room 506
Juneau, AK 99801-1182

RE: S.B. 148/149 – Request for Amendments

Dear Chairman Bunde:

I write on behalf of the Information Technology Association of America (ITAA), representing over 400 companies in the information technology (IT) industry – the enablers of the information economy. Our members, located throughout the United States, range from the smallest IT start-ups to industry leaders in the custom software, services, systems integration, hardware, telecommunications, Internet, and computer consulting fields.

We share your commitment to addressing security breaches that harm people. Recently, ITAA announced a six-point strategy (enclosed) to enhance the privacy and security of consumer data. ITAA also called for all involved in assuring the privacy of consumer records, including government agencies, the financial services industry, data aggregators and other technology firms, to work together in implementing the strategy.

While we pursue our pro-active strategy to bring business and government together on solutions, we are also addressing the many state legislative proposals that have been advanced. Many, like S.B. 148 and S.B. 149, have sound foundations, but include some provisions that are harmful to electronic commerce and data storage, without commensurate benefits to consumers.

With respect, we would like to recommend the following changes to S.B. 148 and 149 in order to maintain their value, but eliminate the potential for harm.

I. Focus on Potentially Harmful Security Breach

First and foremost, it is important to focus on those security breaches which present real harm or the potential of harm to consumers. Because some, but certainly not all, incidents of security breach are important, it would be counterproductive to treat inconsequential breaches with the same weight as those which represent harm or potential harm to the consumer. There are even documented cases of "false alarms" where student pranksters claimed to have affected a breach, but were later found to be lying. Therefore, employing a mechanism to distinguish among important, inconsequential or even

fictional breaches is crucial to sustaining the public's respect for such notices. We recommend that S.B. 148 and 149 be amended to provide for such a mechanism.

Information Technology Association of America
1401 Wilson Blvd - Suite 1100, Arlington, Virginia 22209-2318 ■ Phone: (703) 522-5055 Fax: (703) 525-2279

The Honorable Con Bunde

April 12, 2005

Page: 2

II. Clarification of "Information Security Policy" Safe Harbor

In order to avoid confusion, the meaning of "information security policy" needs clarification. Most companies and entities describe their security practices within their overall privacy policies. Therefore, the bills should be amended as follows:

"A person that maintains its own notification procedures as part of an information privacy or security policy for the treatment of personal information....."

III. Removal of "E-Sign" Requirement (opt-in) from ability to provide Electronic Notice

S.B. 148 and S.B. 149 allow for notice to be provided electronically "if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. Sec. 7001." While there is a current legal debate as to whether the scope of this E-Sign provision includes government transactions, it certainly covers private transactions, and as such, presents entities who wish to provide notice electronically with significant compliance hurdles.

For example, a government agency or private entity with 1 million email addresses could not use them to send electronic notice until it first determined whether doing so is "consistent" with the federal act. If the act does not apply at all, consistency will exist. If the act does apply, then the agency or entity could not send electronic notice of the security breach (or even make recorded telephone calls), until it *first* provided detailed disclosures about electronic notices generally and also obtained the consent of the consumer to receive electronic notices.

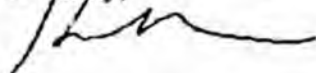
This not only delays notice of the security breach but effectively eliminates the ability of the agency or entity to send electronic notice at all. Absent the ability to send or use electronic notice, the agency/entity must send written notice, but it may not have regular mailing addresses and mailing costs can be prohibitive. Otherwise, the agency/entity could give "substitute notice," but that requires use of "major statewide media," which increases the likelihood of additional fraud by criminals or phishers posing to be representatives of the entity providing notice. **Striking the "E-Sign" requirement will ensure that private communication is facilitated by the bills, not impeded.**

IV. Removal of Private Right of Action

Given the abundance of frivolous civil litigation in the United States, we strongly recommend that this legislation feature an alternative enforcement mechanism to penalize those who recklessly disregard the requirements of this act and whose actions result in demonstrable harm to individuals. We request that the bill's provisions establishing a private right of action against security breaches be deleted.

Thank you for your time and attention to this critical issue.

Sincerely,



Harris N. Miller
President, ITAA

Information Technology Association of America

1401 Wilson Blvd. - Suite 1100, Arlington, Virginia 22209-2318 ■ Phone: (703) 522-5055 Fax: (703) 525-2279



For Immediate Release
March 23, 2005

Contact: Bob Cohen, 703-284-5301, bcohen@itaa.org
Charlie Greenwald, 703-284-5305, cgreenwald@itaa.org

ITAA Calls for More Law Enforcement Resources, Inter-Industry Action to Fight Data Breaches

Arlington, VA, - The Information Technology Association of America (ITAA) today announced a six-point strategy to enhance the privacy and security of consumer data. ITAA also called for all involved in assuring the privacy of consumer records, including government agencies, the financial services industry, data aggregators and other technology firms, to work together in implementing the strategy.

ITAA's plan focuses on three areas: improving law enforcement powers and capabilities to focus on the lawbreakers; reducing the number of breaches; and notifying affected individuals in the event personal data are improperly disclosed or obtained.

"Consumers should not have to worry about their information getting into the hands of identity thieves and other criminals," said ITAA President Harris N. Miller. "People have a reasonable expectation that information they disclose on a credit application or for other purposes will be treated responsibly and that their right to privacy will be protected.

"More emphasis on law enforcement is a key element of this battle because the criminals involved must be identified, prosecuted and punished," Miller continued. "Industry must also step up to the plate. We call on all stakeholders to work together to address this growing problem in a manner that meets and even exceeds society's privacy and security expectations while preserving the efficiency and productivity of electronic records. Custodians of data, government and individuals all have a share of the responsibility in protecting personally identifiable information and other sensitive data and assuring its appropriate use."

The six points of the strategy include the following:

A reasonable and effective national breach notification law applicable to credit reporting agencies as well as other data custodians;

- Such a national law must meet several objectives: establish a clear definition of what constitutes a breach; specify means and methods of notification; identify the level of detailed information to be provided; describe special exceptions and conditions where notification is not provided (as in national security matters); take into account technological approaches to protect data, such as data encryption; assure that the financial risks of non-compliance outweigh the costs of compliance; and preempt state laws and eliminate state-to-state disparities.

A national law enforcement strategy that reinforces prosecutors' tools and increases penalties for individuals who engage in illegally obtaining consumer records, whether electronically or by other deceptive acts;

- A single national law enforcement agency should serve as the primary focus for combating identity theft. This will facilitate closer, systematic cooperation between law enforcement and the financial services and consumer data industries. The rapid exchange of information in real time concerning suspicious activity will help apprehend identity thieves. Similarly, consumers need a single point of contact for reporting incidents and clearing their records. The current patchwork of law enforcement response gives identity criminals extra time to commit their frauds and confuses consumers.

Stronger industry-law enforcement cooperation;

- A series of regional meetings between industry executives and federal, state and local law enforcement would also enhance cooperation between industry and law enforcement to prevent and react to identity theft incidents. Those meetings should be designed to culminate in a body of specific policy recommendations and best practices.

Additional resources for federal, state and local law enforcement to focus on identity thieves;

- Additional resources at all levels of law enforcement are necessary to support investigation of identity theft incidents as well as apprehension of suspects. This additional funding should also support training in identity theft investigations and cooperation with corporations or other industry entities.

Accelerated development and adoption by data aggregators of information security process and methods as well as new technology tools to foil perpetrators and catch offenders;

- A robust and meaningful information security policy is the first line of defense for any organization seeking to assure the confidentiality of electronic records. Promising technologies can improve the identity management process and thereby mitigate the risks of identity theft. Improvements in areas like authentication, credentialing, vetting and issuance must be explored to deter individuals considering identity theft, to block attempts in progress and to prevent breaches in the future. Preventative steps must recognize that identity theft is both an external and an internal threat. To the extent that breaches do occur, mechanisms must also be put in place to re-establish data integrity.

A coordinated inter-industry effort to establish a consensus set of best practices, policy standards, solutions and education;

- A national conference attended by high-level representatives of all industry stakeholders should be held to produce an agreement to develop and pursue a joint strategy to fight identity theft and associated breaches of private data.

The Information Technology Association of America (ITAA) provides global public policy, business networking, and national leadership to promote the continued rapid growth of the IT industry. ITAA consists of over 380 corporate members throughout the U.S. The Association plays the leading role in issues of IT industry concern including information security, taxes and finance policy, digital intellectual property protection, telecommunications competition, workforce and education, immigration, online privacy and consumer protection, government IT procurement, human resources and e-commerce policy. ITAA members range from the smallest IT start-ups to industry leaders in the Internet, software, IT services, ASP, digital content, systems integration, telecommunications, and enterprise solution fields. For more information visit www.itaa.org. ITAA is secretariat of the World Information Technology and Services Alliance, consisting of 65 IT trade associations around the world.

FISCAL NOTE

STATE OF ALASKA
2005 LEGISLATIVE SESSION

Fiscal Note Number: _____
Bill Version: SE149-LAW-C&FB-4-9-C
() Publish Date: _____

Revision Date/Time (Note if correction): _____ Dept. Affected: LAW
Title: "An Act relating to breaches of security involving RDU: CIVIL
personal information; and relating to consumer report..." Component: Commercial & Fair Business
Sponsor: Senator Guess
Requester: Senate Labor and Commerce 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 a Governor's FY 2006 budget proposal:

POSITIONS

Full-time						
Part-time						
Temporary						

ANALYSIS: (Attach a separate page if necessary)
This bill adds 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.
Article 2 adds 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 Daughhete, Director Phone 465-3673
Division: Administrative Services Division Date/Time 4/9/05 2:53 PM
Approved by: Kathryn Daughhete for David Marquez, Attorney General Date 4/9/2005
Agency: Department of Law

FISCAL NOTE

STATE OF ALASKA
2005 LEGISLATIVE SESSION

BILL NO. _____

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.

Article 3 adds a section that requires credit reporting agencies to disclose information in a consumer's credit file upon request by the consumer. Article 4 adds a section that prohibits a person from disclosing the social security number of an individual, or requiring a SSN to access an internet site. Article 5 adds a section that requires a business to implement and monitor a system that requires the disposal of all records that contain personal information. Article 6 adds a section that allows a victim of identity theft to petition the superior court for a determination that the victim is factually innocent of the crime in instances where the perpetrator, using the victim's identify, committed a crime. Article 7 adds a section that prohibits disclosure of credit header information, and provides victims the right to file a police report regarding identify theft.

Each of the articles described in this bill are subject to enforcement by individual consumers by bringing court action for damages injunctive relief, and attorneys' fees and costs. The state is also authorized to bring an action in some circumstances, but is not required to. Passage of this legislation will have no significant fiscal impact on the Department of Law



ALASKA STATE LEGISLATURE
SENATOR GRETCHEN GUESS

Sponsor Statement

Senate Bill 149:

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

The intent of SB 149 is to protect consumers from the growing problem of identity theft and fraud. The measures are designed to secure consumers' private information and ensure consumers will be able to affordably access their credit reports. This problem is growing and consumers must have the tools necessary to fight and prevent identity theft and consumer fraud.

The following are the provisions of the bill.

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

Thank you for your consideration.

January-May: State Cap
June-December: 716 W. 41
Email: Senator.Gretchen

Sponsor Statement

5 • Fax (907) 465-6615
-0120 • Fax (907) 269-0122
www.GretchenGuess.com

SB

157

SENATE COMMITTEE REPORT
First Committee of Referral

DATE: 3/31/05

FURTHER: Finance

Date of 5-Day Notice: _____
 (in accordance with Uniform Rule 23)

DATE TURNED
 IN TO OFFICE: 4/14/05

Labor and Commerce Committee considered SENATE BILL NO. 157

SB 157 REG. COST CHARGES: UTILITIES/PIPELINES

"An Act relating to the maximum annual regulatory cost charge collected from certain regulated public utilities and pipeline carriers; and providing for an effective date."

and recommends:

- be replaced with _____ CS _____ (_____)
- adopt previous _____ CS _____ (_____)
- attached amendment(s)
- adopt Letter of Intent by _____ Committee
- further referral to _____ Committee

CS Senate Bill:	
<input type="checkbox"/>	Same Title
<input type="checkbox"/>	New Title
SCS House Bill:	
<input type="checkbox"/>	Same Title
<input type="checkbox"/>	Technical Title Change
<input type="checkbox"/>	New Title w/ SCR # _____

NEW FISCAL NOTE(S):

Department	Date	Fiscal	Indet.	Zero	FN#
DCED	4/1/05			✓	

PREVIOUS FISCAL NOTE(S):

Department	Date	Fiscal	Indet.	Zero	FN#

APPROPRIATION - no fiscal note

SIGNATURES AND RECOMMENDATIONS:	Do PASS	Do NOT PASS	NO REC	AMEND
<i>Betty Davis</i>	✓			
<i>John Ellis</i>			✗	
<i>John Hines</i>	✓			
CHAIR: <i>A. Brant</i>	✓			

REGULATORY COMMISSION OF ALASKA

TO: CHAIRMAN CON BUNDE, SENATE LABOR AND COMMERCE
FROM: KATE GIARD, RCA
SUBJECT: BENEFIT TO RATEPAYERS FROM RCC IT PROJECTS
DATE: 04/14/05
CC:

Question One: The question has been asked by how Alaska's ratepayers can be assured of a benefit from the RCA's proposed IT Projects which The RCA has esumated that a typical ratepayer with 3 regulated services could pay a total of \$6.48 in increased fees over the three year period.

Question Two: The question was also asked about the RCA's phase-in plan for the IT Projects.

The Chair of the RCA offers these responses.

Question One:

This matter was debated during the January 2005 public meetings held by the Commission. At the time of this discussion, the RCA had crafted a proposal which would have returned the Post IT Project Rate to .685 percent instead of .7 percent to provide a verifiable "payback" to the ratepayers over the course of the following years. This would have equaled a \$97,000 (approximate) reduction in RCA revenues annually after the IT projects were completed. This mechanism, together with the indirect benefits ratepayers received from utility efficiencies (principally addressed by Enstar to the Committee in its comments on April 12) was to deliver ratepayers a more concrete "return on investment".

The Governor's office suggested we reevaluate this approach after learning that the RCA, in this current fiscal year, had to perform a reduction in force, laying off up to 8 positions effective May 2, 2005 because the current RCC rates were not sufficient to maintain the current staffing levels.

Question Two:

The overall goal of these IT Projects, is to put those projects in place early which will allow the RCA to maximize its ability to manage its dockets to a higher level of performance. Subsequently, to fill in with projects that will substantially enhance the RCA's interaction with the public, its utilities and the legislature. Basically, that translates to the RCA putting the Case Management System in place first, following with the Electronic Filing Project for Utilities, then the Electronic Content Management System, followed by the upgrades to the web portal and web site. Last will be the conversion of all of our current data files from pictures and paper to electronic searchable databases. This entire project will span three years, with the majority of the work performed in fiscal 2006 and early 2007. The conversion of the data base may take an additional year, due to the volume of the data resident with the RCA.

SB157



FRANK H. MURKOWSKI
GOVERNOR
GOVERNOR@GOV.STATE.AK.US

P.O. Box 110001
JUNEAU, ALASKA 99811-0001
(907) 465-3500
FAX (907) 465-3532
WWW.GOV.STATE.AK.US

STATE OF ALASKA
OFFICE OF THE GOVERNOR
JUNEAU

March 30, 2005

The Honorable Ben Stevens
President of the Senate
Alaska State Legislature
State Capitol, Room 111
Juneau, AK 99801-1182

Dear President Stevens:

Under the authority of art. III, sec. 18, of the Alaska Constitution, I am transmitting a bill relating to the calculation of the annual regulatory cost charge for public utilities and pipeline carriers within the jurisdiction of the Regulatory Commission of Alaska (RCA).

Currently, the operations of the RCA are financed through a regulatory cost charge collected from regulated public utilities and pipeline carriers in accordance with AS 42.05.254 and AS 42.06.286, which, under existing statute, may not exceed .7 percent of the total adjusted gross revenue applicable to the regulated public utility and pipeline carrier sectors. The bill would increase that percentage to .9 percent for the fiscal years beginning July 1, 2005, July 1, 2006, and July 1, 2007, to finance certain information system improvements within the RCA. The improvements include the implementation of a case management system, a time management system, and an interactive RCA website that would allow regulated entities to electronically file forms and pleadings on-line.

Because it is anticipated that the information system improvements will result in lower operating costs for the RCA, the bill would then reduce that .9 percent maximum regulatory cost charge to the previous .7 percent level for the fiscal year beginning July 1, 2008, and for subsequent fiscal years. This bill would not change the existing maximum for the portion of the regulatory cost charge that finances operations of the public advocacy function under AS 42.04.070(c) and AS 44.23.020(e) within the Department of Law.

I urge your prompt and favorable action on this measure.

Sincerely yours,

Frank H. Murkowski
Governor

Enclosure

COMMITTEE COPY

STATE OF ALASKA

DEPARTMENT OF COMMERCE
COMMUNITY AND ECONOMIC DEVELOPMENT
REGULATORY COMMISSION OF ALASKA

FRANK H. MURKOWSKI, GOVERNOR

701 WEST EIGHTH AVENUE, SUITE 300
ANCHORAGE, ALASKA 99501-3469
PHONE: (907) 276-6222
FAX: (907) 276-0160
TTY: (907) 276-4533
WEBSITE: www.state.ak.us/rca/

April 7, 2005

The Honorable Con Bunde, Chairman
Senate Labor & Commerce Committee
Alaska State Legislature
State Capitol, MS 301
Juneau, Alaska 99801-1182

RE: SB 157 - An Act relating to the maximum annual regulatory cost charge collected from certain regulated public utilities and pipeline carriers; and providing for an effective date

Dear Chairman Bunde:

On March 31, 2005, SB 157 (Companion Bill HB 243) was introduced by the Senate Rules committee on behalf of the Governor and referred to your committee. The purpose of this legislation is to increase the regulatory cost charge (RCC) rate from 0.7 percent to 0.9 percent for three years to fund efforts to improve the RCA's timeliness, accountability and regulatory transparency.

In July 2004, the Commission initiated a comprehensive effort to understand and respond to concerns about aspects of its regulatory operations. Over the past several years, the Commission has received comment that its decisions took too long, that the cost of regulation was burdensome and that utilities could not track the progress of their cases through the RCA's adjudicatory process. While some of these issues naturally exist within the regulatory paradigm, I strongly believe the process itself is within our control and we can improve it.

In the last few months, the Commission significantly reorganized its structure. We visited with CEOs of utilities and pipelines. We opened our 2005 regulations schedule for public and industry comment, a first, I believe. We also proposed to purchase and implement data systems designed to achieve the results sought by regulated entities including (1) a system to track cases, staff resources and timelines; (2) a system to receive, store and retrieve data filed with the RCA electronically; and (3) a web site allowing citizens and regulated entities to electronically track regulatory matters.

Last winter, the Commission held public meetings, taking testimony from interested parties as to whether an increase in the RCC should be used to fund



RECYCLED
PAPER

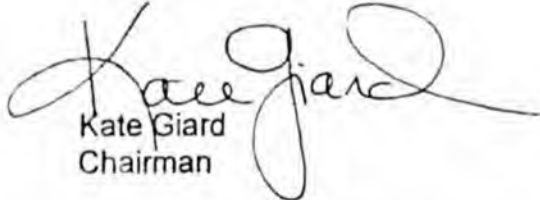
these data systems. An advisory group volunteered to work with us, reviewing the overall scope of the project and budget. Written and oral testimony from regulated utilities and pipelines supported both implementing the data systems and the RCC funding mechanism.

Regulated entities generally pass the RCC cost to consumers. Having concern for consumer impact, we calculated that this legislation would increase utility costs for consumers by an average of six (6) cents per month, per regulated service. If a consumer uses three regulated services, (generally telephone, gas and electric) the cumulative impact would be \$2.16 per year or \$6.48 for the three years this legislation is in effect.

We respectfully request that you schedule SB 157 for hearing in your committee, and we urge favorable action on this bill. Attached is the related fiscal note describing impact of the increased RCC. I would be pleased to meet with you and committee Members, if you wish, to provide any other information you may require.

Thank you for considering this request, which we believe is both in the best interest of and supported by industry.

Sincerely,



Kate Giard
Chairman

Attachment: SB 157 Fiscal Note

FISCAL NOTE

STATE OF ALASKA
2005 LEGISLATIVE SESSION

Fiscal Note Number: _____
 Bill Version: SB 157
 () Publish Date: _____

Revision Date: Corrected 4/7/05 Dept. Affected: Commerce
 Title: Regulatory Cost Charges: Utilities and Pipelines RDU: Regulatory Commission of Alaska (399)
 Component: Regulatory Commission of Alaska
 Sponsor: Rules by Request of the Governor
 Requester: Senate Labor & Commerce Component No: 2417

Expenditures/Revenues (Thousands of Doll: _____)

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

OPERATING EXPENDITURES	FY 200C	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
Personal Services						
Travel						
Contractual	1,300.0	1,300.0	1,300.0			
Supplies						
Equipment						
Land & Structures						
Grants & Claims						
Miscellaneous						
TOTAL OPERATING	1,300.0	1,300.0	1,300.0	0.0	0.0	0.0

CAPITAL EXPENDITURES						
-----------------------------	--	--	--	--	--	--

CHANGE IN REVENUES (1141)	1,300.0	1,300.0	1,300.0			
----------------------------------	----------------	----------------	----------------	--	--	--

FUND SOURCE (Thousands of Dollars)

1002 Federal Receipts						
1003 GF Match						
1004 GF						
1005 GF/Program Receipts						
1037 GF/Mental Health						
1141 RCA Receipts	1,300.0	1,300.0	1,300.0			
TOTAL	1,300.0	1,300.0	1,300.0	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 statutory revision allows for a three year increase in the Regulatory Cost Charge (RCC) rate from .007 to .009 to fund several initiatives that will improve the agency's ability to mitigate regulatory lag, reduce utilities' filing costs and increase transparency in agency activities. It is anticipated that this legislation will increase utility costs by approximately 6 cents per month or 72 cents per year, per regulated utility service. If a consumer uses three regulated services, (generally telephone, gas and electric) the approximate cumulative impact would be \$2.16 per year or \$6.48 for the three year period.

Prepared by: Kate Giard, Chair Phone 907.276.6222
 Division: Regulatory Commission of Alaska Date/Time 4/7/05 10:53 AM
 Approved by: Edgar Blatchford, Commissioner Date 4/7/2005
 Agency: Commerce, Community, and Economic Development

SB

165

SENATE COMMITTEE REPORT
First Committee of Referral

TE: 4/8/05

FURTHER: Finance

Notice of 5-Day Notice: _____
 accordance with Uniform Rule 23)

DATE TURNED
 IN TO OFFICE: _____

For and Commerce Committee considered SENATE BILL NO. 165

SB 165 CARD ROOMS & OPERATIONS

Act relating to card rooms and card operations."

Committee recommends:

- be replaced with _____ CS _____ (_____)
- adopt previous _____ CS _____ (_____)
- attached amendment(s)
- adopt Letter of Intent by _____ Committee
- further referral to _____ Committee

CS Senate Bill:	
<input type="checkbox"/>	Same Title
<input type="checkbox"/>	New Title
SCS House Bill:	
<input type="checkbox"/>	Same Title
<input type="checkbox"/>	Technical Title Change
<input type="checkbox"/>	New Title w/ SCS # _____

NEW FISCAL NOTE(S):

PREVIOUS FISCAL NOTE(S):

Department	Date	Fiscal	Indet.	Zero	FN#

Department	Date	Fiscal	Indet.	Zero	FN#

APPROPRIATION - no fiscal note

SIGNATURES AND RECOMMENDATIONS:	DO PASS	DO NOT PASS	NO REC	AMEND
<i>Betty Davis</i>				X
<i>John E. Ellis</i>			X	
<i>Stephen Leebins</i>				X
<i>Ben Thomas</i>	X			
CHAIR: <i>Ben Thomas</i>	✓			

LEGAL SERVICES

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

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

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

MEMORANDUM

April 21, 2005

SUBJECT: Card Rooms and Indian Gaming (HB 272)

TO: Representative Pete Kott

FROM: Kathryn L. Kurtz *KK*
Legislative Counsel

You asked whether this bill would affect Indian gaming in Alaska. I do not think this bill will open the door to class three gaming.

The federal Indian Gaming Regulatory Act (IGRA), 25 U.S.C. § 2701 et seq., gives Indian tribes the authority to conduct gaming and gambling on Indian lands. The Indian Gaming Regulatory Act divides gaming into three classes:

- (1) Class I gaming includes social gaming for minimal prizes and traditional Indian gaming conducted at ceremonies or celebrations;
- (2) Class II gaming includes bingo, lotto, pull-tabs, punch boards, tip jars and non banking card games, as well as banking card games operated on or before May 1, 1988;¹ and
- (3) Class III gaming includes casino-type gambling, pari-mutual horse and dog racing, lotteries, and all other forms of gaming that are not class I or II gaming.

Class I gaming on Indian lands is within the exclusive jurisdiction of the tribes and is excluded from the provisions of the IGRA. Class II gaming on Indian lands is within the jurisdiction of the tribes but is subject to the provisions of the IGRA, including oversight by the National Indian Gaming Commission. For example, an Indian tribe seeking to conduct bingo games could choose to do so under the authority of state law or could do

¹ Class II gaming does not include:

- (i) any banking card games, including baccarat, chemin de fer, or blackjack (21), or
- (ii) electronic or electromechanical facsimiles of any game of chance or slot machines of any kind.

25 U.S.C. § 2703(b).

Representative Pete Kott
April 21, 2005
Page 2

so separately under a permit from the National Indian Gaming Commission. Class III gaming activities are lawful on Indian lands only if authorized by a tribal ordinance or resolution, the activities are conducted on lands located in a state that permits such gaming for any purpose by any person, organization, or entity, and the activities are conducted in conformance with a tribal-state compact entered into by the tribe and state.

The Act provides a framework for negotiation of a tribal-state compact -- the tribe requests the state to enter into negotiations; upon receiving such a request, the state "shall" negotiate with the tribe in "good faith" to enter into such a compact.

There has been a good deal of litigation involving the various provisions of the IGRA since its passage. Some of that has involved the definition of "Indian lands." Although Alaska has only one remaining reservation, it is not safe to assume that there are no other "Indian lands" in Alaska. There certainly are parcels that are held in trust by the United States that might qualify for purposes of IGRA.

This underscores the significance of the difference between class II and class III gaming. If the legislature permitted class III gaming in state law, it would pave the way for tribes to conduct class III gaming on Indian lands under federal law. However, HB 272 permits only non-banking card games, specifically poker, pan, rummy, bridge, and cribbage games. Poker falls under IGRA's definition of class II games. 25 C.F.R. 502.3; National Indian Gaming Commission Opinion dated June 17, 1999, Re: Game Classification Opinion - "Poker Club."² House banked card games, such as blackjack and baccarat, as well as player banked games, such as chemin de fer, are class III games, 25 C.F.R. 502.4; National Indian Gaming Commission Bulletin No. 95-1, April 10, 1995, but those types of games are not permitted in card rooms under HB 272.

KLK:med
05-284.med

² According to this National Indian Gaming Commission opinion, "Banking games, as commonly understood and defined in the NIGC regulations, are games in which the banker (usually the house) takes on, that is, competes against, all players, collecting from losers and paying winners. See 25 C.F.R. 502.11(c). Conversely, non-banking card games are games where players play against each other. Poker is the typical example of a non-banking card game." The opinion went on to conclude that the proposed poker club would constitute class II, rather than class III gaming: "[A]s proposed, the players in the Nation's Club would play against each other in a non-banking format, not against the house or other banker. Turning Stone and its dealers would not have an interest, financial or otherwise, in the outcome of any poker game. Thus, the poker games to be played at the Club qualify as non-banking card games."

SENATOR
JOHN J.
COWDERY

Anchorage



Senate

January - May:
State Capitol, Suite 101
Juneau, Alaska 99801 - 1182
Tel: 907-465-3879
Toll Free: 888-269-3879
Fax: 907-465-2069

May - December:
716 W. 4th Avenue
Anchorage, Alaska 99501
Tel: 907-269-0222
Fax: 907-269-0223

Senator_John_Cowdery@legis.state.ak

Committees

Chair: Rules

Chair: World Trade &
State/Federal Relations

Vice-Chair: Transportation

Legislative Council

To: Senator Con Bunde, Chairman
Senate Labor and Commerce Committee

From: Senator Cowdery

Date: 4/19/2005

Re: SB 165 - Change between SB165 Version Y and CS for SB 165 Version L

Sec. 05.18.030

Adds "rake" to the title of the section.

Gives the Department the power to determine maximum rake for games played in card room.

Also removes minimum wager, so that department only decides maximum wager on games.

Adds provision that only players in a card game may place a wager related to that game.

Sec. 05.18.200

Changes licensing for card rooms. If population is lower than 30,000 people, a license may be issued only if an ordinance is adopted by the municipality and ratified by a vote of the people

Changes number of licensed facilities so that a population of 30-59,999 can have two facilities and a population of 60,000 or more can have a maximum of three card rooms.

Sec. 05.18.210

Removes "submission of design" from section title.

This has been removed because the section doesn't relate to design

Sec. 05.18.900

Under Definitions

Adds (13) "player" means an individual actively participating in a card game;

Adds (14) "rake" means a set fee or percentage of the total amount wagered by all players in a game in the course of that game.

24-LS0767L
Kurtz
4/12/05

CS FOR SENATE BILL NO. 165()
IN THE LEGISLATURE OF THE STATE OF ALASKA
TWENTY-FOURTH LEGISLATURE - FIRST SESSION

BY

Offered:
Referred:

Sponsor(s): SENATOR COWDERY

A BILL
FOR AN ACT ENTITLED

1 **"An Act relating to card rooms and card operations."**

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

3 *** Section 1.** The uncodified law of the State of Alaska is amended by adding a new section
4 to read:

5 **LEGISLATIVE INTENT.** This chapter is intended to benefit the people of Alaska by
6 promoting tourism and assisting economic development. The public's confidence and trust
7 will be maintained only through the comprehensive law enforcement supervision and strict
8 regulation of card rooms and card operations under AS 05.18.

9 *** Sec. 2.** AS 05 is amended by adding a new chapter to read:

10 **Chapter 18. Card Rooms.**

11 **Article 1. Card Games and Card Rooms.**

12 **Sec. 05.18.010. Card rooms.** (a) Notwithstanding AS 11.66, a person may
13 establish and operate a card room in the state if the person complies with the licensing
14 and other requirements of this chapter, as well as the statutory requirements applying
15 to businesses generally.

1 (b) The following non-banking card games may be played in a card room,
2 according to rules prescribed in regulation by the department:

- 3 (1) poker;
4 (2) pan;
5 (3) rummy;
6 (4) bridge; and
7 (5) cribbage.

8 **Sec. 05.18.020. Presence of department employees in card rooms.**
9 Employees of the department have the right to be present in a card room or any
10 adjacent facilities under the control of a licensed owner.

11 **Sec. 05.18.030. Wagers and rake.** (a) The department shall determine the
12 maximum amount a player may wager in a card game. The department shall set the
13 maximum rake a licensed owner may collect from players in a card game for
14 providing a dealer, table, location for playing the card game, or other services related
15 to the card game.

16 (b) A licensed owner may not permit any form of wagering on card games
17 except as permitted under this chapter.

18 (c) Only a player in a card game may place a wager relating to that game. A
19 player in a card game may not place a wager relating to that game on behalf of another
20 individual.

21 (d) Wagering may not be conducted with money or other negotiable currency.

22 (e) All tokens or chips that are used to make wagers must be purchased from
23 the owner of the card room while the purchaser is in the card room or at a facility that
24 is adjacent to the card room and has been approved by the department. The tokens or
25 chips may be purchased by means of an agreement under which the licensed owner
26 extends credit to the patron.

27 **Sec. 05.18.040. Persons under 21 years of age.** (a) A person who is under
28 21 years of age may not be present in a card room.

29 (b) A person who is under 21 years of age may not make a wager under this
30 chapter.

31 **Article 2. Administration.**

1 **Sec. 05.18.100. Administration, regulation, and enforcement.** (a) The
2 department shall administer, regulate, and enforce the provisions of this chapter. The
3 department

4 (1) shall have all powers and duties specified in this chapter;

5 (2) shall have all powers necessary to execute this chapter;

6 (3) shall exercise jurisdiction and supervision over the following:

7 (A) all authorized card operations in the state;

8 (B) all persons in card rooms where card operations are
9 conducted;

10 (4) shall investigate and reinvestigate applicants and license holders
11 and determine the eligibility of applicants for licenses and to require applicants and
12 license holders to reimburse the department for the costs of the investigation and
13 reinvestigation;

14 (5) shall select from among competing applicants the applicants that
15 promote the most economic development and that best serve the interests of the
16 citizens of the state;

17 (6) shall take appropriate administrative enforcement or disciplinary
18 action against a licensee under this chapter that violates the provisions of this chapter;

19 (7) shall investigate alleged violations of this chapter;

20 (8) shall establish fees for the review and investigation of applications
21 for the licenses that are authorized under this chapter;

22 (9) may conduct hearings;

23 (10) may issue subpoenas to compel the attendance of witnesses and
24 subpoenas duces tecum for the production of books, records, and other relevant
25 documents;

26 (11) may administer oaths and affirmations to witnesses;

27 (12) shall prescribe a form to be used by a licensed owner as an
28 application for employment by potential employees of the card room and licensees of
29 the department;

30 (13) may revoke, suspend, or renew licenses issued under this chapter;

31 (14) may hire employees to gather information, conduct investigations,

1 and carry out other tasks under this chapter;

2 (15) may take any appropriate action to enforce this chapter, including
3 the issuance of notices of violations of this chapter or regulations of the department,
4 orders to cease and desist, and closure orders;

5 (16) may adopt regulations for the implementation and enforcement of
6 this chapter;

7 (17) shall adopt regulations governing the conduct of card games that
8 may be played in card rooms;

9 (18) shall adopt regulations specifying the form and amount of charges
10 a card room may impose on players for playing card games in the card room;

11 (19) may, through the office of the attorney general, apply to the courts
12 for injunctive and declaratory relief in aid of any action or decision of the department
13 on any matter within the jurisdiction of the department.

14 (b) The Department of Public Safety and the attorney general may assist the
15 department in conducting background investigations of applicants. The department
16 shall reimburse the Department of Public Safety for the costs incurred by the
17 department as a result of assistance provided to the department under this section. The
18 department shall make the payment from fees collected from applicants for licenses.

19 **Sec. 05.18.110. Violations; fees; inspections.** (a) The department shall

20 (1) provide for the establishment and collection of license fees
21 imposed under this chapter and deposit the license fees in the state gaming fund;

22 (2) levy and collect penalties for noncriminal violations of this chapter
23 and deposit the penalties in the state gaming fund.

24 (b) The department may enter an office, a card room, or other premises of a
25 person holding an owner's license where evidence of compliance or noncompliance
26 with this chapter is likely to be found.

27 **Sec. 05.18.120. Licensing.** (a) The department shall adopt standards for the
28 licensing of persons regulated under this chapter.

29 (b) The department shall require that the records, including financial
30 statements, of a person holding an owner's license must be maintained in the manner
31 prescribed by the department.

1 (c) The department may not issue a license to a person who has been
2 convicted of a felony in this or another jurisdiction.

3 (d) An applicant for a license under this chapter shall provide the following
4 information to the department:

5 (1) the name, business address, and business telephone number of the
6 applicant;

7 (2) an identification of the applicant;

8 (3) the following information for an applicant that is not an individual:

9 (A) the state of incorporation and any states where the
10 corporation is registered to do business;

11 (B) the names and addresses of all corporate officers;

12 (C) the identity of

13 (i) any entity in which the applicant has an equity
14 interest of at least 20 percent; the identification must include the state
15 of incorporation or registration, if applicable; however, an applicant
16 that has a pending registration statement filed with the United States
17 Securities and Exchange Commission is not required to provide
18 information under this item;

19 (ii) the shareholders or participants of the applicant; an
20 applicant that has a pending registration statement filed with the United
21 States Securities and Exchange Commission is required to provide only
22 the names of persons holding an interest of more than 20 percent of all
23 shares;

24 (4) an identification of any business, including the state of
25 incorporation and all states where the business is registered to do business, if
26 applicable, in which an applicant or the spouse or children of an applicant has an
27 equity interest of more than 20 percent of all shares;

28 (5) if the applicant has been indicted, been convicted, pled guilty or
29 nolo contendere, or forfeited bail concerning a criminal offense other than a traffic
30 violation under the laws of any jurisdiction, the applicant must include the following
31 information under this paragraph:

1 (A) the name and location of the court, the arresting agency,
2 and the prosecuting agency;

3 (B) the case number;

4 (C) the date and type of offense;

5 (D) the disposition of the charge;

6 (E) the location and length of incarceration, if any;

7 (6) a statement of whether the applicant has filed or had filed against
8 the applicant a proceeding in bankruptcy or been involved in a formal process to
9 adjust, defer, suspend, or work out the payment of a debt, including the date of filing,
10 the name and location of the court, and the case and number of the disposition;

11 (7) a statement of whether the applicant has filed or been served with a
12 complaint or notice filed with a public body concerning a delinquency in the payment
13 of or a dispute over a filing concerning the payment of a tax required under federal,
14 state, or local law, including the amount, type of tax, taxing agency, and times
15 involved;

16 (8) the name and business telephone number of the attorney who will
17 represent the applicant in matters before the department;

18 (9) a description of a proposed or an approved card room, including
19 the expected economic benefit to local communities;

20 (10) the following information from each licensee involved in the
21 ownership or management of card operations:

22 (A) an annual balance sheet;

23 (B) an annual income statement;

24 (C) a list of the stockholders or other persons having at least 20
25 percent beneficial interest in the card room activities of the person who has
26 been issued the owner's license;

27 (D) any other information the department considers necessary
28 for the effective administration of this chapter.

29 (e) The department shall review and approve or disapprove promptly and in
30 reasonable order all license applications.

31 (f) A party aggrieved by an action of the department denying, suspending,

1 revoking, restricting, or refusing the renewal of a license may request a hearing before
2 the department. A request for a hearing must be made to the department in writing not
3 more than 10 days after service of notice of the action of the department.

4 (g) Except as provided in AS 05.18.170, the department shall serve notice of
5 the department's actions under this section on a party by personal delivery or by
6 certified mail. Notice served by certified mail is considered complete on the business
7 day following the date of the mailing.

8 (h) The department shall conduct all requested hearings under this section
9 promptly and in reasonable order.

10 **Sec. 05.18.130. Card room advisory board.** (a) The governor shall appoint
11 five individuals to serve on a card room advisory board. Appointments to the board
12 shall be for a period of five years.

13 (b) The card room advisory board shall make recommendations to the
14 department relating to license applications and policy issues relating to card rooms

15 (c) Members of the card room advisory board serve without compensation and
16 are not entitled to per diem and travel expenses authorized by law for boards and
17 commissions under AS 39.20.180.

18 **Sec. 05.18.140. Violations of chapter; fraudulent acts.** If a licensee or an
19 employee of a licensee violates this chapter or engages in a fraudulent act, the
20 department may

21 (1) suspend, revoke, or restrict the license of a licensee;

22 (2) require the removal of a licensee or an employee of a licensee from
23 the card room;

24 (3) impose a civil penalty of not more than \$5,000 against an
25 individual who has been issued an occupational license for each violation of this
26 chapter;

27 (4) impose for each violation of this chapter by a licensed owner a
28 penalty of not more than the greater of \$10,000 or an amount equal to the licensee's
29 daily gross receipts for each day of the violation.

30 **Sec. 05.18.150. Investigative procedure; complaints.** (a) The department
31 shall review and make a determination on a complaint by a person who has been

1 issued an owner's license concerning an investigative procedure that the licensee
2 alleges is unnecessarily disruptive of card operations.

3 (b) A licensee filing a complaint under this section must prove by clear and
4 convincing evidence that the investigative procedure

5 (1) does not have a reasonable law enforcement purpose; and

6 (2) is so disruptive as to unreasonably inhibit card operations.

7 (c) For purposes of this section, the need to inspect and investigate a licensee
8 shall be presumed at all times.

9 **Sec. 05.18.160. Transfer of licenses; rules of procedure; prohibitions.** (a)

10 A licensed owner or another person shall apply for and must receive the department's
11 approval before an owner's license is transferred, sold, or purchased or a voting trust
12 agreement or other similar agreement is established with respect to the owner's
13 license. A licensed owner or another person may not lease, hypothecate, or borrow or
14 loan money against an owner's license.

15 (b) The department shall adopt regulations governing the procedure a licensed
16 owner or another person shall follow to take an action under (a) of this section. The
17 regulations must specify that a person who obtains an ownership interest in a license
18 shall meet the criteria of this chapter and regulations adopted by the department. A
19 licensed owner may transfer an owner's license only in accordance with this chapter
20 and regulations adopted by the department.

21 **Sec. 05.18.170. Suspension of license without notice or hearing; revocation**
22 **of license.** (a) The department may suspend a license issued to the owner of a card
23 room without notice or hearing if the department determines that the safety or health
24 of patrons or employees would be threatened by the continued operation of the card
25 room. The opportunity for a hearing shall be provided within a reasonable time
26 following a suspension.

27 (b) The suspension of a license under this section may remain in effect until
28 the department determines that the cause for suspension has been abated. The
29 department may revoke the license if the department determines that the owner has not
30 made satisfactory progress toward abating the hazard.

31 **Sec. 05.18.180. Department records.** (a) Notwithstanding any other law,

1 upon written request from a person, the department shall provide the following
2 information to the person:

3 (1) the information provided under this chapter concerning a licensee
4 or an applicant;

5 (2) a copy of a letter providing the reasons for the denial of an owner's
6 license;

7 (3) a copy of a letter providing the reasons for the department's refusal
8 to allow an applicant to withdraw the applicant's application.

9 (b) The department may assess fees for the copying of information provided
10 by the department to a person requesting information under (a) of this section.

11 Article 3. Licenses.

12 Sec. 05.18.200. Owner's licenses. (a) The department may issue to a person
13 a license to own a card room and conduct card games. If the population of a
14 municipality is less than 30,000, only one owner's license may be issued in the
15 municipality. If the population of a municipality is 30,000 or more, but less than
16 60,000, two owner's licenses may be issued in the municipality. If the population of a
17 municipality is 60,000 or more, a maximum of three owner's licenses may be issued in
18 the municipality. The department may not issue an owner's license for a card room in
19 a municipality with a population of less than 30,000 unless the municipality has
20 adopted an ordinance, ratified by a majority of the municipal voters voting on the
21 question, authorizing operation of a card room in the municipality.

22 (b) A person applying for an owner's license under this chapter shall pay a
23 nonrefundable \$25,000 application fee to the department.

24 (c) An applicant shall submit the following on forms provided by the
25 department:

26 (1) the information required under AS 05.18.120;

27 (2) if the applicant is an individual, two sets of the individual's
28 fingerprints;

29 (3) if the applicant is not an individual, two sets of fingerprints for
30 each officer and director who will actively participate in the daily operation of the
31 business of the applicant.

1 (d) The department shall review an application for an owner's license under
2 this chapter and inform each applicant of the department's decision concerning the
3 issuance of an owner's license.

4 (e) The costs of investigation of an applicant for an owner's license under this
5 chapter shall be included in the application fee paid by the applicant.

6 (f) An applicant for an owner's license under this chapter shall pay all
7 additional costs that are associated with the investigation of the applicant that exceed
8 the portion of the application fee paid by the applicant that is assessed for the
9 investigation.

10 (g) The department may not issue an owner's license under this chapter to a
11 person if the person

12 (1) has been convicted of a felony under the laws of the state, the laws
13 of another state, or laws of the United States;

14 (2) has knowingly or intentionally submitted an application for a
15 license under this chapter that contains false information;

16 (3) is an officer, a director, or a managerial employee of a person
17 described in (1) or (2) of this subsection; or

18 (4) employs an individual described in (1), (2), or (3) of this subsection
19 and that individual participates in the management or operation of card operations
20 authorized under this chapter.

21 **Sec. 05.18.210. Factors considered in granting owner's licenses.** In
22 determining whether to grant an owner's license to an applicant, the department shall
23 consider

24 (1) the character, reputation, experience, and financial integrity of

25 (A) the applicant;

26 (B) a person that

27 (i) directly or indirectly controls the applicant; or

28 (ii) is directly or indirectly controlled by the applicant

29 or by a person that directly or indirectly controls the applicant;

30 (2) the card room or proposed card room;

31 (3) the good faith affirmative action plan of each applicant to recruit,

1 train, and upgrade minorities in all employment classifications;

2 (4) the financial ability of the applicant to purchase and maintain
3 adequate liability and casualty insurance;

4 (5) whether the applicant has adequate capitalization to provide and
5 maintain the card room for the duration of the license;

6 (6) the extent to which the applicant exceeds or meets other standards
7 adopted by the department by regulation.

8 **Sec. 05.18.220. Issuance of license; fee; bond.** (a) The department may
9 issue an owner's license to an eligible person if the person pays an initial license fee
10 and posts a bond as required in this section. The annual license fee is \$10,000 for each
11 card table. After a license has been issued, additional tables may be added for an
12 initial license fee of \$10,000 each; however, the full annual renewal fee for each table
13 must be paid on or before the anniversary of issuance of the owner's license,
14 regardless of when the table was added. The department may suspend or revoke a
15 license if the annual license fee is not paid in a timely fashion.

16 (b) A licensed owner must post a \$500,000 cash bond with the department at
17 least 60 days before the commencement of the construction of a card room or the
18 commencement of a card operation under the license, whichever is earlier.

19 (c) The principal of the bond shall be placed without restriction at the disposal
20 of the department, but interest earned on the principal shall inure to the benefit of the
21 licensee.

22 (d) The bond is subject to the approval of the department and must be payable
23 to the department for use by the department in satisfaction of the licensed owner's
24 financial obligations to the local community, the state, and other parties, as determined
25 by regulations of the department.

26 (e) If, following a hearing held after at least 15 days written notice, the
27 department determines that the amount of a licensed owner's bond is insufficient, the
28 licensed owner shall, upon written demand of the department, file a new bond.

29 (f) The department may require a licensed owner to file a new bond with a
30 satisfactory surety in the same form and amount if

31 (1) liability on the old bond is discharged or reduced by judgment

1 rendered, payment made, or otherwise; or

2 (2) in the opinion of the department, a surety on the old bond becomes
3 unsatisfactory.

4 (g) If a new bond obtained under (e) or (f) of this section is unsatisfactory, the
5 department shall cancel the owner's license. If the new bond is satisfactorily
6 furnished, the department shall release, in writing, the surety on the old bond from any
7 liability accruing after the effective date of the new bond.

8 (h) The total and aggregate liability of the surety on a bond is limited to the
9 amount specified in the bond, and the continuous nature of the bond may not be
10 construed as allowing the liability of the surety under a bond to accumulate for each
11 successive approval period during which the bond is in force.

12 (i) A bond filed under this section is released 60 days after the owner's license
13 expires and a written request for release is submitted by the licensed owner.

14 **Sec. 05.18.230. Tournaments.** The holder of an owner's license for a card
15 room shall host a card tournament at least once each calendar quarter, with the
16 proceeds of the tournament to be distributed to a nonprofit educational institution or
17 group designated by the owner. An application for issuance or renewal of an owner's
18 license must include proposed dates for the tournaments, and specify the nonprofit
19 educational institution or group designated to benefit from each tournament. The
20 licensed owner shall notify the department of any change in the date or beneficiary of
21 a tournament. A nonprofit educational institution or group may be the designated
22 beneficiary of only one tournament each year under this section.

23 **Sec. 05.18.240. Term of a license.** An owner's initial license expires five
24 years after the effective date of the license.

25 **Sec. 05.18.250. Revocation of owner's license for delay.** The department
26 may revoke an owner's license if

27 (1) the licensee begins regular operations more than 12 months after
28 receiving the department's approval of the application for the license; and

29 (2) the department determines that the revocation of the license is in
30 the best interests of the state.

31 **Sec. 05.18.260. Renewal of owner's license; compliance investigations.** (a)

1 The owner's license may be renewed for an additional five-year period, if the bond
2 required under AS 05.18.220 remains in force, the annual license fees have been paid
3 in a timely fashion, and the requirements of this section are met.

4 (b) A licensed owner shall undergo a complete investigation by the
5 department every five years to determine whether the licensed owner remains in
6 compliance with this chapter.

7 (c) Notwithstanding (b) of this section, the department may investigate a
8 licensed owner at any time the department determines necessary to ensure that the
9 licensee remains in compliance with this chapter.

10 (d) The licensed owner shall bear the cost of an investigation or
11 reinvestigation of the licensed owner and an investigation resulting from a potential
12 transfer of ownership.

13 **Sec. 05.18.270. Schools for training occupational licensees.** This chapter
14 does not prohibit a licensed owner from operating a school for the training of
15 occupational licensees.

16 **Sec. 05.18.280. Nature of license.** An owner's license is a revocable privilege
17 granted by the state and is not a property right.

18 **Sec. 05.18.290. Occupations requiring license.** The department shall
19 determine the occupations related to card games and card rooms that require a license
20 under this chapter. The department shall require that an individual applying for an
21 occupational license may manage card operations for only one licensed owner.

22 **Sec. 05.18.300. Occupational license; requirements; fees; duration;
23 renewal; compliance investigations.** (a) The department may issue an occupational
24 license to an individual if

25 (1) the individual has applied for the occupational license and provided
26 the information required under AS 05.18.120;

27 (2) a nonrefundable application fee set by the department has been
28 paid on behalf of the applicant in accordance with (b) of this section;

29 (3) the department has determined that the applicant is eligible for an
30 occupational license; and

31 (4) an annual license fee set by the department has been paid on behalf

1 of the applicant in accordance with (b) of this section.

2 (b) A licensed owner or an applicant for an owner's license shall pay the
3 application fee of an individual applying for an occupational license to work at the
4 licensed owner's card operation and any renewal fees on behalf of an employee or
5 potential employee. The licensed owner or applicant for an owner's license may seek
6 reimbursement of the application fee or annual license fee from an employee who is
7 issued an occupational license by the department.

8 (c) A license issued under this section is valid for two years after the date of
9 issuance.

10 (d) Unless an occupational license is suspended, expires, or is revoked by the
11 department, the occupational license may be renewed annually upon the payment of a
12 license renewal fee by the licensed owner on behalf of the licensee, or by the licensee
13 in an amount established by the department and a determination by the department that
14 the licensee is in compliance with this chapter.

15 (e) The department may investigate the holder of an occupational license at
16 any time the department determines necessary to ensure that the licensee is in
17 compliance with this chapter.

18 (f) A licensed owner or an applicant for an owner's license shall pay the cost
19 of an investigation or reinvestigation by the department of a holder of an occupational
20 license who is employed by the licensed owner. The licensed owner or applicant for
21 an owner's license may seek reimbursement of the cost of an investigation or
22 reinvestigation from an employee who holds an occupational license.

23 **Sec. 05.18.310. Qualifications for occupational license.** The department
24 may not issue an occupational license to an individual unless the individual

25 (1) is at least 21 years of age;

26 (2) has not been convicted of a felony under the laws of this state, the
27 laws of another state, or the laws of the United States;

28 (3) has demonstrated a level of skill or knowledge that the department
29 determines is necessary to operate card games; and

30 (4) has met standards of character and fitness adopted by the
31 department for the holding of an occupational license.

1 **Sec. 05.18.320. Application for occupational license.** (a) An application for
2 an occupational license shall be made on forms prescribed by the department and
3 contain all information required by the department.

4 (b) An applicant for an occupational license shall provide the following
5 information in the application:

6 (1) a statement of whether the applicant has held any other licenses
7 related to card rooms;

8 (2) if the applicant has been licensed in another state under any other
9 name, the name under which the applicant was licensed in the other state;

10 (3) the applicant's age.

11 (c) An applicant for an occupational license shall submit with the application
12 two sets of the applicant's fingerprints. The applicant must submit the fingerprints on
13 forms provided by the department. The department shall charge each applicant the fee
14 set by the Department of Public Safety for state and national fingerprint record
15 searches.

16 **Sec. 05.18.330. Restrictions on issuance of occupational license.** The
17 department may refuse to issue an occupational license to an individual who

18 (1) is unqualified to perform the duties required of the applicant;

19 (2) does not disclose or states falsely any information required by the
20 application;

21 (3) has been found guilty of a violation of this chapter; or

22 (4) has not met standards of character and fitness adopted by the
23 department for the holding of an occupational license.

24 **Sec. 05.18.340. Suspension, revocation, or restriction of licenses.** The
25 department may suspend, revoke, or restrict an occupational licensee for

26 (1) a violation of this chapter;

27 (2) a cause that, if known to the department, would have disqualified
28 the applicant from receiving the occupational license;

29 (3) a default in the payment of an obligation or a debt due to the state;

30 or

31 (4) any other just cause.

1 **Sec. 05.18.350. Schools for training occupational licensees.** (a) This
2 chapter does not prohibit a licensed owner from entering into an agreement with a
3 school approved by the department for the training of an occupational licensee.

4 (b) Training offered by a school described in (a) of this section must be in
5 accordance with a written agreement between the licensed owner and the school and
6 approved by the department.

7 **Sec. 05.18.360. Training locations.** Training provided for occupational
8 licensees may be conducted in a card room or at a school with which a licensed owner
9 has entered into an agreement under this chapter.

10 **Sec. 05.18.370. Convicted felons; rehabilitation; waiver.** (a) An individual
11 applying for an occupational license who is disqualified under AS 05.18.310 due to a
12 conviction for a felony may apply to the department for a waiver of that
13 disqualification, and the department may issue a license to the person if the
14 department determines that the individual has demonstrated by clear and convincing
15 evidence the individual's rehabilitation.

16 (b) In determining whether the individual applying for the occupational
17 license has demonstrated rehabilitation under (a) of this section, the department shall
18 consider

19 (1) the nature and duties of the position for which the individual has
20 applied;

21 (2) the nature and seriousness of the offense or conduct;

22 (3) the circumstances under which the offense or conduct occurred;

23 (4) the date of the offense or conduct;

24 (5) the age of the individual when the offense or conduct was
25 committed;

26 (6) whether the offense or conduct was an isolated or a repeated
27 incident;

28 (7) a social condition that may have contributed to the offense or
29 conduct;

30 (8) evidence of rehabilitation, including good conduct in prison or in
31 the community, counseling or psychiatric treatment received, acquisition of additional

1 academic or vocational education, successful participation in a correctional work
2 release program, or the recommendation of a person who supervises or has supervised
3 the individual;

4 (9) the complete criminal record of the individual;

5 (10) the prospective employer's written statement that

6 (A) the employer has been advised of all of the facts and
7 circumstances of the individual's criminal record; and

8 (B) after having considered the facts and circumstances, the
9 prospective employer will hire the individual if the department grants a waiver
10 of the requirements of this chapter.

11 (c) The department may not waive the requirements of this chapter for an
12 individual who has been convicted of committing any of the following:

13 (1) a felony in violation of federal law, as classified in 18 U.S.C. 3559;

14 (2) a felony of fraud, deceit, or misrepresentation under the laws of this
15 state or another jurisdiction; or

16 (3) a felony of conspiracy to commit a felony of fraud, deceit, or
17 misrepresentation under the laws of this state or another jurisdiction.

18 Article 4. Crimes.

19 Sec. 05.18.400. Crimes. (a) A person commits a class A misdemeanor if the
20 person knowingly

21 (1) makes a false statement on an application submitted under this
22 chapter;

23 (2) operates a card operation in which wagering is conducted or is to
24 be conducted in a manner other than the manner required under this chapter;

25 (3) permits a person under 21 years of age to make a wager;

26 (4) aids, induces, or causes a person under 21 years of age who is not
27 an employee of the card room to enter or attempt to enter the card room;

28 (5) makes a false statement on an application submitted to the
29 department under this chapter; or

30 (6) enters or attempts to enter a card room and is not an employee of
31 the card room and is under 21 years of age.

1 (b) A person commits a class C felony if the person knowingly

2 (1) offers, promises, or gives anything of value or benefit

3 (A) to a person who is connected with the owner of a card
4 room, including an officer or an employee of a licensed owner or holder of an
5 occupational license; and

6 (B) under an agreement to influence or with the intent to
7 influence

8 (i) the actions of the person to whom the offer, promise,
9 or gift was made in order to affect or attempt to affect the outcome of a
10 card game; or

11 (ii) an official action of the department;

12 (2) solicits, accepts, or receives a promise of anything of value or
13 benefit

14 (A) while the person is connected with a card room, including
15 an officer or employee of a licensed owner or a holder of an occupational
16 license; and

17 (B) under an agreement to influence or with the intent to
18 influence the actions of the person to affect or attempt to affect the outcome of
19 a card game or an official action of the department;

20 (3) uses, or possesses with the intent to use, a device to assist in
21 projecting the outcome of a card game;

22 (4) cheats at a card game;

23 (5) manufactures, sells, or distributes any cards, chips, or device that is
24 intended to be used to violate this chapter;

25 (6) alters or misrepresents the outcome of a card game on which
26 wagers have been made after the outcome is made sure but before the outcome is
27 revealed to the players;

28 (7) places a bet on the outcome of a card game after acquiring
29 knowledge that is not available to all players and that concerns the outcome of the card
30 game that is the subject of the bet;

31 (8) aids a person in acquiring the knowledge described in (7) of this

1 subsection for the purpose of placing a bet contingent on the outcome of a card game;

2 (9) claims, collects, takes, or attempts to claim, collect, or take money
3 or anything of value in or from a card game with the intent to defraud or without
4 having made a wager contingent on winning a card game;

5 (10) claims, collects, or takes an amount of money or thing of value of
6 greater value than the amount won in a card game;

7 (11) uses or possesses counterfeit chips or tokens in or for use in a card
8 game;

9 (12) possesses a key or device designed for opening, entering, or
10 affecting the operation of a card game, drop box, or an electronic or mechanical
11 device connected with the card game or removing coins, tokens, chips, or other
12 contents of a card game; this paragraph does not apply to a licensee or an employee of
13 a licensee acting in the course of the employee's employment;

14 (13) possesses materials intended to be used in a manner that violates
15 this chapter.

16 **Sec. 05.18.410. Possession of cheating devices; presumption.** The
17 possession of more than one of the devices described in AS 05.18.400(b) as cheating
18 devices creates a rebuttable presumption that the possessor intended to use the devices
19 for cheating.

20 **Article 5. General Provisions.**

21 **Sec. 05.18.500. State gaming fund.** There is created in the general fund the
22 state gaming fund. The state gaming fund consists of all revenue received from card
23 room activities under this chapter and all other money credited or transferred to the
24 fund from another fund or source.

25 **Sec. 05.18.900. Definitions.** In this chapter,

26 (1) "card game" means a non-banking card game listed in
27 AS 05.18.010(b);

28 (2) "card operation" means the conduct of card games in a licensed
29 card room;

30 (3) "card room" means a structure in which card games authorized
31 under this chapter are conducted by an owner licensed under this chapter;

1 (4) "cheat" means to alter the selection of criteria that determine the
2 result of a card game or the amount or frequency of payment in a card game;

3 (5) "department" means the Department of Revenue;

4 (6) "gross receipts" means the total amount of money exchanged for
5 the purchase of chips or tokens by card room patrons;

6 (7) "intentionally" has the meaning given in AS 11.81.900;

7 (8) "knowingly" has the meaning given in AS 11.81.900;

8 (9) "license" means a license issued by the department under this
9 chapter;

10 (10) "licensed owner" means a person that owns a card room who is
11 licensed under this chapter;

12 (11) "licensee" means a person holding a license issued under this
13 chapter;

14 (12) "owner's license" means a license issued under this chapter that
15 allows a person to own and operate a card room;

16 (13) "player" means an individual actively participating in a card
17 game;

18 (14) "rake" means a set fee or percentage of the total amount wagered
19 by all players in a game in the course of that game.

20 * Sec. 3. AS 11.66.280(2) is amended to read:

21 (2) "gambling" means that a person stakes or risks something of value
22 upon the outcome of a contest of chance or a future contingent event not under the
23 person's control or influence, upon an agreement or understanding that that person or
24 someone else will receive something of value in the event of a certain outcome,
25 "gambling" does not include

26 (A) bona fide business transactions valid under the law of
27 contracts for the purchase or sale at a future date of securities or commodities
28 and agreements to compensate for loss caused by the happening of chance,
29 including contracts of indemnity or guaranty and life, health, or accident
30 insurance;

31 (B) playing an amusement device that

1
2
3
4
5
6
7
8
9

(i) confers only an immediate right of replay not exchangeable for something of value other than the privilege of immediate replay; and

(ii) does not contain a method or device by which the privilege of immediate replay may be cancelled or revoked; or

(C) an activity authorized by the Department of Revenue under AS 05.15 or AS 05.18;

* Sec. 4. AS 44.64.030(a)(2) is amended to read:

(2) AS 05.15 and AS 05.18 (charitable gaming; card rooms);

April 11, 2005

J. PATRICK BEATTIE
10700 PROSPECT DR.
ANCHORAGE, AK 99507

Senator John Cowdery
State Capitol Building
Juneau, Ak. 99801

Dear Senator Cowdery

I would like to voice my support for Senate Bill No. 115. As an accountant (now retired) for nearly thirty years, I believe the State should explore all reasonable and responsible avenues to raise state revenues. The legalization of card rooms has been successfully accomplished in other states. Properly regulated, I believe it can provide a proper means of entertainment in a positive environment, while still raising state revenues in a time of decline.

Sincerely,

J. Patrick Beattie

E-Mail jpbeattie@griesfamily.com



PRESBYTERY OF ALASKA

5750 Glacier Highway, C-16 • Juneau, AK 99801

(907) 780-6100
FAX (907) 780-4017

presbyt1@alaska.net
INBOX: PRESBY ALASKA

April 18, 2005

The Honorable Con Bunde
Chair, Senate Labor and Commerce Committee
Alaska State Senator, District P
Room 506
State Capitol
Juneau, AK 99801-1182

Dear Senator Bunde:

It has come to our attention the Senate Labor and Commerce Committee will be conducting a public hearing on Senate Bill 165 "An Act relating to card rooms and card operations". Unfortunately, prior commitments prevent our having an individual to speak at this hearing; however we would like to go on record strongly opposing the passage of this bill.

Included with this letter is a full statement giving some of the reasons for this position and additional supporting information.

In particular, we would urge the committee to seek out independent research on the social ills that would accompany expanded legalized gambling within the state. We would also encourage the legislature to seek official opinions on the likelihood that this legislation would expand the amount of non-state regulated "Indian Gaming". Our belief is that contrary to some opinions, the enactment of this law would permit this expansion.

On behalf of the Presbytery, which is made up of 15 Presbyterian churches from Metlakatla and Ketchikan to the south and Yakutat to the north, I sincerely encourage you to consider these materials when debating this legislation.

Sincerely,

Elder Guy Warren
Stated Clerk, Presbytery of Alaska

enclosures

Statement by the Stated Clerk of The Presbytery of Alaska on Senate Bill 165.

The Presbytery of Alaska consists of the 15 member churches of the Presbyterian Church U.S.A. from Yakutat in the north to Metlakatla in the south.

We believe that this bill represents a significant step towards situations, which will not be in the best interest of the state government or the citizens it serves. It will increase the social problems we face, and it will result in decreased state control through the introduction of increased "Indian gaming".

While some hold that the approval of this legislation will eliminate illegal gambling, we believe that the experience seen in other localities would demonstrate this is not the case. We also believe that the solution to illegal gambling is not simply to legalize it. Certainly we would believe that the legislature would never consider such a solution to other illegal acts. We also believe that the costs the state will incur attempting to repair the social ills that gambling brings with it will exceed whatever benefits the approval of this bill might bring. These social ills include increased domestic violence, various psychological and social problems and an increased incidence of suicide.

While others might disagree, we firmly believe that the introduction of legal card rooms within the state, will, through the terms of the Federal Indian Gaming Act, permit the introduction of similar facilities in locations this bill does not intend, and without any of the controls the state would want to see. We have provided the committee with additional materials from the Federal Indian Gaming Commission detailing our reasons for this belief.

We believe it would be prudent and only right for the Legislature to seek detailed and independently researched estimates on the social costs expanding legalized gambling will bring, and independent legal opinions on the status of the Indian Gaming Laws before introducing more gambling to the state.

The people of this state have spoken in the matter of gambling and they spoke loudly. A proposal to expand gambling within the state was presented to the people in 1990. This measure was defeated by over 40,000 votes, almost a 2:1 margin. We would think it only appropriate that the legislature not override this clear mandate of the people.

Finally, we are not unaware of the increased popularity of card games in this country. Cable television has an impressive array of televised Poker games on display. The players of these games appear happy and certainly not troubled by the ills of gambling. There is a simple reason for this. Those seen in these programs have already won. As an example, the typical World Poker Tour program begins with six players. Each of these players will win thousands of dollars. What the program does not show is the hundreds of players who lost \$15,000 to \$25,000 each to finance the televised prizes. Do we ever hear the stories of the problems these losses cause? Naturally, we do not. Rest assured, these problems do exist there, and will exist at the card rooms, this bill would establish.

Our state's problems with illegal gambling are not nearly so desperate as to take the significant gamble this bill proposes. The attractions we already have for bringing tourists to our state are unmatched.

Thank you.

World Poker Tour Statistics

A recent World Poker Tour event had 376 players paying \$15,000 each for the chance to win \$1,770,218. Prizes are traditionally given to the top 20 to 30 players. This means that at least 346 of those players went home empty-handed, with \$15,000 less than they started with.

Federal Indian Gaming Act

In an article in the April 9, 2005 edition of the *Anchorage Daily News*, Anchorage Attorney Lloyd Miller is reported as holding that "it didn't appear as though the card room plan would trigger the potential for any tribal operations beyond what is allowed in the bill. I would strongly encourage the Legislature to seek an independent legal opinion on this matter. Our research into this matter leads us to a different conclusion, namely that the legalization of card rooms within the State of Alaska, would permit the tribal operation of their own card rooms, and that these rooms would be exempted from the limits provided in the original version of SB 195. The following is a quote from an overview of the Federal Indian Gaming Regulatory Act appearing on the Indian Gaming Commission website.

"The Indian Gaming Regulatory Act, enacted in 1988 as Public Law 100-497 and now codified at 25 U.S.C. §2701, establishes the jurisdictional framework that presently governs Indian gaming. The Act establishes three classes of games with a different regulatory scheme for each. Class I gaming is defined as traditional Indian gaming and social gaming for minimal prizes. Regulatory authority over class I gaming is vested exclusively in tribal governments.

Class II gaming is defined as the game of chance commonly known as bingo (whether or not electronic, computer, or other technological aids are used in connection therewith) and if played in the same location as the bingo, pull tabs, punch board, tip jars, instant bingo, and other games similar to bingo. Class II gaming also includes non-banked card games, that is, games that are played exclusively against other players rather than against the house or a player acting as a bank. The Act specifically excludes slot machines or electronic facsimiles of any game of chance from the definition of class II games. **Tribes retain their authority to conduct, license, and regulate class II gaming so long as the state in which the Tribe is located permits such gaming for any purpose and the Tribal government adopts a gaming ordinance approved by the Commission. Tribal governments are responsible for regulating class II gaming with Commission oversight.**"

URL: <http://www.nigc.gov/nigc/laws/iqra/overview.jsp>

Emphasis ours

Further elaboration on this opinion can be found in the opinions issued by the General Counsel of the Commission. Within the State of Arizona, the General Counsel deemed non-banked Poker games as a Class II game. For the State of New York, the General Counsel deemed a "Poker Club" as a Class II game. In both cases, the Counsel held that as Class II games, they were subject to tribal and federal regulation only. Full details on these opinions can be found on the Indian Gaming Commission's website at the addresses:

<http://www.nigc.gov/nigc/documents/opinions/pokeraz.jsp>

<http://www.nigc.gov/nigc/documents/opinions/pokerclub.jsp>

FISCAL NOTE

STATE OF ALASKA
2005 LEGISLATIVE SESSION

Fiscal Note Number: _____
 Bill Version: SB 165 (L&C)
 () Publish Date: _____

Revision Date/Time (Note if correction): _____ Dept. Affected: Revenue 04
 Title Card Rooms & Operations RDU Treasury and Tax
 Component Tax Division
 Sponsor Senator Cowdery
 Requester (S) L&C Component No. 2476

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: 00
 Check 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)
 (see attached)

Prepared by: Larry Meyers & Brett Fried Phone 465-2320
 Division Tax Division Date/Time 4/18/05 4:15 PM
 Approved by: Tom Boutin, Deputy Commissioner Date 4/18/2005
 Agency Revenue

FISCAL NOTE

STATE OF ALASKA
2005 LEGISLATIVE SESSION

BILL NO. SB 165 (L&C)

ANALYSIS CONTINUATION

Revenue Discussion

This bill would legalize non-banked card rooms in Alaska, with the caveat that "the total number of owner's licenses issued in a municipality may not exceed the total population of the municipality divided by 30,000". A non-banked card room is one in which players compete against each other rather than against the house and the house has no stake in the outcome of a game. Texas Hold-Em poker is an example of a game that might be played in a non-banked card room. It is not clear if "the most recent federal census information" refers to the Decennial Census or the most recent estimate by the U.S. Bureau of Census for purposes of determining the number of card rooms allowed. We used the April 1, 2000 U.S. Census to determine that a maximum of 13 card rooms would be possible under this bill: 8 in Anchorage, 2 in the Fairbanks North Star Borough, 1 in Juneau, 1 in the Kenai Peninsula Borough and 1 in the Matanuska-Susitna Borough. If we were instead to use the July 1, 2004 annual estimates of population from the Census Bureau, then 15 card rooms would be possible: 9 in Anchorage, 2 in the Fairbanks North Star Borough, 1 in Juneau, 1 in the Kenai Peninsula Borough and 2 in the Matanuska-Susitna Borough. We assume the definition of "municipality" in AS 29.71.800, which includes first-class and home-rule cities and boroughs.

There are three reasons why we did not include a revenue or cost estimate on the front page of this fiscal note. First, the decision to open and operate a card room is a business decision that will be made by potential licensees. Second, under this bill the department is given authority to set many rules and regulations that will affect this business decision. The department will set these rules and regulations after consulting the recommendations made by the advisory board appointed by the governor. Third, the fees imposed on card rooms in different states and localities vary widely and make comparisons to Alaska difficult. For example, the state of Montana charges a processing fee to cover the cost of determining whether to issue a license plus \$250 for the first table and \$500 for each additional table. Washington charges \$3,650 for up to 5 tables and \$1,060 per additional table up to a maximum of 15, plus any investigation costs exceeding the license fees. SB 165 imposes an owner's license fee of \$25,000 to apply for a five-year license plus an annual \$10,000 per table fee. Operators are also responsible for investigation costs that exceed the portion of the \$25,000 fee that is assessed for the investigation, and the department is authorized to set occupational licensing fees.

Based on several assumptions, we estimate that the maximum of 13 card rooms in Alaska would generate about \$2.5 million in fees for the state in the first year. During years 2-5, we estimate the maximum of 13 card rooms in Alaska would generate \$2.1 million in annual fees for the state. These estimates assume that there will be the maximum of 13 card rooms with an average of 15 tables each (15 is the maximum allowed in Washington and in California the average is 14.3). All card rooms are assumed to pay their owner's license fees in the first year and would not transfer ownership over the 5-year license period. These estimates also assume an occupational licensing system similar to Washington, where annual licenses are \$175 initially and \$84 for renewals. We assume that Washington's average of 6.7 gaming employees per table will hold in Alaska and that after the first year, all of the licenses will be renewals. We assume that, like in Washington, all gaming employees will be covered but non-gaming employees such as bartenders will not require licenses. Of course, a significant variable affecting revenues is the actual number of tables any individual card room would have. This is difficult to estimate, as in California non-banked card rooms range from a single table to 243 in the Commerce Casino in Los Angeles with the average being 1-3 tables per card room. One or more very large card rooms in Alaska could significantly boost revenues. California and Washington are useful comparisons because both states have data available specifically for non-banked card rooms.

This bill stipulates that card rooms must hold at least one card tournament per quarter with proceeds donated to a nonprofit group. There are many variables that would help determine tournament proceeds, including the number of card rooms, the number of tables, rules and regulations adopted by the department, and other factors. In Michigan the average Texas Hold-Em tournament generates \$1,099 in profit for charities, with a \$500 per person per day prize limit. Any prize limits in Alaska would be determined by the department and may influence the profitability of tournaments. In an article in the Boston Globe, card tournament supplier Mike Sheehy estimated that "A well-run tournament will attract up to 200 players, each of whom pays a \$100 entrance fee [. . .] A tournament of that size can offer pots of \$5,000 for the first-place player and a few thousand for the second and third and still generate \$10,000 for the charity after expenses."

Cost Discussion

The costs of implementing this bill are difficult to estimate because we do not know the number nor size of potential card rooms. Given the assumptions in our revenue discussion, we would anticipate \$609,000 in total costs with \$532,000 in personnel costs and related expenditures and \$77,000 in RSAs to Public Safety for fingerprint background checks. The personnel costs are for an Investigator IV, four Investigator III's and an Admin Clerk III. Based on the experience of other states and our own experience, this staff should be sufficient to investigate, license and regulate up to 13 card rooms with an average of 15 tables each. Also having two teams of investigators would ensure that teams could be available during all hours of card room operations (assumed to be 12:00 noon to 2:00 am). If the card rooms are larger on average than the assumed 15 tables we would require additional staff and resources for investigation and regulation. We did not include any additional costs that would be incurred by municipalities as a result of this Bill.