"You're behind the counter, people are shoving stuff at you from both sides, and he just slipped through," Harris said. "You try to look at everybody and make sure you ask them for the IDs, but it happens."

Eleven Juneau stores refused to sell alcohol to the agent, including Kmart, Kenny's Liquor, Liquor Cache, Percy's, Imperial Bar, Douglas Breeze In, Valley Breeze In, Fred Meyer, Fisherman's Bend, Carrs and Duck Creek Market.

State and local investigators launched the effort in 2000 with funding from a federal grant - about $100,000 doled out statewide each fiscal year. Juneau's share the past two years was $11,000 and $14,000, said Kalwara, noting police officers volunteer for overtime to help in the effort.

Juneau investigators are renewing the grant for the fiscal year that began July 1 and tentatively plan to start a new rash of undercover operations in August. Kalwara said the next round could include a follow-the-keg program, meaning undercover officers posted outside stores would follow people who buy kegs to see if minors consume the beer.

They also might do more storefront stakeouts in which the underage agent, usually an 18-year-old, would ask adults to buy alcohol for him. Officers would cite adults who agree to the illegal transaction.

In addition, officers might pose as store clerks to catch minors who try to buy alcohol and adults who buy it for them, said Kalwara, who added they would first get permission from store owners.

Kathy Dye can be reached at kdye@juneauempire.com.

Click here to return to the original story

YIA survey shows adults willing to buy alcohol for minors

Actual violations could result in $10,000 fine, 1 year in jail

January 14, 2005

Mothers Against Drunk Driving

Last weekend, teens working with Mothers Against Drunk Driving's Youth In Action and state Alcohol Beverage Control officers discovered that it is not difficult to find adult strangers who will buy alcohol for teens.

Ranging in age from 14 to 19, the teens stood downtown near liquor stores and asked passing strangers to buy alcohol for them while admitting to be underage. Whether the adult answered yes or no, the teens then presented him with a card that explained this was only a survey, and the legal consequences of actually buying for someone underage. An ABC officer stood nearby to ensure the teens' safety and to assure people of the legality of the survey.

One pair of teens, which included a 14-year-old with braces on his teeth, had to wait only eight minutes before a young man said he would buy for them. Another pair of teens had to wait only about a minute before a middle-aged woman agreed. Overall, the teens spent one hour in two different locations downtown and found that four out of the 24 parties they asked were willing to buy.

"We were surprised and disappointed at how easy it was to find someone willing to buy," YIA coordinator Jessica Paris said. "However, we also had some adults who responded very admirably. One woman, not realizing it was a survey, went into the nearest liquor store and asked them to call the police. And at Kenny's Liquor Market, the clerk came out to investigate what the teens were doing."

One adult the teens asked happened to be state Rep. Kevin Meyer, who sponsored legislation last year allowing liquor stores to sue adults for buying alcohol for minors as well as the teens who solicit the alcohol. Rep. Meyer refused to buy for them, warning them he could get in big trouble.

"This survey shows us that we have to work harder to convince people they shouldn't provide alcohol to teens," Paris said. "Adults need to know about the tragedies that accompany underage drinking, as well as the serious legal consequences for providing to a minor."

ABC also conducted compliance checks over the weekend in which teen agents, aged 18 to 19, attempted to buy alcohol directly from liquor stores. Although Juneau had 100 percent compliance in last summer's checks, in 27 checks held last weekend, clerks sold to underage teens twice. Clerks, bartenders and wait staff face the same penalties for providing to an underage person that regular adults do - fines of up to $10,000 and up to one year in jail, though a typical sentence is $1,000 and five days in jail.

OJJDP
U.S. Department of Justice
Office of Justice Programs
Office of Juvenile Justice and Delinquency Prevention

Guide to Conducting Alcohol Purchase Surveys

Prepared by

Pacific Institute
FOR RESEARCH AND EVALUATION

In support of the
OJJDP Enforcing the Underage Drinking Laws Program

ntroduction

People who care about youth are aware of the serious problems caused by underage drinking. They realize that:

- Alcohol is the drug most commonly used by youth—more than tobacco and far more than marijuana or any other illicit drug.
- Alcohol is one of the most common contributors to injury, death, and criminal behavior among youth.
- Underage alcohol use can have immediate and potentially tragic consequences, as well as long-range h mful consequences, such as increased risk for chronic alcohol addiction.

There is no doubt that underage alcohol use is an extremely serious problem. But there are many effective strategies for reducing the problem. Strategies that *limit access* to alcohol by youth are some of the most powerful and well-documented approaches to reducing underage drinking and related problems.

The purpose of this guide is to promote the use of an important tool for monitoring underage access to alcohol—the purchase survey. These surveys involve sending young adults who appear underage (or minors under appropriate adult and police supervision) into stores to purchase alcohol. Communities and local groups can carry out purchase surveys of retail alcohol sales outlets to find out how easily available alcohol is to young people and to identify who is selling alcohol to youth. Such surveys provide extremely valuable information that can be used in addressing the problems of underage alcohol purchase and underage drinking.

This guide gives some of the background and rationale for these surveys as well as practical, step-by-step instructions for carrying out alcohol purchase surveys. The guide also shows how the information from the survey can be used to strengthen community awareness, promote better policies, and improve merchant compliance with the law.

Safe, efficient, and valid alcohol purchase surveys can be carried out in almost any community. This guide will show how.

Alcohol: The drug of choice for youth

National surveys of young people consistently show that alcohol is the drug of choice among young people. By the 12th grade, more than 80 percent of adolescents have experimented with alcohol, more than 50 percent report drinking within the previous month, and more than 30 percent report consuming five or more drinks in a row at least once in the previous 2 weeks (Johnston, O'Malley, & Bachman, 1998).

A recent study indicates that alcohol is responsible for 69 percent of all drug-related hospital stays among 10- to 19-year-olds. In contrast, tobacco accounts for 22 percent and other drugs for 9 percent of these hospital stays. Overall, 87 percent of years of life lost between the ages of 10 and 19 are alcohol related (Xie, Rehm, Single, & Robson, 1996).

In 1996, more than 6,300 young people between 15 and 20 years old died in traffic crashes. Of these fatalities, 2,315 (37 percent) were alcohol related. More than 21 percent of drivers aged 15–20 years old who were killed in traffic crashes in 1996 had been drinking (National Highway Traffic Safety Administration [NHTSA], 1998).

How Do Kids Get Alcohol?

Underage drinkers can obtain alcohol in many different ways—they can steal it or get it from their friends or their parents. In fact, kids are frequently quite creative in their schemes to get access to alcohol. All too often, however, they simply walk into a store and buy it—no questions asked, no identification requested, no problems encountered. Cutting off this type of easy access is the most important step toward preventing underage drinking in most communities.

Surveys carried out in various areas around the country have found that youth were able to buy alcohol in between 50 percent and 97 percent of stores, bars, and restaurants where attempts were made.

Studies indicate that enforcement of underage sales laws is lax in many communities. Police cite a number of reasons for not enforcing underage sales laws; most importantly, they perceive a lack of public support for such activities. This is unfortunate because research shows that enforcement can significantly reduce alcohol sales to minors.

Why Conduct Alcohol Purchase Surveys?

Illegal sales to minors can be prevented. A variety of strategies have been shown to be very effective, but most communities need valid information in order to make the best use of these strategies and to monitor their impact. Alcohol purchase surveys can help provide this information. In addition, the data obtained from purchase surveys can be used to increase support from the public and from public officials for policy changes and for more generous allocation of resources. This process is depicted in figure 1 as circular and involves a variety of segments of the community.

How Do You Conduct Purchase Surveys?

In order to carry out a purchase survey, a representative sample of alcohol outlets is selected. At each outlet in the sample, a buyer who appears to be underage attempts to purchase alcohol without presenting age identification (ID). If the outlet sells alcohol to the buyer, it is considered noncompliant. If the outlet refuses to sell to the buyer, it is considered in compliance. Details of this procedure vary, but the basic process is similar in all alcohol purchase

surveys. A flowchart of the tasks involved in conducting an alcohol outlet purchase survey is presented in appendix 1.

Purchase surveys are extremely useful, and they can be conducted practically, efficiently, and flexibly. This guide explains how to plan and carry out surveys under a variety of circumstances. It also provides sample protocols and materials that can be adapted for use in communities across the country.

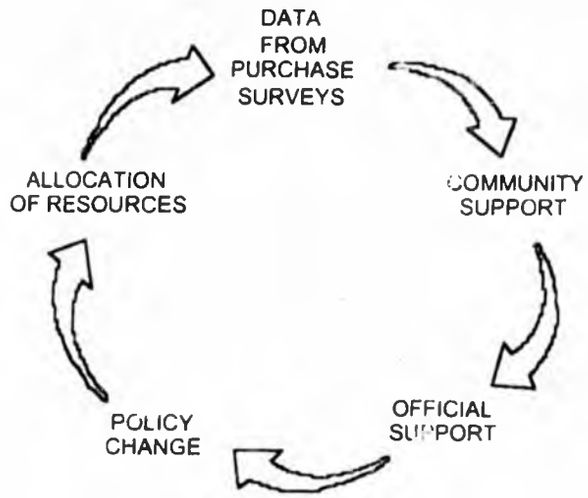


Figure 1. Survey Data and Community Process

Underage Purchase of Alcohol

Purchase surveys conducted in medium and small cities in Minnesota and Wisconsin have found youth able to purchase alcohol in about half of the attempts in both on- and off-premises outlets (Forster et al., 1994; Forster, Murray, Wolfson, & Wagenaar, 1995).

Another study surveyed communities in New York State and Washington, DC. Fully 97 percent of the Washington, DC, outlets sold to youth. Sales rates in New York varied from 44 percent to 80 percent (Preusser & Williams, 1992).

Five Reasons for Conducting Alcohol Purchase Surveys

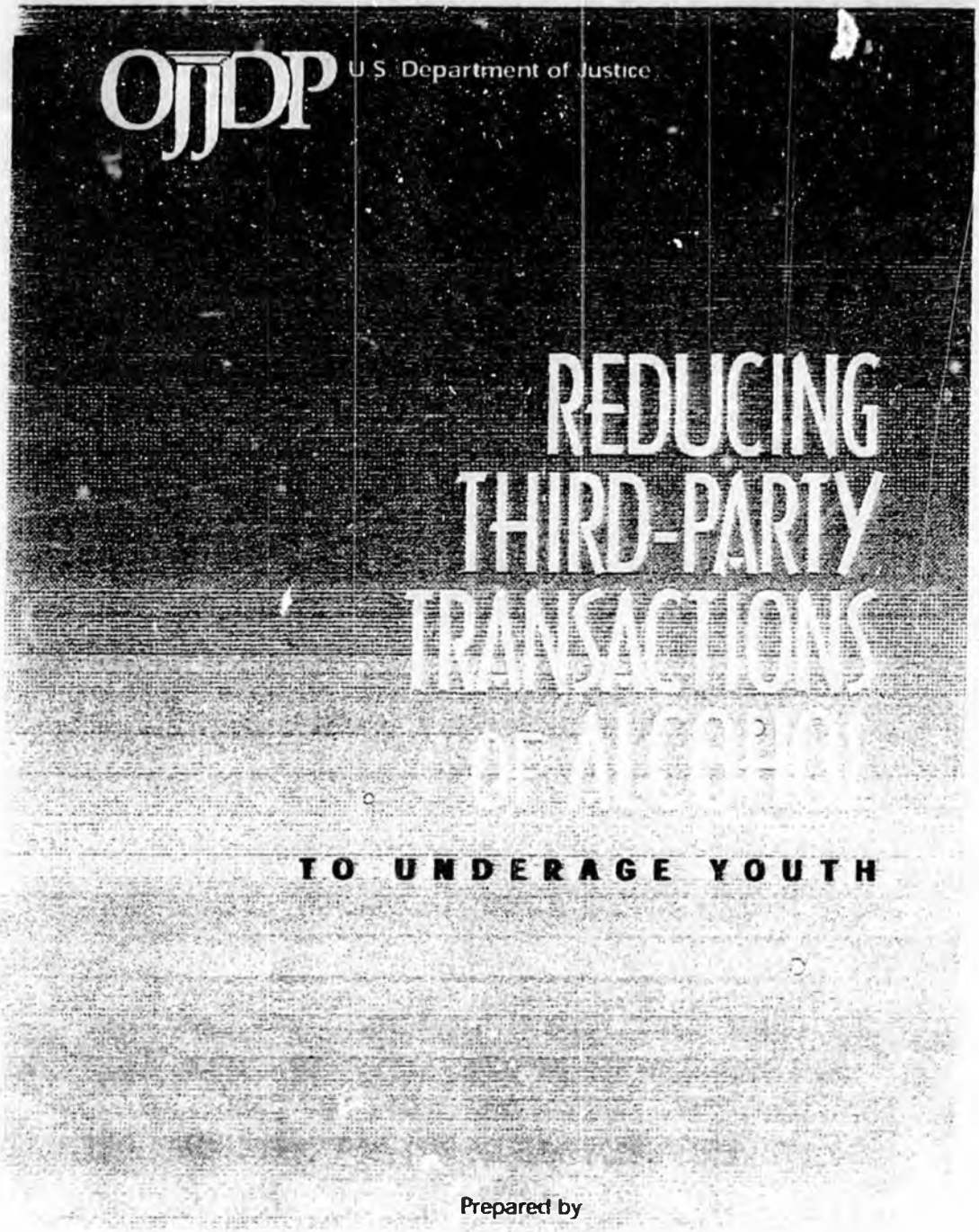
1. Purchase surveys indicate who is selling alcohol to minors and how often. This lets a community know how large the problem of underage sales is and among which outlets. This information can be very useful in allocating scarce enforcement and prevention resources.

2. The results of surveys can be used to help raise community awareness and build support for efforts to reduce sales to minors. For example, some communities have called press conferences in which the buyers pose with all the beer they have managed to purchase from local stores. Such events can bring attention to the problem of alcohol sales to minors and make it easier for policymakers, merchants, and concerned citizens to act.

3. Purchase surveys can be an intervention. Informing merchants that they are being monitored by the community and providing them with feedback can motivate those with good policies and sales practices to continue them and motivate those with poor policies and practices to change them.

4. Purchase surveys can be an important part of enforcement. Some communities choose to issue citations to outlets who sell to minors during the surveys. Other communities use the information from the surveys to help target later enforcement efforts. *In either case, local police or Alcohol Beverage Control (ABC) authorities must always be involved when enforcement efforts are planned as part of a purchase survey.*

5. Purchase surveys can be used to measure the impact of prevention strategies. A series of surveys carried out over time can indicate whether prevention efforts are having an effect on sales to minors. This information can help communities decide whether to continue or discontinue particular policies or programs and can indicate how to modify prevention strategies to make them more effective.



Prepared by

Pacific Institute
FOR RESEARCH AND EVALUATION

In support of the
OJJDP *Enforcing the Underage Drinking Laws* Program

community who is aware of alcohol sales to people under the age of 21 (third-party or otherwise) to pass this information along to enforcement agencies. These "tip lines" may be through the police department, liquor control agency, or a community agency/ organization working closely with enforcement efforts in the area.

Surveillance

Surveillance is another strategy for assessing where and when third-party transactions happen in your area. This observation within your jurisdiction can take a variety of forms and levels of intensity. If your department and community are still trying to determine where third-party sales occur, surveillance activity may involve asking officers on their routine patrol to be on the lookout for these transactions. While many third-party sales occur in open areas such as store parking lots or street corners, other exchanges happen in remote, hidden areas of the community, such as dead end streets, woods, and vacant lots. Therefore, it is important for patrol officers to include these areas in their rounds.

If you already have a sense of the "hot spots" in your area, you can conduct more specific surveillance in order to interrupt third-party transactions as they occur. Officers placed at or near locations popular for "shoulder taps" can watch for an exchange to start and address both parties as the transaction occurs. Some enforcement agencies use officers in "plain clothes" during surveillance in order to blend into the scene and not raise the suspicions of the adult purchaser or the youth.

"Shoulder tap" Enforcement Programs

"Shoulder tap" enforcement programs are similar to compliance check programs except that they target the underage drinkers and/or the non-commercial supplier of alcohol to youth instead of the vendor. Police departments or liquor control agencies carry out these programs, working closely with the community, youth, and local media to ensure their effectiveness. An example of a "shoulder tap" enforcement effort that focuses on stopping the underage purchasers is run by the Montgomery (MD) County Police

Conducting "shoulder tap" enforcement programs using underage decoys

Some enforcement agencies have established procedures for "shoulder tap" enforcement programs using underage decoys. While each department's guidelines must conform to local and state laws, a summary of the California ABC Department's procedures is offered as an example.

Implementation

The California ABC Department finds that its Decoy Shoulder Tap Program is most effective in areas where compliance checks have already been conducted and where most licensed premises were found in compliance. Additionally, the department uses this program when it has specific information or complaints that underage youth have changed their method of gaining alcohol from attempting to purchase directly from retailers to requesting that adults purchase and furnish them with alcohol. The department obtains this information from a variety of sources, including parents, youth officers, patrol officers, and members of community groups.

Preparation

The department contacts the local District Attorney's Office to ensure that they are willing to prosecute any misdemeanor violations found during the "shoulder tap" enforcement program. It is also recommended that the Municipal Court Judge most likely to preside over criminal charges be contacted and given an overview of the program and its purpose. To educate the public and gain support of these efforts, the department sends a formal press release to all local news media to announce the "shoulder tap" enforcement program. The department uses this media contact to emphasize that the goal of the program is not necessarily to make arrests, but to inform the public about the problems related to furnishing alcohol to underage youth and the legal consequences for doing so.

The selection of the underage decoys is clearly a critical part of the department's preparation. Requirements for the underage operatives include

- the decoy should be under the age of 20 at the time of the operation, preferably under 19 years old
- the decoy should have the appearance of a person his or her age

Department. Montgomery County police officers dress in "plain clothes" and stand in parking lots of retail establishments. The officers then wait to see if youth ask them to purchase alcohol. Often, the officers will wear clothes that allow them to blend in with a

- the decoy should be willing to wear a radio transmitter and to have his or her conversations recorded
- the decoy must be willing to testify in any criminal and administrative proceedings resulting from the operation.

As an additional preparatory step with the underage operatives, the Minneapolis Police Department photographs the decoys immediately before conducting the operations; this procedure offers proof that no attempts were made to make youth look older than their actual ages.

The California ABC Department instructs the underage volunteers to always tell the truth about their age and the fact that they cannot purchase alcohol for themselves.

Investigation and operation

The underage decoys are equipped with a radio transmitter and placed under the *direct* supervision of a law enforcement officer. If the approached adult does furnish alcohol to the decoy, the youth walks to a pre-designated location. To provide added security to the youth, the adult is allowed to move away from the decoy before being detained by the enforcement officers. The detained adult is then Mirandized and asked to give a verbal statement. Enforcement officers ask the adult why he or she provided alcohol to the young person and how old he or she thinks the decoy is. The suspect is then booked into the jail whenever justified; the California ABC Department, working with local law enforcement, uses the state's "misdemeanor non-release" provisions whenever possible.

This abbreviated account of the California ABC Department's procedures may offer your department a blueprint if you plan to operate a "shoulder tap" enforcement program. **However, it is important that you check your state and local statutes to ensure that the use of underage operatives is permitted and that other laws governing the distribution of alcohol to those under the age of 21 will support this strategy.**

(California ABC Department, n. d.)

neighborhood's street alcoholics, who are frequently "shoulder tapped" by underage drinkers.

Other "shoulder tap" enforcement programs use underage "decoys" to approach adults outside an alcohol outlet and request that the

adult purchase alcohol on the decoy's behalf. *Not all states permit the use of underage operatives in the enforcement of alcohol statutes; check with prosecutors in your area if you are considering this type of "shoulder tap" enforcement program.* The California Alcohol Beverage Control Department, Montgomery County (MD) Police Department, and the Minneapolis (MN) Police Department are examples of enforcement entities that use this strategy to address third-party transactions. These departments have established procedures for "shoulder tap" enforcement programs (see box on pages 12–13), including guidelines for the decoy's actions that are similar to those used in compliance checks (e.g., no deception, false identification, or attempts to look older). The departments also take precautions to safeguard the underage decoys by training them prior to the operations, equipping them with radio transmitters during the attempts, and placing them under the direct supervision of a law enforcement officer. Attempts to complete these enforcement activities are broken off immediately if there is any sign of danger (e.g., the adult asking the decoy to get into a car, the transaction moves out the direct view of the back-up teams). In conducting these enforcement activities, the California ABC Department discovered an added benefit to these operations. During one year of the "shoulder tap" enforcement program, 37 percent of the adults cited for purchasing alcohol for youth were either on parole, probation, or had outstanding arrest warrants. Therefore, their efforts to reduce underage drinking also resulted in other enforcement benefits in the state.

Strategies To Reduce Familiar Third-party Transactions

While strangers providing alcohol to youth contribute to underage access, parents, older siblings, other relatives, and friends are also a significant source of alcohol for underage drinkers. Because most of

HB

124

HOUSE COMMITTEE REPOI

(7)

Date Referred to Committee: February 2, 2005 **FURTHER REFERRALS: Finance**

Date of Committee Action: February 23, 2005

The JUDICIARY Committee considered: **HB 124**

HOUSE BILL NO. 124 **COLLECTION OF DNA/USE OF FORCE**

"An Act relating to the collection of, and the use of reasonable force to collect, a deoxyribonucleic acid sample from persons convicted of or adjudicated delinquent for certain crimes."

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

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

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

***NEW* FISCAL NOTES**
*Assigned by Chief Clerk's Office

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

***PREVIOUS* FISCAL NOTES**

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

Signing with recommendations	Printed Last Name	DP	DNP	NR	AM
	Gruenberg	–			
	ANDERSON	X			
	Coghill			–	
	Gara			✓	
Chair:	McGUIRE	X			
Chair:					

Conceptual Amendment #1 by Rep. Gara
FAILS

to HB 124

Limit § 2 to cases involving crimes against a person.

Conceptual Amendment #2 by Rep. Gara
FAILS
to HB 124

Sect. 2
P. 2, line 14

After "oral"
Insert "swab"

After "sample"
Insert ", unless another type of sample is necessary,"

How do you define reasonable force?

Why are probation officers and parole officers included on the list?

Shouldn't there be exceptions for adjudicated youth? Is the same amount of 'reasonable force' used on youth as adults?

What procedures are in place to ensure that unnecessary violence will not be used to collect the DNA? Video cameras, multiple people in the room etc.?

Are individuals kept in the DNA database for the rest of their life?

What systems are in place to 'clean up' the database if individuals die?

How effective has the collection of DNA been in Alaska? How many cases have been aided by this tool?

Why is DNA collected for all felonies? Even when they crimes are non violent? How much does it cost to collect the DNA of every single person who commits a felony, and now with this bill, a municipal offense of similar nature to a felony? How backlogged is the current system?

Does the bill clearly prevent individual from filing civil lawsuits of a frivolous nature? Is more language needed? How many lawsuits (that are later found to be frivolous) are filed by inmates in Alaska annually? Does the Department of Law find lawsuits to be a problem? How can the language be worded so substantial cases can receive proper attention, while frivolous lawsuits can be easily identified?

What is the procedure on collecting DNA from individuals convicted of a felony who are currently on parole and/or released yet were convicted before DNA collection was required by law? Can we collect from them?

ALASKA STATE HOUSE OF REPRESENTATIVES

Labor & Commerce Committee, Chair
Administrative Regulation Review, Chair
Judiciary Committee, Vice-Chair
Health, Education and Social Services

State Capitol Suite 408
Juneau, AK 99508
Phone (907) 465-4939
Fax (907) 465-2418

Representative Tom Anderson

Email: Representative_Tom_Anderson@legis.state.ak.us

MEMORANDUM

Date: February 14, 2005

To: Representative Lesil McGuire, Chair
House Judiciary Committee

From: Representative Tom Anderson

Re: HB 124

I respectfully request scheduling of HB 124 for consideration by the House Judiciary Committee.

Enclosed are:

1. The most recent version of the bill
2. Current Sponsor Statement
3. Sectional Analysis
4. Letters of support and other appropriate backup documentation

Thank you for your consideration of this request. Please contact Jon Bittner at 465-5031 in my office if you have any questions or concerns.

Alaska State Legislature

Interim:
716 W. 4th Ave.
Anchorage, AK 99501-2133

Phone: (907) 269-0265
Fax: (907) 269-0264

Session:
Alaska State Capitol, Rm 408
Juneau, AK 99801-1182

Phone: (907) 465-4939
Fax: (907) 465-2418
Toll Free: (800) 465-4939
Rep.Tom_Anderson@legis.state.ak.us

Representative Tom Anderson
District 19 - Anchorage

Sponsor Statement
HB 124

HB 124 allows a correction, probation or parole officer to use reasonable force in the collection of DNA samples required by law and absolves them from civil or criminal liability for the use of that force. Officers shouldn't run the risk of being punished for carrying out their duties.

Currently, there is no way for a corrections, parole or patrol officer to collect the DNA samples required by law if the individual the DNA is to be collected from is uncooperative. If an officer were to try and use reasonable force to collect the sample, under current law they could be held liable for civil or criminal penalties.

For some convicted felons there is no incentive to provide this type of evidence because anything added to their sentence would make little difference. People serving life sentences are one example. There is no punishment under the current statutes to efficiently encourage cooperation.

I urge your support of this bill.

Alaska State Legislature
House of Representatives

Official Business

State Capitol
Juneau, AK 99801-1182

Sectional Analysis for HB 124
BY: Representative Tom Anderson

Section 1. Amends AS 44.41.035(b)

This section of the bill adds municipal violations similar to felonies to the list of violations for which the state can collect DNA evidence.

Section 2. Adds a new subsection to AS 44.41.035

Gives a juvenile or adult correctional, probation or patrol officer the authority to use reasonable force in the procurement of DNA samples when such samples are required by law. Also provides immunity from civil and criminal liability stemming from the use of that force.

Some inmates say 'no' to DNA sample

04/15/2002 - Updated 12:36 AM ET

By Richard Willing, USA TODAY

Inmates nationwide are refusing to give authorities DNA samples that could link them to other crimes, threatening nascent efforts to build a nationwide database of convicts' genetic profiles that officials say could help clear thousands of unsolved cases.

Authorities say inmates in as many as a dozen states — including Maine, Massachusetts, New York and Illinois — have refused to give blood or saliva samples containing DNA since states began requiring them from inmates during the 1990s.

The refusals are centered in California, where since last summer more than 900 inmates in at least five prisons have declined to give samples, prison officials say. The officials say the prisoners have cited privacy concerns and a general distaste for authority as reasons for refusing. Refusals "have broken out sporadically in the past, but the California situation seems unique," says Dawn Herkenham, a consultant to the FBI on DNA database laws. "If it spreads, it could be very harmful" to efforts to perfect a national DNA database.

During the past 13 years, all 50 states and the District of Columbia have passed laws setting up crime-fighting databases. They work by taking DNA, a cellular acid that contains an individual's unique genetic code, and matching it by computer to the codes found in blood, semen and other body fluids left at crime scenes.

All states are authorized to collect DNA from convicted sex offenders. Most also take it from murderers, kidnappers, robbers and child molesters.

Since 1998, state DNA databases have been linked by a national computer system maintained by the FBI. The national system allows crimes committed in one state to be solved through comparisons with DNA samples taken from convicts in other states. As of February, the national system contained DNA profiles of 802,000 convicts and had been used to identify suspects or develop evidence in 3,911 investigations, according to the FBI.

Since the mid-1990s, 11 states have passed laws permitting authorities to use "reasonable force" to take samples from reluctant inmates. In California, prison officials have used administrative sanctions, including a loss of parole credits, to try to coax inmates into cooperating. Critics say the sanctions are not persuasive to convicts who are serving long sentences with little hope of parole.

At the state's Vacaville prison, for instance, convicted murderer Fred Clark refused to give DNA samples, telling prison officers, "What are you going to do? Put me in jail?"

Some prosecutors are critical of officials for not forcing prisoners to comply.

"It's the Leona Helmsley approach: They want their guests to be completely comfortable," says Rockne Harmon, an Alameda County, Calif., deputy prosecutor, referring to the owner of luxury hotels in New York City. "With guys who have nothing to do all day but talk about how the system is screwing them, it just doesn't work."

Terry Thornton, spokeswoman for California's corrections department, says the department has used court orders permitting the use of force to obtain samples from about 30 inmates. A bill that would permit authorities to force inmates to comply without seeking a court order is scheduled to be taken up April 30 by a state Senate panel.

San Diego defense lawyer Christopher Plourd, who recently used a state DNA database to exonerate a man who had been convicted of murder in Arizona, says defense lawyers should join prosecutors in insisting that convicts give DNA.

Arresting Developments In DNA Typing

Phillip B.C. Jones, Ph.D., J.D.

I. Introduction: Identity testing in criminal investigation

During the mid-to late nineteenth century, European intellectuals and government leaders worried about the rising crime rate that accompanied industrial progress and colonial expansion (Sankar, 2001). Analysts proposed a biological degeneration as the cause of rising crime in general, and in particular, the creation of a criminal class. To reverse this degeneration in England, Francis Galton proposed compulsory marriages between people of good stock. This presented the challenge of finding an outward sign of inward character, so that it would be possible to identify those who should be breeding. In the 1880s, Galton thought that he had found this marker in fingerprints. However, his studies showed that variations in papillary ridges would not provide an external marker of internal character, and hypothesized that this was due to a millennia of indiscriminate mixing of character types. Nevertheless, he decided that fingerprints could aid social improvement by providing a unique identifier, which would be especially useful to identify habitual criminals who took advantage of the anonymity offered by the new, large cities (Cole, 2001).

One hundred years later, Alec Jeffreys, a geneticist working in England on blood anomalies, developed DNA typing. As the analytic techniques evolved, "DNA fingerprinting" became more popular. In 1995, Britain began to take DNA samples from anyone arrested for a felony or misdemeanor (Cole, 2001). The United Kingdom's National DNA Database currently holds DNA profiles of more than 1.5 million suspects (Forensic Science Service, 2002). The United States is beginning to get as aggressive as the UK in collection of DNA samples for criminal identification.

II. DNA Testing in the United States

All states have laws authorizing the collection of biological samples for DNA analysis from convicted sex offenders (Gugliotta, 1999; Willing, 2002a). Although requirements vary from state to state, most also take samples from murderers, kidnappers, robbers, and child molesters. Virginia, which has the oldest DNA database in the U.S., has been at the forefront: taking samples from convicted felons, as well as from juvenile offenders whose crimes would have been felonies had they been of age (Siegel, 2002).
More states are moving to collect DNA samples from thousands of non-violent criminals, such as burglars and check forgers (Willing, 2002b). The number of states collecting DNA from all convicted felons rose from seven in 2000 to 19 in 2002, a trend that may be driven by the observation that state DNA databases now routinely solve murders, rapes, and other violent crimes by linking them to criminals convicted of non-violent offenses (Willing, 2002b). In Virginia, for

example, nearly two-thirds of the 60 crimes linked to people convicted of drug possession were rapes or murders, and ten out of 22 forgers who were linked to other crimes were linked to murders or sexual assaults. The success of DNA databases has also spurred the authorization of the use of "reasonable force" with inmates reluctant to donate samples. To date, 11 states have authorized the use of such force (Willing, 2002a).
In addition to an expansion of the types of crimes that trigger biological sample collection, states are changing the point at which samples can be taken. In February, a Texas law took effect that requires testing of those indicted in sex crimes (Rein, 2002). That same month, Virginia took a more radical step. The legislature passed a bill that allows authorities to take biological samples for DNA analysis of everyone arrested in a felony case.

Virginia's SB535, which has an effective date of January 1, 2003, requires a saliva or tissue sample from every person arrested for a violent felony. A "violent felony" includes: first and second degree murder, voluntary manslaughter, mob-related felonies, a kidnapping or abduction felony, any malicious felonious assault or malicious bodily wounding, robbery, carjacking, a criminal sexual assault punishable as a felony, and certain forms of arson. After the law is in effect, a magistrate will determine that probable cause exists for the arrest, and then a biological sample will be taken prior to the person's release from custody. If the charge is dismissed or the person is acquitted at trial, the DNA sample will be destroyed by the Division of Forensic Science.

Dr. Paul Ferrara, the Director of the Virginia Division of Forensic Science, sees that the primary benefit of the new law is that, by taking a sample at the time of arrest instead of waiting for a conviction, DNA information is available earlier for comparing against DNA samples from unsolved crimes (Sigel, 2002). However, the notion of taking DNA samples from arrestees has stirred protests that it is unconstitutional and should not be done.

III. DNA Collection at the Time of Arrest

1. Is it permissible under the law?

Those who find DNA collection unconstitutional point to the Fifth or Fourth Amendments. Some commentators have argued that a suspect's Fifth Amendment right not to act as a witness against themselves provides a basis for refusing to give a genetic sample (Morin, 2002). However, courts have limited the right against self-incrimination to a suspect's oral testimony, and physical or behavioral characteristics are not testimonial. In Boling v. Romer, for example, a federal appellate court found that requiring DNA samples from inmates was not compulsory self-incrimination because DNA samples are not testimonial in nature. The Fourth Amendment provides a more substantial challenge to DNA testing.

Under the Fourth Amendment, suspects have a due process right against unreasonable searches and seizures. As a result, a warrant must be issued to conduct a search and probable cause must exist before the warrant is issued. One proponent of DNA testing detects support for the procedure in the U.S. Supreme Court decision, *Schmerber v. California*, in which the Court found that an involuntary blood draw to assess blood alcohol concentration was allowable without a warrant, because the evidence would have been metabolized by the time a warrant was issued (Scott, 2001). Of course, a suspect's DNA should be more stable than blood alcohol; if not, than the suspect has bigger problems than the law.

The Fourth Amendment guarantees that all people shall be "secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." A governmental action is a search or

seizure within the scope of the Fourth Amendment if the person invoking its protection can claim a legitimate expectation of privacy in the place search or the item seized. Courts have found that obtaining a biological sample, such as saliva, for DNA analysis can be considered a search under the Fourth Amendment (see, for example, *In re Shaddie Clark Shabazz*). However, the Fourth Amendment does not proscribe all searches and seizures, but only those deemed "unreasonable." The general rule is that the question of whether a particular action is unreasonable is judged by balancing its intrusion on the individual's Fourth Amendment interests against its promotion of legitimate governmental interests (see, for example, *The People v. James Edward King*). When the governmental action is the taking of a sample for DNA analysis, courts have analogized to fingerprinting.

In *Rise v. State of Oregon*, the court noted that the gathering of fingerprint evidence from "free persons" constitutes a sufficiently significant interference with an individual's expectation of privacy that authorities are required to demonstrate that they have probable cause, or at least an articulable suspicion, to believe that the person committed a criminal offense and that the fingerprinting will establish or negate the person's connection with the offense. In contrast:

> [E]veryday "booking" procedures routinely require even the merely accused to provide fingerprint identification, regardless of whether investigation of the crime involves fingerprint evidence. . . . Thus, in the fingerprinting context, there exists a constitutionally significant distinction between the gathering of fingerprints from free persons to determine their guilt of an unsolved criminal offense and the gathering of fingerprints for identification purposes from persons within the lawful custody of the state. (p. 1560; citations omitted)

The same argument can be made for the routine collection of a biological sample, such as saliva or a buccal swab, for DNA analysis.

2. Should it be allowed?

In 1998, New York City Police Commissioner Howard Safir went public with his plan for city police to take a DNA sample along with fingerprints of everyone arrested ("DNA," 1998; "Proposal," 1998). Norman Siegel, the Director of the New York Civil Liberties Union, objected that the major fallacy in Safir's plan was that he equated a fingerprint with DNA when taking a DNA sample, unlike recording a fingerprint, reveals a person's complete genetic makeup and is too intrusive ("DNA," 1998). The Director of the Connecticut Civil Liberties Union has gone further. According to Joseph Grabarz, when you give up DNA information, you are not just giving up information about yourself, but about your family, past, present, and future (Halloran, 1999). This concern, in turn, fuels the fear that genetic information will be used for genetic discrimination, or that law enforcement agencies might use the information for commercial purposes (Halloran, 1999; Kertscher, 2001). These fears are based upon a misunderstanding about the information derived from DNA analyses by crime laboratories.

There is a difference between the genetic information required for identification and the genetic information that informs about disease or phenotype. Fisher and Jones (2001) explain the differences this way. A genetic marker used for identification should be highly variable, and the more variable the markers, the fewer are needed for positive identification. In contrast, a gene examined in a genetic test is unlikely to be highly variable, because the test is geared to detect an abnormality, which most will not have. Furthermore, a nucleotide sequence is usually of interest in genetic testing because it codes for a protein. In identification, however, a noncoding nucleotide sequence is of most interest. This is because the mathematical modeling used in identification

works best with noncoding sequences that are considered unaffected by natural selection.

3. Can it be done?

Even if the sampling of all arrestees' DNA may be performed, the question remains about whether it can be done. Arizona now tests only those convicted of certain crimes, including homicide, sexual offenses, and home burglary. However, the state legislature may soon pass a bill that would phase in testing of all convicted felons. Yet this increase in scope, which does not include arrestees, presents the unresolved issue of how to pay the estimated $2 million annual cost of expanded testing (Davenport, 2002). Since 1999, Louisiana has a law mandating arrestee testing, but staffing and funding problems have delayed the program (Rein, 2002).

On the federal level, experts have concluded that the collection of DNA samples at the time of arrest is cost prohibitive. According to the National Commission on the Future of DNA Evidence, the majority of crime laboratories face difficult prioritization decisions due to limited financial and personnel resources (National Institute of Justice, 2000). Laboratories find their first priority in cases necessary for upcoming trials, as they struggle to keep pace with prosecutors' demands for DNA evidence in court. The next priority lies in DNA analysis for investigative purposes, where a suspect exists but DNA evidence is necessary to effectuate an arrest. It is only after prioritizing court cases and suspect cases that laboratories can allocate resources to analysis of non-suspect crime scene samples. This is the class for which the FBI's Combined DNA Index System (CODIS) was designed and the class of cases where offenders are at liberty to re-offend.

Due to current prioritization and funding constraints, most police departments maintain policies that prevent the submission of non-suspect cases to laboratories, creating a backlog of DNA cases maintained in police evidence lockers. To place the extent of the backlog into perspective, Congress is considering the DNA Database Completion Act of 2001 (H.R. 2680), which authorizes grants to eligible States for DNA analyses of samples taken from individuals convicted of a qualifying State offense, and of samples from crime scenes, for inclusion in the Combined DNA Index System. The cost: $100,000,000 for each of fiscal years 2002 through 2006.

Given the current volume of DNA cases facing the nation's forensic labs and the current inability of the labs to keep pace with that volume, the Commission recommended that the Department of Justice should not pursue arrestee sampling unless the convicted offender database backlog is substantially eliminated, significant sources are allocated for the analysis of non-suspect cases, and sufficient funds are made available for the collection and analysis of arrestee samples. Until these conditions are met, the Commission concluded, the pursuit of arrestee sampling would seriously exacerbate the backlog and casework and prove more harmful than beneficial by diverting resources from non-suspect cases

IV. Conclusion

The social development of DNA analysis is paralleling that of fingerprints: initial hesitancy followed by acceptance of police departments and courts, followed by a rush to implement the technology with an ever-expanding scope. According to Cole (2001), the history of fingerprinting should teach the difference between a biological marker and a code that informs about a person's abilities, weaknesses, or destinies. An emphasis on this distinction may aid the social acceptance of collecting DNA samples from arrestees, as long as there are sufficient assurances that DNA typing will only be used for identification. The cost of implementing such a biological sample collection is another matter. However, the U.S. public may be more inclined to foot the bill since

the September 11 terrorist attacks.

References

Boling v. Romer, 101 F.3d 1336 (10th Cir. 1996).

Cole, S.A. (2001). *Suspect Identities* (Harvard University Press).

Davenport, P. (April 12, 2002). "Lawmakers moving to expand state's DNA testing of criminals," *The Associated Press State & Local Wire.*

"DNA from suspects: Plan raises fears," *Seattle Times* (Final Edition) A6 (December 15, 1998).

Fischer, E.A. and Jones, N.L. (2001). *DNA Identification and Evidence: Applications and Issues* (Novinka Books).

Forensic Science Service (2002). "History of the Forensic Science Service," Available: http://www.forensic.gov.uk/forensic/entry.htm.

Gugliotta, G. (July 7, 1999). "A rush to DNA sampling: Vital police tool? Affront to Liberty?" *The Washington Post*, A01.

Halloran, L. (October 24, 1999). "DNA testing fuels debate over privacy some say justice wins, others fear losing rights," *Hartford Courant*, A1.

In re Shaddie Clark Shabazz, 2002 U.S. Dist. LEXIS 8078 (April 23, 2002).

Kertscher, T. (May 4, 2001). "DNA tests raise privacy worries," *Milwaukee Journal Sentinel*, 0[illegible]3.

Morin, S.K. (Spring 2002). "The physician as gatekeeper to the use of genetic information in the criminal justice system," *The Journal of Law, Medicine, & Ethics* 30:88-94.

National Institute of Justice. (January 16, 2000). "Recommendation of the National Commission on the Future of DNA Evidence to the Attorney General Regarding Arrestee DNA Sample Collection," Available: http://www.ojp.usdoj.gov/nij/dna/arrestrc.html.

"Proposal: DNA sample at arrest/Safir to speak today on controversial plan," *Newsday* (Combined Editions), A31 (December 14, 1998).

Rein, L. (February 11, 2002). "Va. Senate Panel Backs DNA tests at time of arrest," *The Washington Post*, A1.

Rise v. State of Oregon, 59 F.3d 1556 (Ninth Cir. 1995).

Sankar, P. (2001). "DNA-Typing: Galton's Eugenic Dream Realized?," in *Documenting Individual Identity*, Caplan, J. and Torpey, J. (Eds.), pages 273-290 (Princeton University Press).

Schmerber v. California, 384 U.S. 757 (1966).

Scott, G. (November 20, 2001). "Should Physicians help law enforcement authorities conduct

'DNA dragnets'?, *The New York Times* (Late Edition), F7.

Siegel, R. (February 18, 2002). All Things Considered National Public Radio.

The People v. James Edward King, 82 Cal. App. 4th 1363 (Ct Ap Cal 2000).

Willing, R. (2002a). "Some inmates say 'no' to DNA sample; Nation's database could be threatened," *USA Today* (Final Edition), A.03 (April 15, 2002).

Willing, R. (2002b). "Collection of prisoner DNA widens; Major crimes linked to non-violent offenders," *USA Today* (Final Edition), A.03 (May 2, 2002).

Additional articles in Biological Evidence.....

Humans and Apes....What Is the [DNA] Difference?
Breath Tests for Blood Alcohol Determination: Partition Ratio
H.G.N. (Horizontal Gaze Nystagmus)

See related article linked in the Identification Evidence section.....

Phenotype v. Genotype: Why Identical Twins Have Different Fingerprints

Return to Master Index

Jon S. Bittner

To: Blake Harrison
Subject: RE: DNA Force

Here are some examples that authorizes reasonable force to obtain the sample.

These are from 2003

Illinois SB 280 b Allows agencies designated by the Department of State Police to contract with third parties to provide for the collection or analysis of offender DNA. Provides that duly authorized law enforcement and corrections personnel may employ reasonable force when an individual refuses to provide required DNA samples.

Louisiana SB 346 b Expands DNA data base to include all persons arrested for or convicted of a felony, including □felony-grade delinquent acts.□ Allows reasonable use of force as needed to collect such samples. Provides for implementation of arrestee samples only to the extent that funding is available. Allows prosecution of sex crimes within three years of statutory statute of limitations when the identity of the offender is established thereafter with a DNA profile, with retroactive application. Establishes that detention, arrest or conviction of a person based on a data base match is not invalidated if it is determined that the sample was obtained or placed in the data base by mistake.

2002 laws

California SB 1242

Allows law enforcement, custodial or corrections personnel to employ reasonable force to collect required specimens, samples or print impressions from persons convicted of specified offenses.

Utah HB 5015E

Requires collection of DNA from all state felonies. Clarifies statutory authority for agencies to collect specimens; requires agencies establish guidelines and procedures; and authorizes use of reasonable force if necessary to collect the specimen; and allows the $75 fee be waived if the collecting agency determines the offender is unable to pay.

Here is the summary I have for your state law.

Alaska H 49 b Expands DNA registration to include all convicted felons and juveniles adjudicated for felonies against a person. Makes it a felony for a person required to submit a DNA sample to refuse to do so. Includes identification of human remains and testing related to exoneration of the innocent to allowed law uses of the DNA registration system.

Blake Harrison
Sr. Policy Specialist Criminal Justice
National Conference of State Legislatures 7700 East First Place, Denver CO 80230 Phone 303.364.7700 Direct line 303.856.1424 Fax 303.364.7800
Email: blake.harrison@ncsl.org
Web site www.ncsl.org

FISCAL NOTE

STATE OF ALASKA
2005 LEGISLATIVE SESSION

Fiscal Note Number:
Bill Version: HB 124
() Publish Date:

Revision Date/Time (Note if correction):
Dept. Affected: Corrections
Title "An act relating to the collection of, and the use of reasonable force to collect, a deoxyribonucleic acid sample"
RDU Institutional Facilities
Component Institution Director's Office
Sponsor Senator Bunde
Requester Judiciary, Finance
Component No. 524

Expenditures/Revenues (Thousands of Dollars)

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

OPERATING EXPENDITURES	FY 2003	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
Personal Services	0.0	0.0	0.0	0.0	0.0	0.0
Travel	0.0	0.0	0.0	0.0	0.0	0.0
Contractual	0.0	0.0	0.0	0.0	0.0	0.0
Supplies	0.0	0.0	0.0	0.0	0.0	0.0
Equipment	0.0	0.0	0.0	0.0	0.0	0.0
Land & Structures	0.0	0.0	0.0	0.0	0.0	0.0
Grants & Claims	0.0	0.0	0.0	0.0	0.0	0.0
Miscellaneous	0.0	0.0	0.0	0.0	0.0	0.0
TOTAL OPERATING	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**
CAPITAL EXPENDITURES	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**
CHANGE IN REVENUES ( )	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**

FUND SOURCE (Thousands of Dollars)

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

Estimate of any current year (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	0	0	0	0	0	0
Part-time	0	0	0	0	0	0
Temporary	0	0	0	0	0	0

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

Passage of this legislation will not have a measurable fiscal impact on the Department of Corrections.

Prepared by: Sharleen Griffin, Acting Director
Phone 465-4641
Division Administrative Services
Date/Time 2/18/05 9:44 AM
Approved by: Portia Parker, Deputy Commissioner
Date 2/18/2005
Agency Department of Corrections

(Revised 9/23/2004 OMB)

FISCAL NOTE

STATE OF ALASKA
2005 LEGISLATIVE SESSION

Fiscal Note Number:
Bill Version: HB124-LAW-CDCO-2-21
() Publish Date:

Revision Date/Time (Note if correction):
Dept. Affected: LAW
Title "An Act relating to the collection of, and the use of reasonable force to collect, a deoxyribonucleic acid..."
RDU CRIMINAL
Component CDCO
Sponsor Representative Anderson
Requester House Judiciary
Component No.

Expenditures/Revenues (Thousands of Dollars)

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

OPERATING EXPENDITURES	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
Personal Services						
Travel						
Contractual						
Supplies						
Equipment						
Land & Structures						
Grants & Claims						
Miscellaneous						
TOTAL OPERATING	0.0	0.0	0.0	0.0	0.0	0.0
CAPITAL EXPENDITURES						
CHANGE IN REVENUES ( )						

FUND SOURCE (Thousands of Dollars)

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

Estimate of any current year (FY2005) cost: 0.0
Mark this box (X) if funding for this bill is included in the Governor's FY 2006 budget proposal:

POSITIONS

Full-time						
Part-time						
Temporary						

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

This bill amends AS 44.41.035(b) (DNA identification system) by both narrowing the statute to apply to convictions that occur in Alaska, and widening to apply to violations of law or ordinances with elements similar to AS 11 (Criminal Law) or AS 28.35 (Motor Vehicle Offenses and Accidents). A new subsection to AS 44.41.035 is added that allows certain officials to use reasonable force in collection of DNA.

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

Prepared by: Kathryn Daughhetee, Director
Phone 465-3673
Division Administrative Services Division
Date/Time 2/22/05 10:34 AM
Approved by: K. Daughhetee for Scott Nordstrand, Acting Attorney General
Date 2/22/2005
Agency Department of Law

(Revised 9/23/2004 OMB)

FISCAL NOTE

STATE OF ALASKA
2005 LEGISLATIVE SESSION

Fiscal Note Number:
Bill Version: HB 124
() Publish Date:

Revision Date/Time (Note if correction):
Dept. Affected: Administration
Title: An Act relating to collection of DNA by force...
RDU: Legal and Advocacy Services
Component: Public Defender Agency
Sponsor: Rep. Anderson
Requester: House Judiciary
Component No.: 1631

Expenditures/Revenues (Thousands of Dollars)

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

OPERATING EXPENDITURES	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
Personal Services	0.0	0.0	0.0	0.0	0.0	0.0
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	0.0	0.0	0.0	0.0	0.0	0.0
1005 GF/Program Receipts						
1037 GF/Mental Health						
Other (Specify Type--Do not abbreviate)						
TOTAL	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**

Estimate of any current year (FY2005) cost: 0.0
Mark this box (X) if funding for this bill is included in the Governor's FY 2006 budget proposal:

POSITIONS

Full-time						
Part-time						
Temporary						

ANALYSIS: *(Attach a separate page if necessary)*
This bill allows public safety employees, including juvenile and adult probation and parole officers to use reasonable force to collect authorized DNA samples, and grants them immunity from any civil or criminal liability. This bill, if enacted, is not expected to have a significant fiscal impact on the operations of the Agency.

Prepared by: Linda K. Wilson, Deputy Director
Phone (907)334-4416
Division: Public Defender Agency
Date/Time 2/22/05 9:52 AM
Approved by: Michael Tibbles, Deputy Commissioner
Date 2/22/2005
Agency: Department of Administration

FISCAL NOTE

STATE OF ALASKA
2005 LEGISLATIVE SESSION

Fiscal Note Number:
Bill Version: HB124-DPS-SS-2-22-05
() Publish Date:

Revision Date/Time (Note if correction):
Dept. Affected: Public Safety
Title: Use of Force for DNA Collection
RDU: Statewide Support
Component: Criminal Records & ID
Sponsor: Representative Anderson
Requester: House Judiciary
Component No.: 1190

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
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:

Section 1 amends AS 44.41.035(b) by expanding the types of convictions that require deoxyribonucleic acid (DNA) registration. Under this bill, upon conviction in this state of crimes similar to crimes against persons, or felonies under AS 11 or AS 28.35, DNA must be collected. "Similar crimes" will include municipal misdemeanors, and preliminary estimates, based on the Uniform Offense Citation Table, are that this would include convictions under approximately 35 municipal misdemeanors from six municipalities – Anchorage, Juneau, Fairbanks, Ketchikan, Sitka, and Petersburg. In FY 2004 there were 680 persons with convictions under those municipal offenses. This number excludes duplicates (persons who were convicted of more than one qualifying municipal offense) and persons for whom DNA has already been collected for prior convictions (for whom subsequent collections will not be necessary).

continued on page 2

Prepared by: Director David Schade
Phone 269-0202
Division: Statewide Services
Date/Time 2/22/05 3:54 PM
Approved by: Commissioner William Tandeske
Date 2/22/2005
Agency: Department of Public Safety

ANALYSIS CONTINUATION

Collecting DNA for municipal misdemeanors will mean that when some defendants are subsequently convicted of other qualifying offenses, their DNA will already be on file, so this does not mean the numbers are absolute additions to the DNA database overall. Basically, this bill will shift the collection of DNA to earlier in a defendant's criminal career. "Similar crimes" will aiso include federal or military convictions, for which no preliminary numbers are available. Adding "similar crimes" will have an impact on Statewide Services Records & Identification and Information Services due to the increase in clerical and technical tasks, such as confirming fingerprints and modifying tables in the Alaska Public Safety Information Network (APSIN). This increase in the workload can be absorbed at present, although there is a cumulative impact on the APSIN staff workload. Similarly, the crime lab can absorb the increase in DNA submissions, although there is a cumulative impact on the crime lab workload as well.

Section 2 provides that reasonable force may be used in the collection of oral DNA samples. This section will have no impact on the workload of Statewide Services.

HB

131

HOUSE COMMITTEE REPORT

(7)
Date Referred to Committee: February 9, 2005 **FURTHER REFERRALS: Finance**

Date of Committee Action: March 18, 2005

The JUDICIARY Committee considered: **HB 131**

HOUSE BILL NO. 131 **ACCESS DEVICE & I.D. DOCUMENT CRIMES**

"An Act increasing the criminal classification of theft of an access device and of obtaining an access device or identification documents by fraudulent means; increasing the criminal classification for certain cases of fraudulent use of an access device; and providing for an effective date."

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

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

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

NEW FISCAL NOTES *Assigned by Chief Clerk's Office

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

PREVIOUS FISCAL NOTES

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

Signing with recommendations	Printed Last Name	DP	DNP	NR	AM
	Gatchalian	–			
	Kott			✓	
	Anderson	X			
	Johnson			X	
	Coghill	✓			
			✓		
Chair:	McGuire	✓			
Chair:					

Reasons to Support HB 131 and the $50 limit
On Fraudulent Use of an Access Device (Credit Card, etc) as a C Felony

- Fraudulent use of an access device is a crime that is very similar in terms of the actor's bad conduct to forgery of a check. Forgery of a check in ***any*** amount is a class C felony under AS 11.46.505.

- There are at least two sets of victims in each case of fraudulent use of an access device: the consumer victim, i.e., the person whose information was used, and the merchant or bank who loses services or merchandise. Costs to merchants or banks from these losses are eventually placed back on the consumer through higher prices or fees.

- The emotional and fiscal impact on consumer victims from fraudulent use of an access device can be more severe than forgery or theft cases and can go on for several years without the victim even being aware of the problem. (Average time spent by victims to repair their identity and credit is 600 hours and cost substantial amount of money). ***Identity Theft: The Aftermath 2003,*** Identity Theft Resource Center, Summer, 2003.

- The legislature has recognized other situations where certain types of property or certain situations warrant class C felony liability regardless of the value of property received.

  - theft of a firearm or explosive, AS 11.46.130(a)(2)
  - theft of any type of property in any value from the person of another, AS 11.46.130(a)(3)
  - theft of a fire extinguisher or supporting equipment, or other "vessel safety or survival equipment" AS 11.46.130(a)(4)

An access device falls within a class of property that deserves special attention and protection regardless of the actual value of the property received. Class C felony liability is justified.

THE
FOLLOWING
DOCUMENT(S)
ARE
POOR
ORIGINAL
COPIES

Chapter 397 of the Acts of 1998

AN ACT RELATIVE TO FALSE IMPERSONATION AND IDENTITY FRAUD.

Be it enacted by the Senate and House of Representatives in General Court assembled, and by the authority of the same, as follows:

SECTION 1. Chapter 266 of the General Laws is hereby amended by inserting after section 37D the following section:-

Section 37E. (a) For purposes of this section, the following words shall have the following meanings:

"Entity", [illegible]

"Personal identifying information", any name or number that may be used, alone or in conjunction with any other information, to assume the identity of an individual, including any name, address, telephone number, driver's license number, social security number, place of employment, employee identification number, mother's maiden name, demand deposit account number, savings account number, credit card number or computer password identification.

"Pose", to falsely represent oneself, directly or indirectly, as another person or persons.

"Victim", any person who has suffered financial loss or any entity that provided money, credit, goods, services or anything of value and has suffered financial loss as a direct result of the commission or attempted commission of a violation of this section.

(b) Whoever, with intent to defraud, poses as another person without the express authorization of that person and uses such person's personal identifying information to obtain or to attempt to obtain money, credit, goods, services, anything of value, any identification card or other evidence of such person's identity, or to harass another shall be guilty of identity fraud and shall be punished by a fine of not more than $5,000 or imprisonment in a house of correction for not more than two and one-half years, or by both such fine and imprisonment.

(c) Whoever, with intent to defraud, obtains personal identifying information about another person without the express authorization of such person, with the intent to pose as such person or who obtains personal identifying information about a person without the express authorization of such person in order to assist another to pose as such person in order to obtain money, credit, goods, services, anything of value, any identification card or other evidence of such person's identity, or to harass another shall be guilty of the crime of identity fraud and shall be punished by a fine of not more than $5,000 or imprisonment in a house of correction for not more than two and one-half years, or by both such fine and imprisonment.

(d) A person found guilty of violating any provisions of this section shall, in addition to any other punishment, be ordered to make restitution for financial loss sustained by a victim as a result of such violation. Financial loss may include any costs incurred by such victim in correcting the credit history of

such victim for any costs incurred in connection with any civil or administrative proceeding to satisfy any debt or other obligation of such victim including lost wages and attorney's fees.

SECTION 2. Chapter 268 of the General Laws is hereby amended by inserting after section 34 the following section:-

Section 34A. Whoever knowingly and willfully furnishes a false name or Social Security number to a law enforcement officer or law enforcement official following an arrest shall be punished by a fine of not more than $1,000 or by imprisonment in a house of correction for not more than one year or by both such fine and imprisonment. Such sentence shall run from and after any sentence imposed as a result of the underlying offense. The court may order that restitution be paid to persons whose identity has been assumed and who have suffered monetary losses as a result of a violation of this section.

Approved December 3, 1998

Return to
List of Laws passed in 1998 Session
General Court home page, or
Commonwealth of Massachusetts home page

Oklahoma Public Legal Research System

Sponsored by the

Oklahoma Attorney General's Office

using *CNIDR Isearch-cgi 1.20.06 (File: 21-1533.1.html)*

[Previous] [Next]

§21-1533.1.

§21-1533.1.

It is unlawful for any person to willfully and with fraudulent intent obtain the name, address, social security number, date of birth, or any other personal identifying information of another person, living or dead, with intent to use, sell, or allow any other person to use or sell such personal identifying information to obtain or attempt to obtain credit, goods, property, or service in the name of the other person without the consent of that person. It is unlawful for any person to use with fraudulent intent the personal identity of another person, living or dead, or any information relating to the personal identity of another person, living or dead, to obtain or attempt to obtain credit or anything of value. Any person convicted of violating any provision of this section shall be guilty of identity theft. Identity theft is a felony offense.

[Previous] [Next]

STATE OF ALASKA

DEPARTMENT OF LAW

OFFICE OF THE ATTORNEY GENERAL

Frank H. Murkowski, Governor

Commercial and Fair Business Section
P.O. BOX 110300
123 4TH ST., DIMOND COURT HOUSE
JUNEAU, ALASKA 99811-0300
PHONE: (907)465-3600
FAX: (907)465-2539

March 1, 2005

Sectional Analysis of HB 131 (ID Theft)

(Prepared by the Department of Law, March 1, 2005)

HB 131 would increase the criminal classification of theft of an access device, of fraudulent use of an access device, and for fraudulently obtaining an access device or identification document.

Section 1 classifies theft of an access device as theft in the second degree, a class C felony.

Section 2 is a conforming amendment that deletes a statutory reference to the provision repealed in sec. 5 of the bill.

Section 3 raises fraudulent use of an access device to a class C felony from a class A misdemeanor when the value of the property or services obtained is between $50 and $25,000; it raises fraudulent use of an access device to a class A misdemeanor when the value of property or services obtained is less than $50.

Section 4 raises fraudulently obtaining an access device or identification document to a class C felony from a class A misdemeanor.

Section 5 repeals the statutory provision classifying theft of an access device as theft in the third degree.

Section 6 would make the bill applicable to offenses occurring on or after the effective date.

Section 7 sets out an effective date of July 1, 2005.

adn.com
Anchorage Daily News

Print Page Close Window

Identity thieves may have hit Alaska

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

By RICHARD RICHTMYER
Anchorage Daily News

(Published: February 24, 2005)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Identity crisis?

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

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

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

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

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

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

Print Page Close Window

Post-it® Fax Note 7671
To Chair McGuire
Co./Dept. House Judiciary
Phone #
Fax # 907-465-6547

To: House Judiciary Members

From: Steve Cleary, AkPIRG – 278-3661

RE: Other means to protect Alaskan consumers from Identity Theft in addition to HB 131 - ACCESS DEVICE & I.D. DOCUMENT CRIMES

Thank you for your effort to raise Identity Theft from a misdemeanor to a felony. This is indeed a serious crime and it is unfortunately on the rise.

In the wake of the Choicepoint security breach, nearly 150,000 consumers across the nation and at least 251 in Alaska have had sensitive, personal information stolen that could lead to their identity being stolen. This lapse in security shows how vulnerable consumers are and highlights the need for the Alaska Legislature to take action to protect consumers here in Alaska. Below are two simple measures that will greatly protect Alaskan consumers from Identity Theft when these types of security breaches occur in the future.

Security Freezes

To help prevent identity theft, individuals should be able to "freeze" or block access to their credit reports and credit scores derived from them until they affirmatively unlock the files by contacting the credit bureaus and providing a security code.

This proposed act would provide consumers the right to prevent credit bureaus from releasing their credit reports and credit scores for the purpose of issuing new extensions of credit. This would limit the activity identity thieves could engage in on the consumer's accounts.

Security Breaches

Any entity that collects and maintains personal customer information as part of business operations has a legal obligation to establish security procedures to maintain the confidentiality and integrity of that data. A necessary component of any security procedure is a plan of notice and response in the event that personal data is at risk of being compromised. For consumers, notice of even a potential breach is necessary to prevent or quickly remedy the problem if a financial institution's information security systems fail.

California is currently the only state that mandates notification of affected consumers. Even though Choicepoint has agreed to notify consumers in all states after receiving pressure from Attorneys General across the nation, Alaskan consumers should know that next time they will be notified in a timely matter so that they can take appropriate action to protect their identity.

This model legislation below is excerpted from:

THE CLEAN CREDIT AND IDENTITY THEFT PROTECTION ACT: MODEL STATE LAWS
A PROJECT OF THE STATE PUBLIC INTEREST RESEARCH GROUPS AND CONSUMERS UNION.
THE FULL REPORT CAN BE FOUND AT:
HTTP://WWW.PIRG.ORG/CONSUMER/CREDIT/MODEL.HTM

SECTION 2: SECURITY FREEZE[1]

COMMENTARY

Identity thieves take advantage of the fact that any business with a "permissible purpose" can access a consumer's credit report for credit or insurance purposes. To help prevent identity theft, individuals should be able to "freeze" or block access to their credit reports and credit scores derived from them until they affirmatively unlock the files by contacting the credit bureaus and providing a security code.

This proposed act would provide consumers the right to prevent credit bureaus from releasing their credit reports and credit scores for the purpose of issuing new extensions of credit. With the security freeze activated, if an identity thief attempts to take out credit in a consumer's name, the creditor would not have access to the consumer's credit report and consequently would not approve the application. Security freezes, however, would not apply to any person or entity with which consumers have existing accounts, nor to a limited number of other parties who may access the files for purposes not related to issuing credit.

The model law would allow consumers to give credit file access to selected users through the use of a security code or a temporary exemption to the freeze. In addition, credit bureaus would be required to notify consumers following new business requests (not from current creditors) for their credit reports or scores in order to assist consumers in detecting illegitimate access as well as attempted or actual fraud.

A security freeze should not be preempted by the federal Fair Credit Reporting Act. The federal law does require credit bureaus, upon the request of a consumer, (1) to put a fraud alert into the consumer's file to warn potential users of the report that new credit should not be extended without first verifying the identity of the credit applicant, and (2) to block the reporting of any information in a consumer's file that the consumer identifies as information resulting from an identity theft.[2] States are preempted from imposing requirements regarding the conduct required by these specific provisions. These two provisions, however, do not establish any conduct with respect to freezing access to the entire report; as such states should be free to enact this model law.

The security freeze under this model law applies to all consumers, and not only to people who already have been victimized by identity theft. Given that reported identity theft complaints are on the rise, and the cost from this conduct is between two and three billion dollars a year for

---

[1] The right to a security freeze should not be confused with trade line blocking or fraud alert rights. The federal Fair Credit Reporting Act provides that a consumer, subject to certain procedures, can act to "block" specific fraud-related items (or trade lines) from appearing in his or her credit report. But trade line blocking does not prevent the issuance of a report, it only limits certain fraud-related information from also being issued. Similarly, a fraud alert attached to a report does not prevent the report from being issued. A fraud alert merely conditions the issuance of credit until certain identity verification procedures are complied with (or the issuer faces liability), but does not prevent the credit bureau from selling or sharing the report. Conversely, a security freeze grants any consumer --whether or not a suspected or actual identity theft victim-- the right to prevent the credit bureau from issuing his or her report for the purpose of issuing new credit. It freezes access to the report except for circumstances such as review of existing accounts and other limited purposes.

[2] The security freeze will provide better protection for consumers than the federal fraud alert and trade line blocking procedure. Under recently released rules, the Federal Trade Commission has created a confusing, burdensome process for consumers to trigger this protection. Each credit bureau may establish different information and documentation to verify the fraud, and they may impose waiting periods totaling up to thirty-five days before they have to begin the blocking. *See* Final Rule, Related Identity Theft Definitions, 16 C.F.R. pts. 603, 613, 614, available at: http://www.ftc.gov/os/2004/10/041029idtheftdefsfrn.pdf.

credit card fraud alone, states have a strong case to make that this statute is a necessary preventative measure to protect consumers. Some states, however, may choose to limit the security freeze provision to victims of identity theft. To that end, states may want to modify the proposed language, using the Texas and Vermont statutes as models.

The authors are disappointed that the credit bureaus have attempted to make the implementation of security freeze laws difficult, and the cost of freezing or unfreezing reports prohibitively high. Modern technology should allow for much more sophisticated and easy to use security freeze products than have been offered so far by the bureaus.

SIMILAR LEGISLATION:

Currently, California, Louisiana, Texas, and Vermont have passed versions of security freeze legislation.[3] Texas and Vermont's statutes are limited to victims of identity theft.

MODEL STATE LAW

Subsection A. Definitions. For the purposes of this section, the following terms shall have the following meanings:

(1) "Security freeze" means a notice, at the request of the consumer and subject to certain exceptions, that prohibits the consumer reporting agency from releasing all or any part of the consumer's credit report or any information derived from it without the xpress authorization of the consumer. If a security freeze is in place, such a report or information may not be released to a third party without prior express authorization from the consumer. This subdivision does not prevent a consumer reporting agency from advising a third party that a security freeze is in effect with respect to the consumer's credit report.

(2) "Reviewing the account" or "account review" includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements.

Subsection B. Security Freeze: Timing, Covered Entities, Cost.

1) A consumer may elect to place a "security freeze" on his or her credit report by:
   a) making a request by certified mail,
   b) making a request by telephone by providing certain personal identification, or
   c) making a request directly to the consumer reporting agency through a secure electronic mail connection if such connection is made available by the agency.

2) A consumer reporting agency shall place a security freeze on a consumer's credit report no later than five business days after receiving a written or telephone request from the consumer or three business days after receiving a secure electronic mail request.

---

[3] Cal. Civil Code Ann. § 1785.11.2, La. Stat. Ann § 9.3571(H) to (Y); Tex. Bus. & Commerce Code Ann. § 20.031 to 20.039; and Vt. Stat. Ann. tit. 9 § 2480a to 2480j.

3) The consumer reporting agency shall send a written confirmation of the security freeze to the consumer within five business days of placing the freeze and at the same time shall provide the consumer with a unique personal identification number or password to be used by the consumer when providing authorization for the release of his or her credit for a specific party or period of time.

4) If the consumer wishes to allow his or her credit report to be accessed for a specific party or period of time while a freeze is in place, he or she shall contact the consumer reporting agency via telephone, certified mail, or secure electronic mail, request that the freeze be temporarily lifted, and provide the following:
   a) proper identification,
   b) the unique personal identification number or password provided by the consumer reporting agency pursuant to paragraph (3) of subsection B, and
   c) the proper information regarding the third party who is to receive the credit report or the time period for which the report shall be available to users of the credit report.

5) A consumer reporting agency that receives a request from a consumer to temporarily lift a freeze on a credit report pursuant to paragraph (4) of subsection (B) shall comply with the request no later than three business days after receiving the request.

6) A consumer reporting agency may develop procedures involving the use of telephone, fax, or, upon the consent of the consumer in the manner required by the Electronic Signatures in Global and National Commerce Act [E-Sign] for legally required notices, by the Internet, e-mail, or other electronic media to receive and process a request from a consumer to temporarily lift a freeze on a credit report pursuant to paragraph (4) of subsection (B) in an expedited manner.

7) A consumer reporting agency shall remove or temporarily lift a freeze placed on a consumer's credit report only in the following cases:
   a) upon consumer request, pursuant to paragraph (4) or paragraph (10) of subsection (B);
   b) if the consumer's credit report was frozen due to a material misrepresentation of fact by the consumer. If a consumer reporting agency intends to remove a freeze upon a consumer's credit report pursuant to this paragraph, the consumer reporting agency shall notify the consumer in writing five business days prior to removing the freeze on the consumer's credit report.

8) If a third party requests access to a consumer credit report on which a security freeze is in effect, and this request is in connection with an application for credit or any other use, and the consumer does not allow his or her credit report to be accessed for that specific party or period of time, the third party may treat the application as incomplete.

9) If a third party requests access to a consumer credit report on which a security freeze is in effect for the purpose of receiving, extending, or otherwise utilizing the credit therein, and not for the sole purpose of account review, the consumer credit

report agency must notify the consumer that an attempt has been made to access the credit report.

10) A security freeze shall remain in place until the consumer requests that the security freeze be removed. A consumer reporting agency shall remove a security freeze within three business days of receiving a request for removal from the consumer, who provides both of the following:
   a) proper identification, and
   b) the unique personal identification number or password provided by the consumer reporting agency pursuant to paragraph (3) of subsection (B).

11) A consumer reporting agency shall require proper identification of the person making a request to place or remove a security freeze.

12) A consumer reporting agency may not suggest or otherwise state or imply to a third party that the consumer's security freeze reflects a negative credit score, history, report or rating.

13) The provisions of this section do not apply to the use of a consumer credit report by any of the following:
   a) a person, or the person's subsidiary, affiliate, agent, or assignee with which the consumer has or, prior to assignment, had an account, contract, or debtor-creditor relationship for the purposes of reviewing the account or collecting the financial obligation owing for the account, contract, or debt.
   b) a subsidiary, affiliate, agent, assignee, or prospective assignee of a person to whom access has been granted under paragraph (4) of subsection (B) for purposes of facilitating the extension of credit or other permissible use.
   c) any person acting pursuant to a court order, warrant, or subpoena.
   d) a State or local agency which administers a program for establishing and enforcing child support obligations.
   e) the [state health department] or its agents or assigns acting to investigate fraud.
   f) the [state tax authority] or its agents or assigns acting to investigate or collect delinquent taxes or unpaid court orders or to fulfill any of its other statutory responsibilities.
   g) a person for the purposes of prescreening as defined by the federal Fair Credit Reporting Act.
   h) any person or entity administering a credit file monitoring subscription service to which the consumer has subscribed.
   i) any person or entity for the purpose of providing a consumer with a copy of his or her credit report upon the consumer's request.

14) A consumer may not be charged for any security freeze services, including but not limited to the placement or lifting of a security freeze. A consumer, however, can be charged no more than $5 only in the following discrete circumstance:
   a) If the consumer fails to retain the original personal identification number provided by the agency, the consumer may not be charged for a one-time reissue of the same or a new personal identification number; however, the consumer may be charged no more than $5 for subsequent instances of loss of the

personal identification number.

Subsection C. Notice of Rights. At any time that a consumer is required to receive a summary of rights required under Section 609 of the federal Fair Credit Reporting Act or under [state law], the following notice shall be included:

[State] Consumers Have the Right to Obtain a Security Freeze

You may obtain a security freeze on your credit report at no charge to protect your privacy and ensure that credit is not granted in your name without your knowledge. You have a right to place a "security freeze" on your credit report pursuant to [State law].

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval.

The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, within five business days you will be provided a personal identification number or password to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report for a specific party, parties or period of time after the freeze is in place. To provide that authorization, you must contact the consumer reporting agency and provide all of the following:

1. The unique personal identification number or password provided by the consumer reporting agency.
2. Proper identification to verify your identity.
3. The proper information regarding the third party or parties who are to receive the credit report or the period of time for which the report shall be available to users of the credit report.

A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days after receiving the request.

A security freeze does not apply to circumstances where you have an existing account relationship and a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities.

If you are actively seeking credit, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze – either completely if you are shopping around, or specifically for a certain creditor – a few days before actually applying for new credit.

You have a right to bring a civil action against someone who violates your rights under the credit reporting laws. The action can be brought against a consumer reporting agency or a user of your credit report."

Subsection D. Violations; Penalties.

If a consumer reporting agency erroneously, whether by accident or design, violates the security freeze by releasing credit information that has been placed under a security freeze, the affected consumer is entitled to:

1) Notification within five business days of the release of the information, including specificity as to the information released and the third party recipient of the information.

2) File a complaint with the Federal Trade Commission and the state Attorney General and [other

state consumer protection agency].

3) In a civil action against the consumer reporting agency recover:
   a) injunctive relief to prevent or restrain further violation of the security freeze, and/or
   b) a civil penalty in an amount not to exceed $10,000 for each violation plus any damages available under other civil laws, and
   c) reasonable expenses, court costs, investigative costs, and attorney's fees.

4) Each violation of the security freeze shall be counted as a separate incident for purposes of imposing penalties under this section.

SECTION 7: PREVENTION OF AND PROTECTION FROM SECURITY BREACHES

COMMENTARY

Recent studies have confirmed that the crime of identity theft claims millions of victims each year, costing both victims and the companies that lawfully collect consumer information billions of dollars in losses. Any entity that collects and maintains personal customer information as part of business operations has a legal obligation to establish security procedures to maintain the confidentiality and integrity of that data. A necessary component of any security procedure is a plan of notice and response in the event that personal data is at risk of being compromised. For consumers, notice of even a potential breach is necessary to prevent or quickly remedy the problem if a financial institution's information security systems fail. For addition information, see comments of the Privacy Rights Clearinghouse, Consumers Union and other groups to federal agencies on security breaches.[4]

SIMILAR LEGISLATION

Currently, California's Security Breach Information Act is the only state law addressing this issue.[5]

MODEL STATE LAW

Subsection A. Definitions. For the purposes of this section, the following terms shall have the following meanings:

1) "Data Collector" may include but is not limited to government agencies, public and private universities, privately and publicly held corporations, financial institutions, retail operators, and any other entity which, for any purpose, whether by automated collection or otherwise, handles, collects, disseminates, or otherwise deals with nonpublic personal information.

---

[4] *See*, Comments of Privacy Rights Clearinghouse *et. al.* on *Federal Agencies' Guidelines regarding Notification by Financial Companies when a Security Breach Compromises Customer Data and Exposes Individuals to Identity Theft*, November 2003 available at http://www.privacyrights.org/ar/secybreach.htm

[5] Cal. Civil Code § 1798.80 – 1798.82.

2) "Breach of the security of the system data" means unauthorized acquisition of computerized data that compromises the security, and confidentiality, or integrity of personal information maintained by the agency. Good faith acquisition of personal information by an employee or agent of the agency for a legitimate purpose of the agency is not a breach of the security of the system data, provided that the personal information is not used for a purpose unrelated to the agency or subject to further unauthorized disclosure. Breach of the security of non-computerized data may include but is not limited to unauthorized photocopying, facsimiles, or other paper-based transmittal of documents.

3) "Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:
   a) Social Security number.
   b) Driver's license number or state identification card number.
   c) Account number, credit or debit card number, if circumstances exist wherein such a number could be used without additional identifying information, access codes, or passwords.
   d) Account passwords or personal identification numbers (PINs) or other access codes.
   e) Any of item (a)-(d) when not in connection with the individual's first name or first initial and last name, if the information compromised would be sufficient to perform or attempt to perform identity theft against the person whose information was compromised.

"Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Subsection B. Notice of Breach.

1) Except as provided in paragraph 2 of subsection B, any data collector that owns or uses personal information in any form (whether computerized, paper, or otherwise) that includes personal information concerning a [State] resident shall notify the resident that there has been a breach of the security that data following discovery or notification of the breach, without regard for whether or not the data has or has not been accessed by an unauthorized third party for legal or illegal purposes. The disclosure notification shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in paragraph (2) of subsection B, or with any measures necessary to determine the scope of the breach and restore the reasonable integrity security and confidentiality of the data system.

2) The notification required by this section may be delayed if a law enforcement agency determines that the notification may impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

3) For purposes of this section, "notice" to consumers may be provided by one of the following methods:

a) Written notice.
b) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures, for notices legally required to be in writing, set forth in Section 7001 of Title 15 of the United States Code.
c) Substitute notice, if the agency demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000) or that the affected class of subject persons to be notified exceeds 500,000, or the agency does not have sufficient contact information. Substitute notice shall consist of all of the following:
   1. E-mail notice when the agency has an e-mail address for the subject persons.
   2. Conspicuous posting of the notice on the agency's Web site page, if the agency maintains one.
   3. Notification to major statewide media.

Subsection C. Waiver. Any waiver of the provisions of this title is contrary to public policy, and is void and unenforceable.

Subsection D. Remedies.

1) Any customer injured by a violation of this section may institute a civil action to recover damages.
2) Any business that violates, proposes to violate, or has violated this section may be enjoined.
3) The rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under law.

ALASKA STATE LEGISLATURE

Chair:
House Finance Subcommittees for;
Department of Public Safety
Department of Law

Member:
House Finance Committee
Legislative Council

Session:
Alaska State Capito
Juneau, AK 99801-1182
Phone: (907) 465-4958
Fax: (907) 465-4928

Interim:
PO Box 464
Chugiak, AK 99567

REPRESENTATIVE BILL STOLTZE

Representative_Bill_Stoltze@legis.state.ak.us

MEMORANDUM

TO: Representative Lesil McGuire, Chair
House Judiciary Committee

FROM: Bill Stoltze

DATE: February 17, 2005

SUBJECT: Hearing Request

I respectfully request a hearing be scheduled for House Bill 131, relating to access device & I.D. document crimes, as soon as possible.

Thank you for your consideration.

ALASKA STATE LEGISLATURE

Vice Chair:
House Finance Committee

Chair:
House Finance Subcommittees for,
Departme[illegible] of Public Safety
Department of Law

Session:
Alaska State Capitol
Juneau, AK 99801-1182
Phone: (907) 465-4958
Fax: (907) 465-4928

Interim:
PO Box 464
Chugiak, AK 99567

REPRESENTATIVE BILL STOLTZE

Representative_Bill_Stoltze@legis.state.ak.us

House Bill 131

Access Device & I.D. Document Crimes

"An Act increasing the criminal classification of theft of an access device and of obtaining an access device or identification documents by fraudulent means; increasing the criminal classification for certain cases of fraudulent use of an access device; and providing for an effective date."

Identity theft is on the increase in Alaska and our country as a whole. The Federal Trade Commission (FTC) reported that identity theft was up 33 percent in 2003. The State of Alaska ranks second in the number of complaints per 100,000 people.

These types of theft average $500; however, this does not take into consideration the countless hours a victim may spend tracking down and stopping the imposter, as well as time and legal costs to repair credit ratings and fight collection efforts. These changes would bring the penalties for such crimes closer in line with federal criminal laws, which provide for as much as 15 years in prison for similar crimes.

The provisions of HB 131:

- Increase the penalty from a class A misdemeanor to a class C felony for:
    1. Theft of an access device, such as a credit card or bank account number.
    2. The crime of fraudulent use of an access device if the value of the property or services obtained is $50 or more.
    3. The crime of obtaining an access device or identification document by fraudulent means.

I ask for your consideration and support of HB 131 to take a step towards meaningful deterrence and punishment for such crimes, which can impact all Alaskans.

National and State Trends in Fraud & Identity Theft

January - December 2004

Federal Trade Commission

February 1, 2005

Source: Data from Consumer Sentinel and the Identity Theft Data Clearinghouse

Report Subject **Page No.**

Consumer Sentinel
Leading Partners & Data Contributors

Between January and December 2004, Consumer Sentinel, the complaint database developed and maintained by the FTC, received over **635,000** consumer fraud and identity theft complaints. Consumers reported losses from fraud of more than $547 million. The reports in this booklet analyze those complaints.

Consumer Sentinel collects information about consumer fraud and identity theft from the FTC and over 150 other organizations and makes it available to law enforcement partners across the nation and throughout the world for use in their investigations. Launched in 1997, the Sentinel database now includes over two million complaints. Some data transfers from other organizations contain complaints from previous months and have not yet been received. Accordingly, the total number of complaints reflected in this report may increase over the course of the next few months. The addition of complaints from other data contributors is also reflected in the larger totals from previous years than were reported in earlier FTC reports.

For more information about Consumer Sentinel, as well as information about consumer fraud and identity theft, visit the Consumer Sentinel public website at www.consumer.gov/sentinel. If you represent a law enforcement organization, call (202) 326-3196 or e-mail sentinel@ftc.gov for membership information.

Australian Competition and Consumer Commission	*Better Business Bureaus*
Department of Defense	*Federal Bureau of Investigation*
Federal Trade Commission	*Internet Crime Complaint Center*
National Association of Attorneys General	*National Consumers League*
Canada's Phonebusters	*Social Security Administration*
U.S. Postal Inspection Service	*U.S. Secret Service*

The Consumer Sentinel Network (For a detailed description see Appendix A)

Consumer — www.consumer.gov/sentinel

econsumer.gov — www.econsumer.gov

Identity Theft Data Clearinghouse — www.consumer.gov/idtheft

Military — www.consumer.gov/military

Executive Summary
Federal Trade Commission (FTC) – 2004 National and State Trends in Fraud and Identity Theft

- Consumer Sentinel now contains over 2 million fraud and identity theft complaints and is accessible to more than 1,200 law enforcement agencies – including every state attorney general in the U.S. and consumer protection agencies in 19 nations.

- The FTC received over 635,000 Consumer Sentinel complaints during calendar year 2004 - 61% represented fraud and 39% were identity theft complaints.

Fraud

- A total of 388,603 of the Consumer Sentinel complaints were fraud-related. Internet Auctions was the leading complaint category with 16% of the overall complaints, followed by Shop-at-Home/Catalog Sales (8%), Internet Services and Computer Complaints (6%), Foreign Money Offers (6%), Prizes/Sweepstakes and Lotteries (5%), Advance-Fee Loans and Credit Protection (3%), Business Opportunities and Work-at-Home Plans (2%), and Telephone Services (2%).

- Consumers reported fraud losses of over $547 million; the median monetary loss was $259.

- Internet-related complaints accounted for 53% of all reported fraud complaints, with monetary losses of over $265 million and a median loss of $214.

- Some 57% of fraud complaints where the company's method of initial contact was reported indicate internet solicitations - electronic mail 35% and web 22%. 80% of all fraud complaints reported the method of initial contact. This is consistent with last year's report.

- The major metropolitan areas with the highest per capita rates of consumer fraud reported are the Washington DC area; San Jose-Sunnyvale-Santa Clara, CA; and Las Vegas-Paradise, NV.

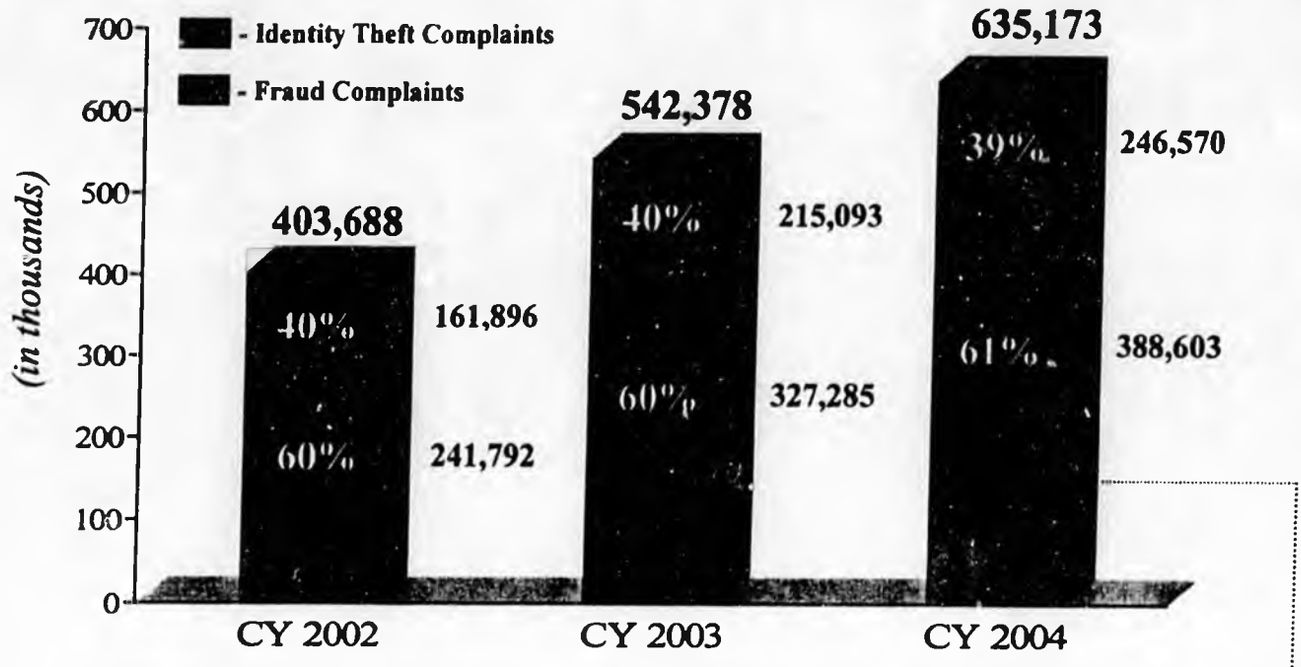
Identity Theft

- Credit card fraud (28%) was the most common form of reported identity theft followed by phone or utilities fraud (19%), bank fraud (18%), and employment fraud (13%). Other significant categories of identity theft reported by victims were government documents/benefits fraud and loan fraud.

- The percentage of complaints about "Electronic Fund Transfer" related identity theft more than doubled between 2002 and 2004.

- The major metropolitan areas with the highest per capita rates of reported identity theft are Phoenix-Mesa-Scottsdale, AZ; Riverside-San Bernardino-Ontario, CA; and Las Vegas-Paradise, NV.

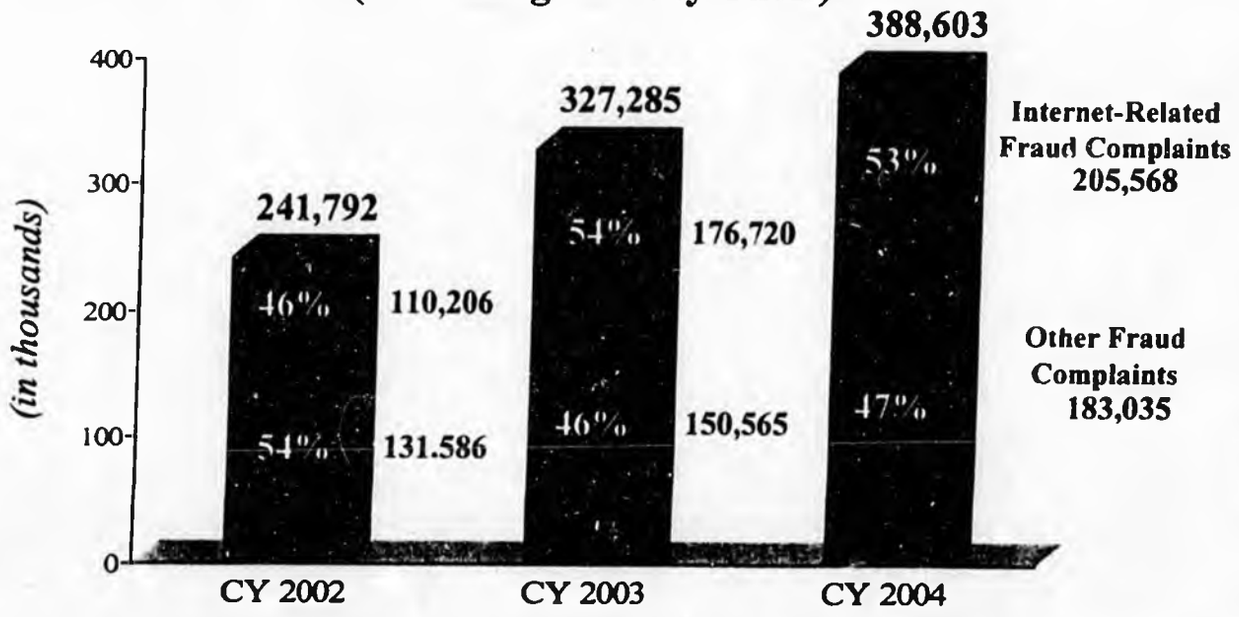
Sentinel Complaints by Calendar Year[1]



[1]Percentages are based on the total number of Sentinel complaints by calendar year. These figures exclude "Do Not Call" registry complaints.

Fraud Complaints by Calendar Year[2]

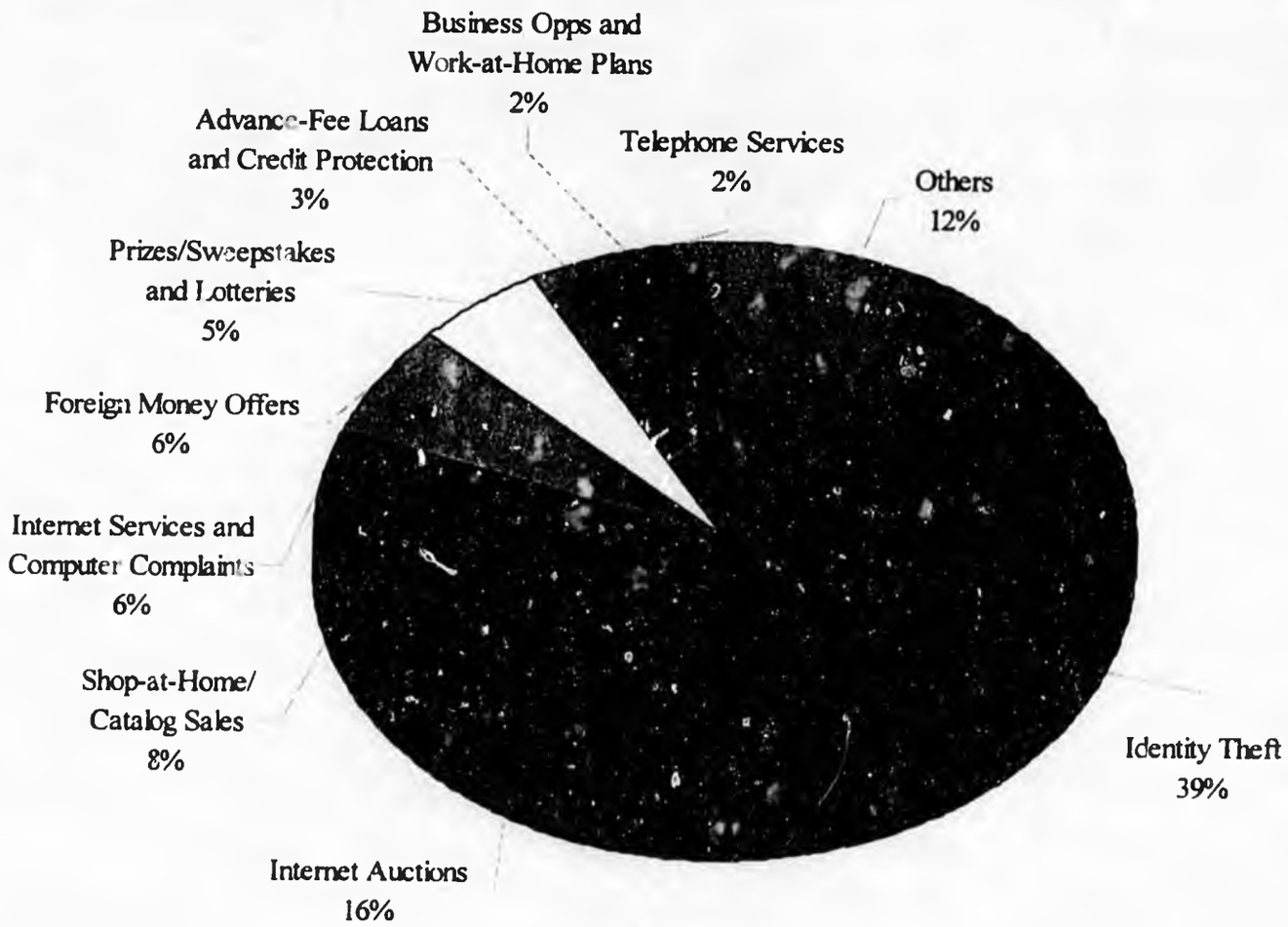
(Excluding Identity Theft)



[2]Percentages are based on the total number of Sentinel fraud complaints by calendar year.

Sentinel Top Complaint Categories[1]

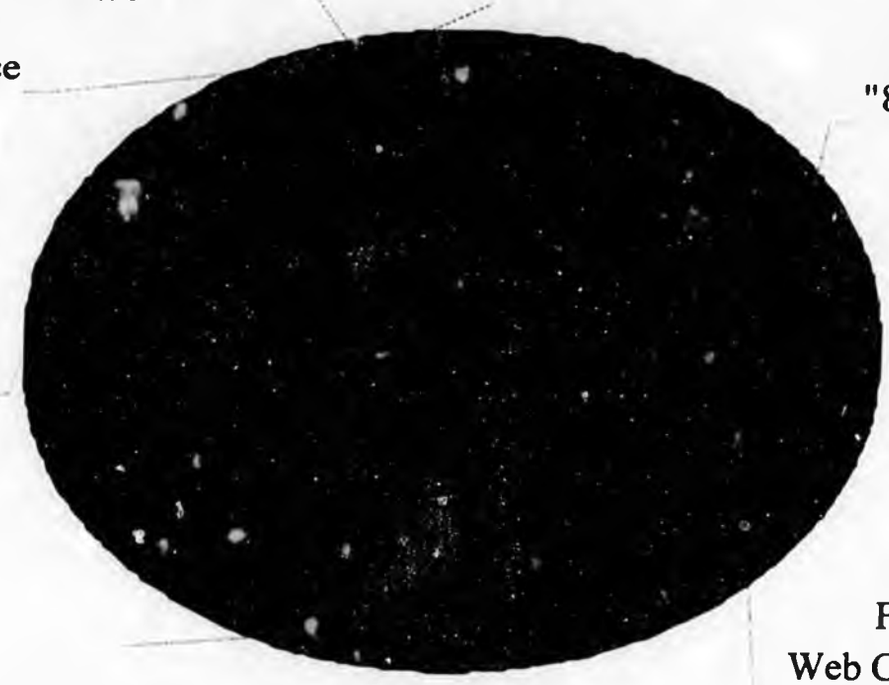
January 1 – December 31, 2004



[1]Percentages are based on the total number of Sentinel complaints **(635,173)** received between January 1 and December 31, 2004. For Sentinel category descriptions and three-year trends, see Appendices B and C.

Sentinel Data Contributors[1]

January 1 – December 31, 2004



[1]Percentages are based on the total number of Sentinel complaints (**635,173**) received between January 1 and December 31, 2004. The type of complaints provided by the organization is indicated in parentheses.

[2]For a list of other organizations contributing to Sentinel, see Appendix D.

Total Number of Fraud Complaints & Amount Paid

January 1 - December 31, 2004

388,603	296,525	76%	$547,854,781	$1,848	$259

[1]Average is based on the total number of consumers who reported amount paid (296,525). Forty-one consumers reported an amount paid of $1 million or more.

[2]Median is the middle number in a set of numbers so half the numbers have values that are greater than the median and half have values that are less. Calculation of the median excludes complaints with amount paid reported as $0.

Fraud Complaints by Reported Amount Paid

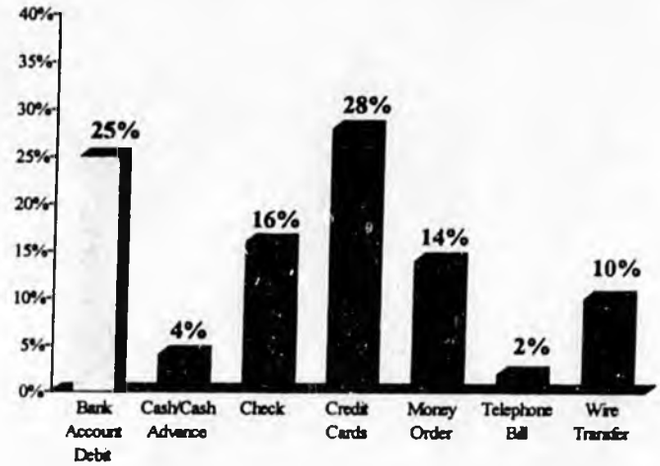
January 1 - December 31, 2004

$0	30%
$1 - 25	7%
$26 - 50	7%
$51 - 75	4%
$76 - 100	4%
$101 - 250	12%
$251 - 500	11%
$501 - 1,000	8%
$1,001 - 5,000	12%
More than $5,000	4%

[3]Percentages are based on the total number of consumers who reported amount paid (296,525). 76% of consumers reported this information.

Methods of Payment Reported by Consumers[4]

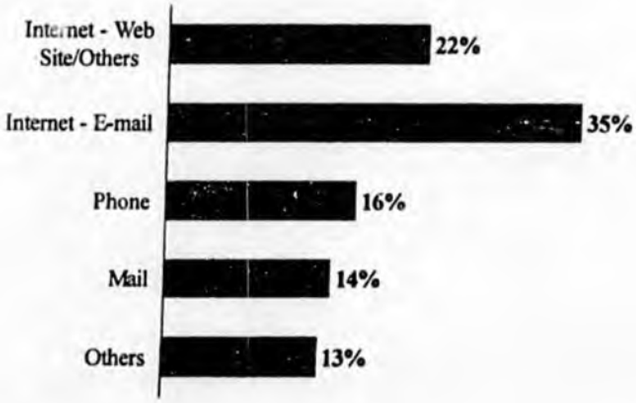
January 1 – December 31, 2004



[4]Percentages are based on the total number of consumers who reported the method of payment (71,175). 18% of consumers reported this information.

Company's Method of Contacting Consumers[5]

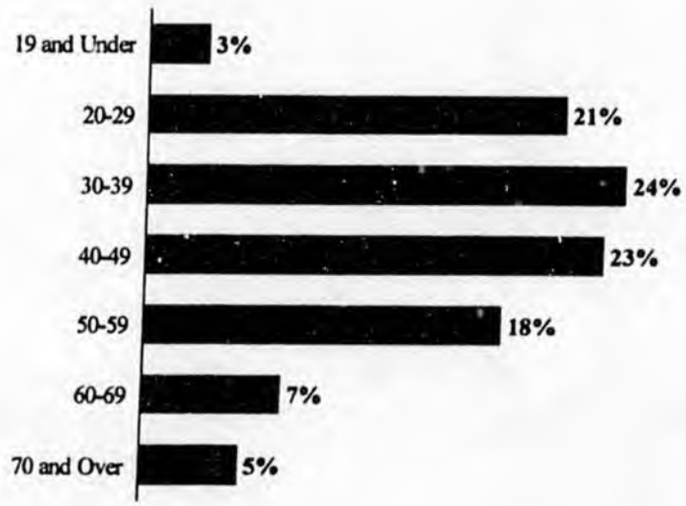
January 1 - December 31, 2004



[5]Percentages are based on the total number of fraud complaints where company's method of initial contact was reported by consumer (311,469). 80% of consumers reported this information.

Fraud Complaints by Consumer Age[6]

January 1 - December 31, 2004



[6]Percentages are based on the total number of fraud complaints where consumers reported their age (313,513). 81% of consumers reported their age.

Definition of "Internet-related": A fraud complaint is "Internet-related" if: it concerns an Internet product or service, the company initially contacts the consumer via the Internet, or the consumer responds via the Internet.

Total Number of Internet-Related Fraud Complaints & Amount Paid

January 1 - December 31, 2004

205,568	184,206	90%	$265,337,866	$1,440	$214

[1]Average is based on the total number of consumers who reported amount paid (184,206). Fifteen consumers reported an amount paid of $1 million or more.

[2]Median is the middle number in a set of numbers so that half the numbers have values that are greater than the median and half have values that are less. Calculation of the median excludes complaints with amount paid reported as $0.

Internet-Related Fraud Complaints by Reported Amount Paid

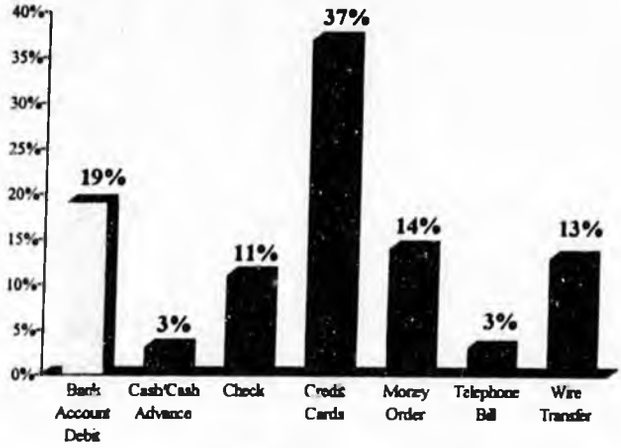
January 1 - December 31, 2004

$0	24%
$1 - 25	8%
$26 - 50	8%
$51 - 75	5%
$76 - 100	5%
$101 - 250	14%
$251 - 500	11%
$501 - 1,000	9%
$1,001 - 5,000	12%
More than $5,000	3%

[3]Percentages are based on the total number of consumers who reported amount paid (184,206). 90% of consumers reported this information.

Methods of Payment Reported by Consumers[4]

January 1 – December 31, 2004



[4]Percentages are based on the total number of consumers who reported the method of payment (31,077). 15% of consumers reported this information.

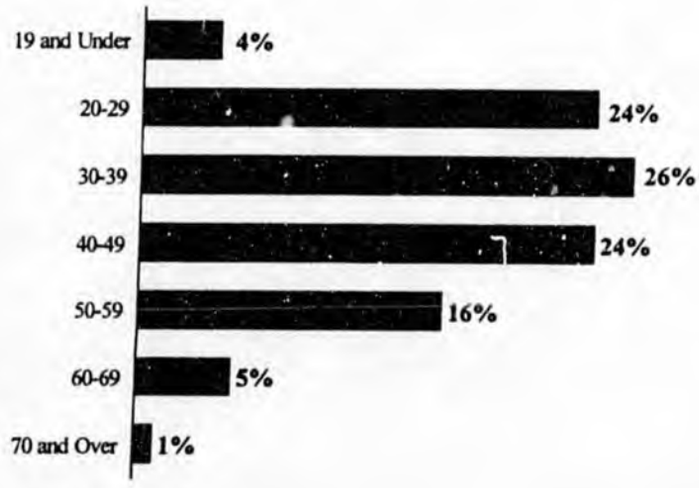
Top Products/Services for Internet-Related Fraud Complaints[5]

January 1 - December 31, 2004

[5]Percentages are based on the total number of Internet-related fraud complaints (205,568) received between January 1 and December 31, 2004.

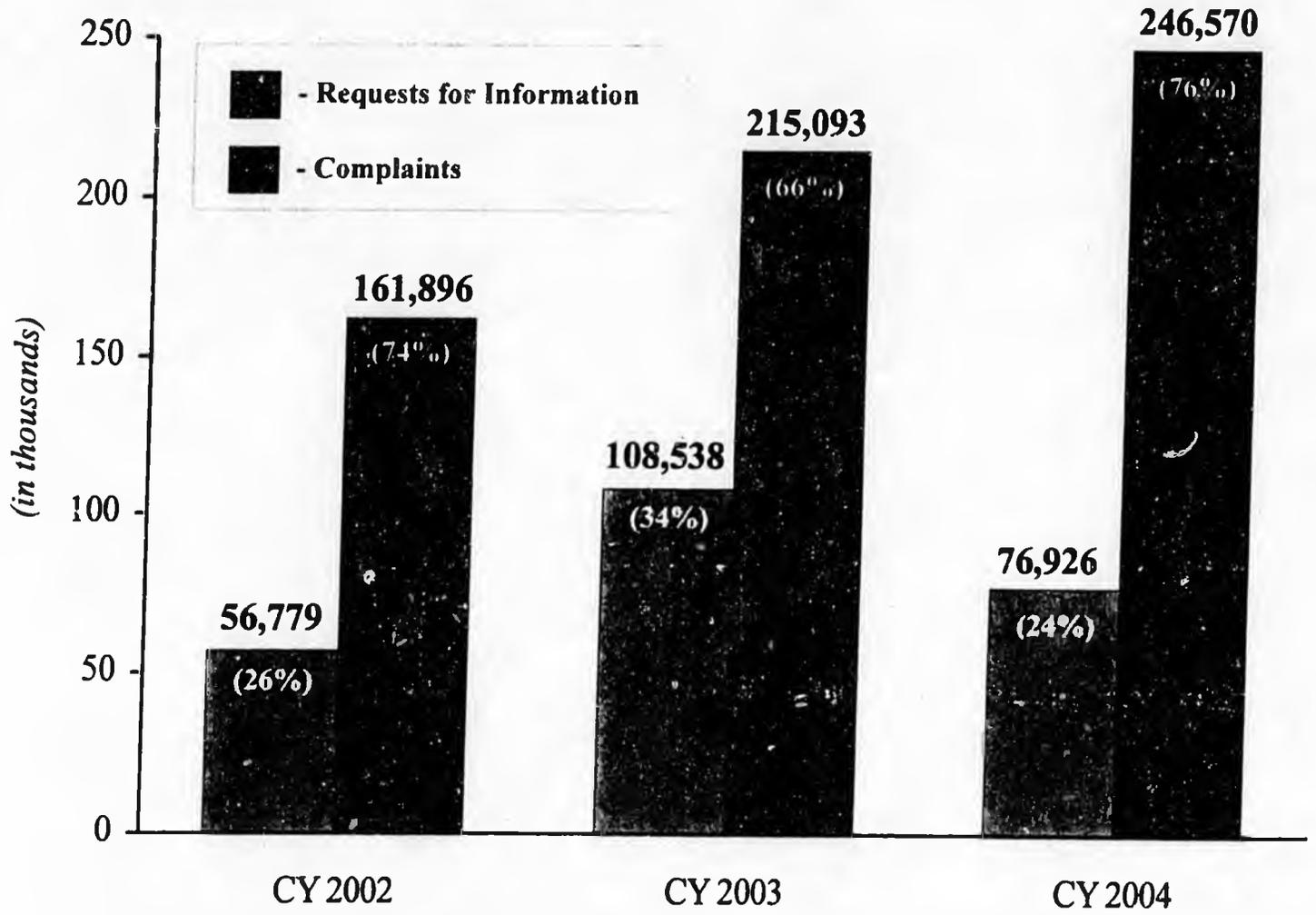
Internet-Related Fraud Complaints by Consumer Age[6]

January 1 - December 31, 2004



[6]Percentages are based on the total number of Internet-related fraud complaints where consumers reported their age (173,403). 84% of consumers reported their age.

Total Identity Theft Records[1] by Calendar Year



[1]Percentages are based on the total number of identity theft records by calendar year.

How Victims' Information is Misused[1]

Calendar Years 2002 through 2004

Credit Card Fraud

	Percentage	Percentage	Percentage
New Accounts	24.4%	19.3%	
Existing Account	12.2%	12.0%	
Unspecified	5.4%	1.4%	
Total	**41%**	**32%**	

Loan Fraud

	Percentage	Percentage	Percentage
Business / Personal / Student Loan	2.7%	2.3%	
Auto Loan / Lease	2.1%	2.0%	
Real Estate Loan	0.9%	1.0%	
Unspecified	0.5%	0.3%	
Total	**6%**	**5%**	

Phone or Utilities Fraud

	Percentage	Percentage	Percentage
Wireless - New	10.6%	10.4%	
Telephone - New	5.2%	5.6%	
Utilities - New	3.0%	3.8%	
Unauthorized Charges to Existing Accounts	0.7%	0.6%	
Unspecified	2.2%	0.8%	
Total	**20%**	**19%**	

Other Identity Theft

	Percentage	Percentage	Percentage
Other	9.1%	11.6%	
Illegal / Criminal	2.0%	2.1%	
Internet / E-mail	1.4%	1.6%	
Medical	1.7%	1.8%	
Apartment / House Rented	1.0%	0.9%	
Insurance[3]	—	0.3%	
Property Rental Fraud[3]	—	0.2%	
Bankruptcy	0.4%	0.3%	
Child Support[3]	—	0.2%	
Magazines[3]	—	0.1%	
Securities / Other Investments	0.2%	0.2%	
Total	**15%**	**19%**	

Bank Fraud[2]

	Percentage	Percentage	Percentage
Existing Accounts	8.1%	8.3%	
Electronic Fund Transfer	3.1%	4.8%	
New Accounts	3.7%	3.8%	
Unspecified	2.0%	0.5%	
Total	**16%**	**17%**	

Employment-Related Fraud

	Percentage	Percentage	Percentage
Employment-Related Fraud	**9%**	**11%**	

Attempted Identity Theft

	Percentage	Percentage	Percentage
Attempted Identity Theft	**8%**	**8%**	

Government Documents or Benefits Fraud

	Percentage	Percentage	Percentage
Fraudulent Tax Return	1.9%	3.7%	
Driver's License Issued / Forged	3.0%	2.3%	
Government Benefits Applied / Received	0.8%	1.3%	
Other Government Docs Issued / Forged	0.3%	0.4%	
Social Security Card Issued / Forged	1.7%	0.4%	
Unspecified	0.1%	<0.1%	
Total	**7%**	**8%**	

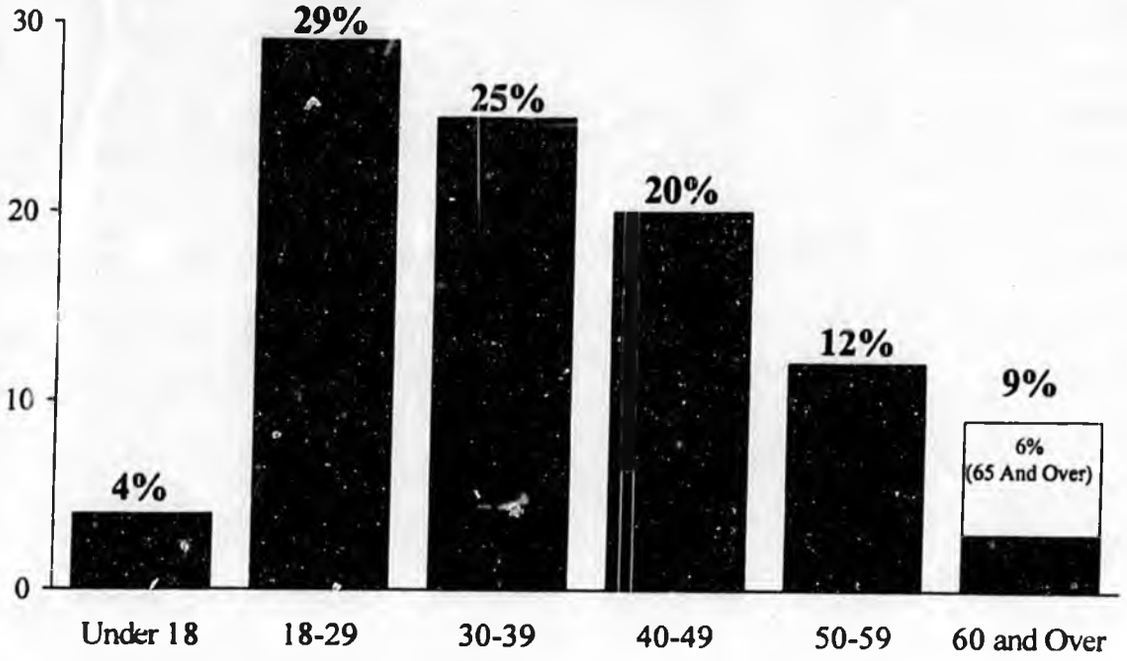
[1]Percentages are based on the total number of complaints in the Identity Theft Data Clearinghouse for each calendar year: CY 2002 = 161,896; CY 2003 = 215,093; CY 2004 = 246,570. Note that percentages total to more than 100 in each year because some victims reported experiencing more than one type of identity theft: 22% in CY 2002; 19% in CY 2003; and 19% in CY 2004.

[2]Includes fraud involving checking and savings accounts and electronic fund transfers.

[3]Theft subtype added in CY 2003.

Identity Theft Complaints by Victim Age[1]

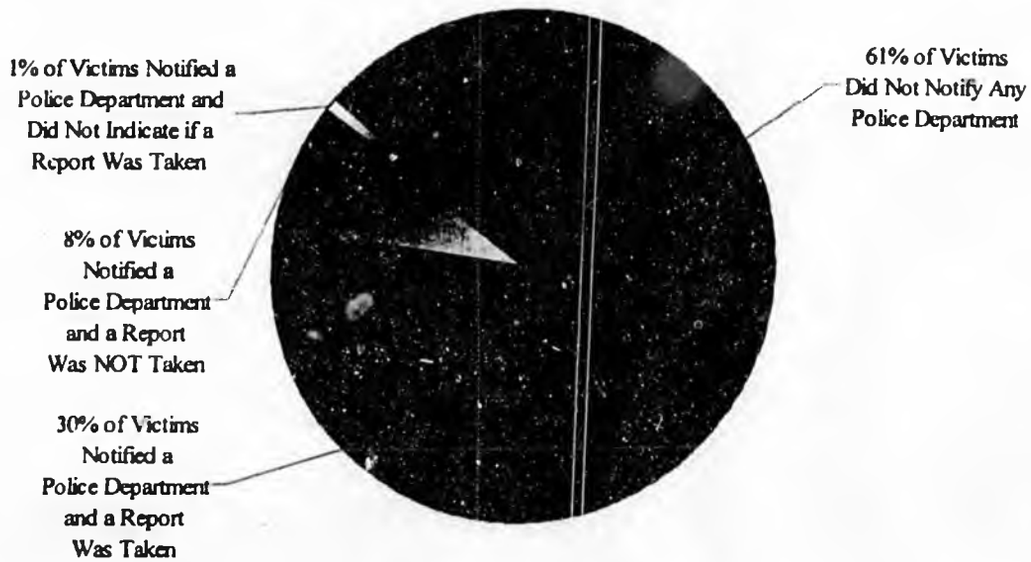
January 1 – December 31, 2004



[1]Percentages are based on the total number of identity theft complaints where victims reported their age (234,263). 95% of the victims who contacted the Federal Trade Commission directly reported their age.

Law Enforcement Contact[2]

January 1 – December 31, 2004



[2]Percentages are based on the total number of identity theft complaints where victims indicated whether they had notified a police department (239,945). 98% of the identity theft victims who contacted the Federal Trade Commission directly reported this information.

Major Metropolitan Areas for Fraud – Related Complaints[1]

January 1 – December 31, 2004

1	Washington-Arlington-Alexandria, DC-VA-MD-WV MSA	8,812	183.7
2	San Jose-Sunnyvale-Santa Clara, CA MSA	2,988	172.1
3	Las Vegas-Paradise, NV MSA	2,358	171.4
4	Columbus, OH MSA	2,726	169.0
5	Phoenix-Mesa-Scottsdale, AZ MSA	5,434	167.1
6	Austin-Round Rock, TX MSA	2,088	167.1
7	San Francisco-Oakland-Fremont, CA MSA	6,748	163.6
8	Tampa-St. Petersburg-Clearwater, FL MSA	3,898	162.7
9	Seattle-Tacoma-Bellevue, WA MSA	4,943	162.4
10	Sacramento--Arden-Arcade--Roseville, CA MSA	2,839	158.0
11	San Diego-Carlsbad-San Marcos, CA MSA	4,394	156.2
12	Portland-Vancouver-Beaverton, OR-WA MSA	2,987	154.9
13	Denver-Aurora, CO MSA	3,331	152.9
14	Orlando, FL MSA	2,427	147.6
15	Indianapolis, IN MSA	2,150	141.0
16	Jacksonville, FL MSA	1,503	133.9
17	Dallas-Fort Worth-Arlington, TX MSA	6,803	131.8
18	Virginia Beach-Norfolk-Newport News, VA-NC MSA	2,066	131.1
19	Kansas City, MO-KS MSA	2,401	130.8
20	Los Angeles-Long Beach-Santa Ana, CA MSA	15,963	129.1
21	Oklahoma City, OK MSA	1,386	126.5
22	Miami-Fort Lauderdale-Miami Beach, FL MSA	6,287	125.6
23	Milwaukee-Waukesha-West Allis, WI MSA	1,877	125.1
24	Pittsburgh, PA MSA	3,039	125.0
25	Rochester, NY MSA	1,297	125.0
26	Baltimore-Towson, MD MSA	3,167	124.1
27	Richmond, VA MSA	1,345	122.6
28	St. Louis, MO-IL MSA	3,270	121.2
29	Minneapolis-St. Paul-Bloomington, MN-WI MSA	3,589	120.9
30	Atlanta-Sandy Springs-Marietta, GA MSA	5,110	120.3
31	Riverside-San Bernardino-Ontario, CA MSA	3,876	119.1
32	Charlotte-Gastonia-Concord, NC-SC MSA	1,559	117.2
33	Cleveland-Elyria-Mentor, OH MSA	2,497	116.2
34	Hartford-West Hartford-East Hartford, CT MSA	1,329	115.7
35	Philadelphia-Camden-Wilmington, PA-NJ-DE-MD MSA	6,515	114.6
36	Boston-Cambridge-Quincy, MA-NH MSA	4,999	113.8
37	Nashville-Davidson--Murfreesboro, TN MSA	1,461	111.4
38	Chicago-Naperville-Joliet, IL-IN-WI MSA	9,991	109.8
39	New York-Northern New Jersey-Long Island, NY-NJ-PA MSA	19,736	107.7
40	Detroit-Warren-Livonia, MI MSA	4,748	106.6
41	Birmingham-Hoover, AL MSA	1,092	103.8
42	Buffalo-Niagara Falls, NY MSA	1,212	103.6
43	Cincinnati-Middletown, OH-KY-IN MSA	2,079	103.5
44	Louisville, KY-IN MSA	1,189	102.3
45	Houston-Baytown-Sugar Land, TX MSA	4,750	100.7
46	New Orleans-Metairie-Kenner, LA MSA	1,313	99.7
47	San Antonio, TX MSA	1,672	97.7
48	Providence-New Bedford-Fall River, RI-MA MSA	1,516	95.8
49	Memphis, TN-MS-AR MSA	1,088	90.3

[1]Ranking is based on the number of fraud complaints per 100,000 inhabitants for each metropolitan area. This chart illustrates major Metropolitan Statistical Areas (MSA) with a population of one million or more. Metropolitan areas presented here are those defined by the Office of Management and Budget (OMB) as of June 6, 2003 (http://www.census.gov/population/cen2000/phc-t29/tab03a.pdf).

Note: Statistics for CY 2003 included only MSAs with a population of two million or more.

Major Metropolitan Areas for Identity Theft – Related Complaints[1]

January 1 – December 31, 2004

Rank	Metropolitan Area	No. of Victims	Victims Per 100,000 Population
1	Phoenix-Mesa-Scottsdale, AZ MSA	5,924	182.2
2	Riverside-San Bernardino-Ontario, CA MSA	5,421	166.6
3	Las Vegas-Paradise, NV MSA	2,253	163.8
4	Dallas-Fort Worth-Arlington, TX MSA	7,524	145.8
5	Houston-Baytown-Sugar Land, TX MSA	6,563	139.2
6	Los Angeles-Long Beach-Santa Ana, CA MSA	17,078	138.1
7	Miami-Fort Lauderdale-Miami Beach, FL MSA	6,577	131.3
8	San Antonio, TX MSA	2,201	128.6
9	San Francisco-Oakland-Fremont, CA MSA	5,284	128.1
10	San Diego-Carlsbad-San Marcos, CA MSA	3,569	126.8
11	Atlanta-Sandy Springs-Marietta, GA MSA	5,191	122.2
12	Orlando, FL MSA	1,926	117.1
13	Sacramento--Arden-Arcade--Roseville, CA MSA	2,102	117.0
14	Denver-Aurora, CO MSA	2,517	115.5
15	Portland-Vancouver-Beaverton, OR-WA MSA	2,222	115.3
16	Austin-Round Rock, TX MSA	1,417	113.4
17	Seattle-Tacoma-Bellevue, WA MSA	3,291	108.1
18	Washington-Arlington-Alexandria, DC-VA-MD-WV MSA	5,142	107.2
19	Chicago-Naperville-Joliet, IL-IN-WI MSA	9,746	107.1
20	New York-Northern New Jersey-Long Island, NY-NJ-PA MSA	18,988	103.6
21	Charlotte-Gastonia-Concord, NC-SC MSA	1,322	99.4
22	Detroit-Warren-Livonia, MI MSA	4,406	99.0
23	Memphis, TN-MS-AR MSA	1,147	95.2
24	San Jose-Sunnyvale-Santa Clara, CA MSA	1,645	94.8
25	Tampa-St. Petersburg-Clearwater, FL MSA	2,210	92.2
26	Kansas City, MO-KS MSA	1,687	91.9
27	Indianapolis, IN MSA	1,375	90.2
28	Jacksonville, FL MSA	960	85.5
29	Philadelphia-Camden-Wilmington, PA-NJ-DE-MD MSA	4,782	84.1
30	Baltimore-Towson, MD MSA	2,142	83.9
31	Cleveland-Elyria-Mentor, OH MSA	1,754	81.7
32	Milwaukee-Waukesha-West Allis, WI MSA	1,182	78.8
33	St. Louis, MO-IL MSA	2,048	75.9
34	Columbus, OH MSA	1,204	74.7
35	Oklahoma City, OK MSA	812	74.1
36	Minneapolis-St. Paul-Bloomington, MN-WI MSA	2,194	73.9
37	Richmond, VA MSA	746	68.0
38	New Orleans-Metairie-Kenner, LA MSA	890	67.6
39	Virginia Beach-Norfolk-Newport News, VA-NC MSA	1,017	64.5
40	Rochester, NY MSA	695	64.1
41	Birmingham-Hoover, AL MSA	673	64.0
42	Nashville-Davidson--Murfreesboro, TN MSA	826	63.0
43	Boston-Cambridge-Quincy, MA-NH MSA	2,758	62.8
44	Buffalo-Niagara Falls, NY MSA	682	58.3
45	Hartford-West Hartford-East Hartford, CT MSA	641	55.8
46	Louisville, KY-IN MSA	605	52.1
47	Cincinnati-Middletown, OH-KY-IN MSA	1,044	51.9
48	Providence-New Bedford-Fall River, RI-MA MSA	791	50.0
49	Pittsburgh, PA MSA	1,211	49.8

[1]Ranking is based on the number of identity theft victims per 100,000 inhabitants for each metropolitan area. This chart illustrates major Metropolitan Statistical Areas (MSA) with a population of one million or more. Metropolitan areas presented here are those defined by the Office of Management and Budget (OMB) as of June 6, 2003 (http://www.census.gov/population/cen2000/phc-t29/tab03a.pdf).

Note: Statistics for CY 2003 included only MSAs with a population of two million or more.

FRAUD COMPLAINTS BY CONSUMER STATE

IDENTITY THEFT VICTIMS BY STATE

January 1 - December 31, 2004

Rank	Consumer State	Complaints Per 100,000 Population	Number of Complaints
1	Arizona	180.5	10,366
2	Alaska	174.4	1,143
3	Nevada	151.3	3,532
4	Washington	151.2	9,378
5	Hawaii	143.1	1,807
6	Colorado	142.5	6,558
7	Virginia	134.4	10,023
8	New Hampshire	133.4	1,734
9	Oregon	132.3	4,756
10	Maryland	131.3	7,298
11	California	130.6	46,867
12	Florida	128.0	22,263
13	Wyoming	127.9	648
14	Delaware	126.6	1,051
15	New Mexico	124.3	2,365
16	Utah	122.5	2,927
17	Wisconsin	120.6	6,643
18	Pennsylvania	119.2	14,786
19	Connecticut	119.0	4,170
20	Montana	118.8	1,101
21	Illinois	116.1	14,766
22	Indiana	114.9	7,168
23	Nebraska	114.6	2,092
24	Ohio	114.0	13,066
25	New Jersey	114.0	9,917
26	Idaho	112.3	1,565
27	Kansas	111.8	3,059
28	Missouri	111.2	6,398
29	South Carolina	109.3	4,588
30	Vermont	109.3	679
31	Michigan	108.8	10,998
32	Massachusetts	108.7	6,976
33	New York	107.7	20,699
34	Minnesota	103.6	5,284
35	Maine	102.1	1,345
36	West Virginia	101.1	1,835
37	Rhode Island	100.8	1,089
38	Oklahoma	97.7	3,444
39	North Carolina	97.1	8,291
40	Georgia	96.8	8,549
41	Texas	95.3	21,435
42	Tennessee	91.6	5,406
43	Alabama	91.5	4,143
44	North Dakota	90.0	571
45	Iowa	89.5	2,645
46	Kentucky	88.4	3,667
47	South Dakota	86.0	663
48	Louisiana	80.3	3,625
49	Arkansas	75.7	2,085
50	Mississippi	66.8	1,939

Rank	Victim State	Victims Per 100,000 Population	Number of Victims
1	Arizona	142.5	8,186
2	Nevada	125.7	2,935
3	California	122.1	43,839
4	Texas	117.6	26,454
5	Colorado	95.8	4,409
6	Florida	92.3	16,062
7	New York	92.0	17,680
8	Washington	91.1	5,654
9	Oregon	87.8	3,156
10	Illinois	87.6	11,138
11	Georgia	84.3	7,440
12	New Mexico	83.4	1,588
13	Maryland	83.0	4,612
14	Utah	76.6	1,831
15	New Jersey	75.1	6,530
16	Michigan	72.3	7,307
17	Indiana	68.5	4,274
18	Missouri	67.9	3,905
19	Delaware	66.6	553
20	Alaska	66.1	433
21	North Carolina	65.8	5,623
22	Virginia	63.6	4,742
23	Kansas	61.3	1,677
24	Massachusetts	61.1	3,921
25	Pennsylvania	61.0	7,563
26	Ohio	60.7	6,956
27	Connecticut	57.1	2,000
28	Minnesota	57.0	2,905
29	Oklahoma	56.0	1,973
30	Tennessee	55.0	3,246
31	South Carolina	51.2	2,148
32	Arkansas	50.8	1,397
33	Hawaii	50.7	640
34	Rhode Island	50.6	547
35	Louisiana	49.9	2,254
36	Alabama	48.9	2,216
37	Wisconsin	48.0	2,646
38	Mississippi	46.5	1,350
39	Nebraska	45.1	788
40	Idaho	43.1	600
41	Wyoming	42.2	214
42	New Hampshire	41.8	543
43	Kentucky	40.1	1,662
44	Montana	39.3	364
45	Iowa	34.8	1,028
46	West Virginia	34.2	621
47	Vermont	33.5	208
48	Maine	32.2	424
49	North Dakota	29.6	188
50	South Dakota	23.2	179

Note: Per 100,000 unit of population estimates are based on the 2004 U.S. Census population estimates (Table NST-EST2004-01 - Annual Estimates of the Population for the United States and States, and for Puerto Rico: April 1, 2000 to July 1, 2004). Numbers for the District of Columbia are: Fraud = 1,196 complaints and 216.1 complaints per 100,000 population; Identity Theft = 922 victims and 166.6 victims per 100,000 population.

Detailed State Information

(one page per state and the District of Columbia)

Fraud Complaints

- Top Fraud Complaint Categories for Consumers
- Amount Paid Reported by Consumers
- Top Consumer City Locations for Fraud Complaints

Identity Theft Complaints

- Identity Theft Types Reported by Victims
- Top Identity Theft Victim City Locations

ALASKA
Consumer Sentinel Complaint Statistics and Trends
January 1 - December 31, 2004

Total Number of Fraud and Identity Theft Complaints from Alaska Consumers = 1,576

Fraud Complaints from Alaska Consumers = 1,143

Top Fraud Complaint Categories for Alaska Consumers

1	Foreign Money Offers	257	22%
2	Internet Auctions	231	20%
3	Prizes/Sweepstakes and Lotteries	139	12%
4	Shop-at-Home/Catalog Sales	118	10%
5	Internet Services and Computer Complaints	81	7%

[1]Percentages are based on the total number of fraud complaints from Alaska consumers (1,143).

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]
1,143	$588,379	778	68%	$756

[2]Average amount paid is based on the total number of fraud complaints where amount paid was reported by Alaska consumers (778).

Top Alaska Consumer Locations for Fraud Complaints

Consumer City	No. of Complaints
Anchorage	388
North Pole	174
Fairbanks	88
Wasilla	59
Eagle River	44

Identity Theft Complaints from Alaska Victims = 433

Identity Theft Types Reported by Alaska Victims

1	Credit Card Fraud	127	29%
2	Phone or Utilities Fraud	78	18%
3	Bank Fraud[2]	59	14%
4	Government Documents or Benefits Fraud	33	8%
5	Employment-Related Fraud	30	7%
6	Loan Fraud	18	4%
	Other	129	30%
	Attempted Identity Theft	31	7%

[1]Percentages are based on the 433 victims reporting from Alaska. Percentages add to more than 100 because approximately 17% of victims from Alaska reported experiencing more than one type of identity theft.
[2]Includes fraud involving checking and savings accounts and electronic fund transfers.

Top Alaska Identity Theft Victim Locations

Victim City	No. of Victims
Anchorage	135
Fairbanks	22
Wasilla	19
Juneau	11
Eagle River	10
Palmer	10

FISCAL NOTE

STATE OF ALASKA
2005 LEGISLATIVE SESSION

Fiscal Note Number:
Bill Version: HB 131
() Publish Date:

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

Title: An act increasing criminal class. for access device crimes...
RDU: Legal and Advocacy Services
Component: Public Defender Agency

Sponsor: Reps. Stoltze, McGuire
Requester: House Judiciary
Component No.: 1631

Expenditures/Revenues (Thousands of Dollars)

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

OPERATING EXPENDITURES	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
Personal Services	*	*	*	*	*	*
Travel						
Contractual						
Supplies						
Equipment						
Land & Structures						
Grants & Claims						
Miscellaneous						
TOTAL OPERATING	*	*	*	*	*	*
CAPITAL EXPENDITURES						
CHANGE IN REVENUES ( )						

FUND SOURCE (Thousands of Dollars)

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

Estimate of any current year (FY2005) cost: 0.0
Mark this box (X) if funding for this bill is included in the Governor's FY 2006 budget proposal:

POSITIONS

Full-time						
Part-time						
Temporary						

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

This bill seeks to amend several offenses related to access devices, like credit cards and bank account numbers, and ID documents to raise the penalty from a misdemeanor to a felony for the theft of, fraudulent use of, and for fraudulently obtaining an access device or ID document. This increase in penalties will increase the workload of the Agency. It is far more costly to defend a person charged with a felony than a misdemeanor. Some of these offenses are currently prosecutable by municipalities as misdemeanors, and if they become felonies, they will be prosecuted by the state resulting in more public defender appointments. It is not possible to predict how many current PD-appointed cases will be affected or new cases appointed, therefore an indeterminate fiscal note is submitted.

Prepared by: Linda K. Wilson, Deputy Director
Phone (907)334-4416
Division: Public Defender Agency
Date/Time 2/22/05 9:54 AM
Approved by: Michael Tibbles, Deputy Commissioner
Date 2/22/2005
Agency: Department of Administration

FISCAL NOTE

STATE OF ALASKA
2005 LEGISLATIVE SESSION

Fiscal Note Number:
Bill Version: HB 131
() Publish Date:

Revision Date/Time (Note if correction):
Dept. Affected: Corrections
Title "An act increasing the criminal classification of theft of an access device and of obtaining an access device..."
RDU Institutional Facilities
Component Institution Director's Office
Sponsor Representatives Stoltze, McGuire
Requester Judiciary, Finance
Component No. 524

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	0.0	0.0	0.0	0.0	0.0	0.0
Travel	0.0	0.0	0.0	0.0	0.0	0.0
Contractual	0.0	0.0	0.0	0.0	0.0	0.0
Supplies	0.0	0.0	0.0	0.0	0.0	0.0
Equipment	0.0	0.0	0.0	0.0	0.0	0.0
Land & Structures	0.0	0.0	0.0	0.0	0.0	0.0
Grants & Claims	0.0	0.0	0.0	0.0	0.0	0.0
Miscellaneous	0.0	0.0	0.0	0.0	0.0	0.0
TOTAL OPERATING	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**
CAPITAL EXPENDITURES	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**
CHANGE IN REVENUES ( )	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**

FUND SOURCE (Thousands of Dollars)

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

Estimate of any current year (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	0	0	0	0	0	0
Part-time	0	0	0	0	0	0
Temporary	0	0	0	0	0	0

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

Due to the estimated small number of successful prosecutions that may occur as a result of the changes contained in the legislation, the department does not anticipate a significant fiscal impact to the Department of Corrections.

Prepared by: Sharleen Griffin, Acting Director
Phone 465-4641
Division Administrative Services
Date/Time 2/25/05 10:26 AM
Approved by: Portia C.K. Parker, Deputy Commissioner
Date 2/25/2005
Agency Department of Corrections

FISCAL NOTE

STATE OF ALASKA
2005 LEGISLATIVE SESSION

Fiscal Note Number:
Bill Version: HB131-LAW-CDCO-2-22
() Publish Date:

Revision Date/Time (Note if correction):
Dept. Affected: LAW
Title "An Act increasing the criminal classification of theft of an access device and of obtaining an access...
RDU CRIMINAL
Component CDCO
Sponsor Representative Stoize
Requester House Judiciary
Component No.

Expenditures/Revenues (Thousands of Dollars)

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

OPERATING EXPENDITURES	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
Personal Services						
Travel						
Contractual						
Supplies						
Equipment						
Land & Structures						
Grants & Claims						
Miscellaneous						
TOTAL OPERATING	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**
CAPITAL EXPENDITURES						
CHANGE IN REVENUES ( )						

FUND SOURCE (Thousands of Dollars)

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

Estimate of any current year (FY2005) cost: 0.0
Mark this box (X) if funding for this bill is included in the Governor's FY 2006 budget proposal:

POSITIONS

Full-time						
Part-time						
Temporary						

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

This bill amends sections of AS 11.46. and would protect citizens, businessess, and financial institutions by increasing the penalty for certain types of identity theft and fraud crimes. The bill would increase the penalty from a class A misdemeanor to a class C felony for (1) theft of an access device, such as a credit card or bank account number, (2) the crime of fraudulent use of an access device if the value of the property or services obtained is $50 or more, and (3) the crime of obtaining an access device or identification document by fraudulent means. The Department of Law does not anticipate a fiscal impact from passage of this legislation.

Prepared by: Kathryn Daughhetee, Director
Phone 465-5427
Division Administrative Services
Date/Time 2/22/05 4:21 PM
Approved by: K. Daughhetee for Scott Nordstrand, Acting Attorney General
Date 2/22/2005
Agency Department of Law

FISCAL NOTE

STATE OF ALASKA
2005 LEGISLATIVE SESSION

Fiscal Note Number:
Bill Version: HB131-DPS-AST-2-22-05
() Publish Date:

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

Title: An Act increasing classification of theft of an access device & obaining an access device or identification...
RDU: Alaska State Troopers
Component: AST Detachments

Sponsor: Representatives Stoltze, McGuire
Requester:
Component No.: 2325

Expenditures/Revenues (Thousands of Dollars)

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

OPERATING EXPENDITURES	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
Personal Services						
Travel						
Contractual						
Supplies						
Equipment						
Land & Structures						
Grants & Claims						
Miscellaneous						
TOTAL OPERATING	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**
CAPITAL EXPENDITURES						
CHANGE IN REVENUES ( )						

FUND SOURCE (Thousands of Dollars)

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

Estimate of any current year (FY2005) cost: 0.0
Mark this box (X) if funding for this bill is included in the Governor's FY 2006 budget proposal:

POSITIONS

Full-time						
Part-time						
Temporary						

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

This bill amends AS 11.46.130 and adds an "access device" [defined in AS 11.81.900(b)(1)] to the crime of theft in the second degree which will increase the criminal classification for theft of an "access device" from a Class A Misdemeanor to a Class C Felony. The bill also increases the criminal classification for fraudulent use of an access device in AS 11.46.285. It will increase the penalty to a Class C Felony if the theft of property or services obtained is $50 or more, but less than $25,000. The present value for a Class C Felony is $500 or more, but less than $25,000.

No fiscal impact on the Department of Public Safety is anticipated.

Prepared by: Lieutenant Todd Sharp
Phone: 907-465-3223
Division: Alaska State Troopers
Date/Time: 2/22/05 5:37 PM

Approved by: Commissioner William Tandeske
Date: 2/22/2005
Agency: Department of Public Safety