



Alaska State Legislature

Senator Gretchen Guess

<http://guess.akdemocrats.org>

Senator Gretchen Guess

Juneau: 907-465-2435

Juneau Toll Free: 800-550-2435

Fax: 907-465-6615

guess@akdemocrats.org

FOR IMMEDIATE RELEASE · April 20, 2006

IDENTITY THEFT IN ALASKA ***Guess, Therriault address growing problem***

JUNEAU – A bill intended to stem the rising tide of identity theft in Alaska is awaiting a hearing in the Senate Finance Committee.

SB 222, sponsored by Sen. Gretchen Guess (D-Anchorage) and Sen. Gene Therriault (R-North Pole) is designed to secure consumers' private information and provide consumers with tools to protect against and recover from identity theft. The bill has been assigned to Senate Finance, but not been brought up again after an introductory hearing on March 23rd.

Over the last six years, Alaska has seen a steady increase in the number of identity theft crimes. Last year alone, Alaskans reported the highest number of fraud complaints per person in the nation. This year has seen a dramatic increase in crimes resulting from the fraudulent use of Alaskans' personal information, and a pressing need for our lawmakers to take action to protect Alaskan consumers.

As recent events in the Mat-Su Borough, Fairbanks, and Anchorage have shown, the results of identity theft related fraud are a serious and growing problem in Alaska. Police in those areas have estimated the cost of fraudulently purchased goods in a recent rash of mailbox thefts at nearly a half million dollars. Reports indicate there were as many as 500 victims over the last six months, many of whom were unaware of any fraudulent activity.

One identity theft victim from the Mat-Su has described the situation as "intolerable." Although victims are often able to get in touch with their banks and identify what charges were fraudulently made, they often do not realize the lasting effect it can have on their credit report. A poor credit report can result in being denied loans for homes or automobiles, and can substantially affect a person's life.

For additional information, please call [Senator Guess](tel:907-465-2435) at 465-2435 or [Senator Therriault](tel:907-465-4797) at 465-4797.

NOTE: For detailed information relating to identity theft and [SB 222](#), please refer to the point paper provided below.

I. Identity Theft in Alaska; SB 222

- Identity theft occurs when someone uses your personal information without your permission to commit fraud or other crimes.
- Identity theft is a *major problem* in the United States, to an extent that most financial institutions are not willing to admit.
- In Alaska, reported instances of identity theft number into the hundreds every year.

- SB222 addresses the problem by making it harder for identity thieves to obtain personal consumer information, as well as providing safeguards for the consumer should a breach of information occur.

II. How does identity theft happen?

- Identity theft can happen in a number of ways; ranging from such simple means as "dumpster diving" for personal records, to more sophisticated methods, such as electronically hacking the databases of financial institutions.
- Essentially, personal information is at risk when it becomes accessible to anyone other than the person for whom it was intended. Bank account statements, loan and credit card statements, physician's statements, office records and even data storage devices such as computer hard drives, floppy disks and CD's, can all be obtained if they are not kept in a secure location, erased or destroyed.
- In addition to sifting through discarded papers, identity thieves commonly intercept sensitive information by stealing mail or even picking pockets for credit cards, social security cards, licenses and other identifying documents.
- As opposed to taking personal information without the consumer's knowledge, identity thieves can impersonate financial institutions, Internet service providers and even government agencies by requesting personal information over the phone, through the mail and in email (commonly known as "phishing").
- The most disturbing form of identity theft happens when consumers have no control and often, no knowledge of their personal information having been compromised. Cases have ranged from hackers breaking into company and merchant databases to recent incidents of computers containing sensitive data having been lost or stolen.

III. What are its effects?

- The effects of identity theft can be devastating. Often, consumers do not know that their identities have been stolen until fraudulent activities are committed.
- According to the Federal Trade Commission, personal information can be used in a number of ways, including but not limited to:
 - *Calling your credit card issuer to change the billing address on your credit card account. The imposter then runs up charges on your account. Because your bills are being sent to a different address, it may be some time before you realize there's a problem.*
 - *Opening new credit card accounts in your name. When they use the credit cards and don't pay the bills, the delinquent accounts are reported on your credit report.*
 - *Establishing phone or wireless service in your name.*
 - *Opening a bank account in your name and writing bad checks on that account.*
 - *Counterfeiting checks or credit or debit cards, or authorizing electronic transfers in your name, and draining your bank account.*

- Filing for bankruptcy under your name to avoid paying debts they've incurred under your name, or to avoid eviction.

- Buying a car by taking out an auto loan in your name.

- Getting identification such as a driver's license issued with their picture, in your name.

- Getting a job or file fraudulent tax returns in your name.

- Giving your name to the police during an arrest. If they don't show up for their court date, a warrant for arrest is issued in your name.

Poor credit ratings are the most common result of identity theft crimes, and can affect a person's ability to purchase a home or vehicle, take out loans, obtain a credit card. A poor credit rating can haunt a person for years, and prevent them from living a normal life.

IV. What will SB222 do to help?

- When the personal records of consumers are compromised through a security breach, record keepers must notify affected parties without unreasonable delay. (Establishes penalties and civil remedies.)
- SB222 allows an individual to invoke a security freeze to be placed on all or part of personal information being released by a consumer-reporting agency about the individual. (Establishes civil remedy and penalties.)
- SB222 requires credit agencies to be accurate in their reporting and responsible for any damage caused through the release of inaccurate credit information, including compensation. (Establishes civil remedy.)
- SB222 limits the public release of a person's social security number except with consent. (Establishes penalties and civil remedies for violations.)
- SB222 requires responsible protection in the disposal of personal information through the use of effective record destruction. (Establishes penalties and civil remedies for violations.)
- SB 222 provides the ability to file police reports of identity theft and obtain court declarations of innocence, valuable steps in reclaiming one's identity.

V. How can you protect yourself in the meantime?

- The best way to protect yourself from fraud arising out of identity theft is to monitor your financial statements carefully, and order a free copy of your credit report at www.annualcreditreport.com.
- If you use the internet, the Federal Trade Commission suggests these tips to help you avoid becoming a victim of electronic identity theft.
 - If you get an email or pop-up message that asks for personal or financial information, do not reply, and don't click on the link in the message, either.*
 - Use anti-virus software and a firewall, and keep them up to date.*
 - Don't email personal or financial information.*

- *Review credit card and bank account statements as soon as you receive them.*
- Be cautious about opening any attachment or downloading any files from emails.
- *Forward spam that is "phishing" for information to spam@uce.gov .*

In addition, The Federal Trade Commission suggests the following tips to avoid identity theft in your everyday life.

- *Place passwords on your credit card, bank, and phone accounts.*
- *Secure personal information in your home.*
- Ask about information security procedures in your workplace or at businesses, doctor's offices or other institutions that collect your personally identifying information.
- Don't give out personal information on the phone, through the mail, or on the Internet unless you've initiated the contact or are sure you know who you're dealing with.
- Treat your mail and trash carefully.
- Deposit your outgoing mail in post office collection boxes or at your local post office, rather than in an unsecured mailbox.
- Tear or shred your charge receipts, copies of credit applications, insurance forms, physician statements, checks and bank statements, expired charge cards that you're discarding, and credit offers you get in the mail.
- Don't carry your Social Security number card; leave it in a secure place.
- Give your Social Security number only when absolutely necessary, and ask to use other types of identifiers.
- Carry only the identification information and the credit and debit cards that you'll actually need when you go out.
- *Be cautious when responding to promotions. Identity thieves may create phony promotional offers to get you to give them your personal information.*
- Keep your purse or wallet in a safe place at work; do the same with copies of administrative forms that have your sensitive personal information.
- When ordering new checks, pick them up from the bank instead of having them mailed to your home mailbox.

VI. What do you do if it happens to you?

- If you are a victim of identity theft, the Federal Trade Commission advises you take these four steps as soon as possible.
 1. *Place a fraud alert on your credit reports, and review your credit reports.*
 2. *Close the accounts that you know, or believe, have been tampered with or opened*

fraudulently.

3. File a report with your local police or the police in the community where the identity theft took place.

4. File a complaint with the Federal Trade Commission.


For more information on SB222, please visit:

<http://www.akdemocrats.org/index.php?bill=SB222>

For more information on identity theft and how to protect yourself, please visit:

<http://www.consumer.gov/idtheft/>

###

-  Print  Forward this page
-  http://www.akdemocrats.org/guess/042006_identity_theft_in_AK.pdf
- **Links:** [SB222 Senator Gretchen Guess](#)

Alaska Can Do Better.
Working for a [Safer](#), [Healthier](#), [Smarter](#) and [Richer](#) Alaska