State Legislation Beyond Federal Law*

To date, a number of states have passed their own laws restricting the sale and/or possession of OTC products that contain PSE.

1. *Alabama*
2. *Arizona*
3. *Arkansas*
4. *California*
5. *Georgia*
6. *Illinois*
7. *Indiana*
8. *Iowa*
9. *Kentucky*
10. *Louisiana*
11. *Michigan*
12. *Mississippi*
13. *Missouri*
14. *Nebraska*
15. *New Mexico*
16. *North Dakota*
17. *Oklahoma*
18. *Oregon*
19. *South Dakota*
20. *Texas*
21. *Utah*
22. *Washington State*
23. *Wyoming*

The degree of restrictiveness varies from state-to-state.

Many state laws exempt PSE pediatric products, liquid products, gel tabs and/or liqui-gels.

* *Sources: CHPA; Buzzeo PDMA; Covington & Burling*

Some States Have Passed Legislation That Restricts Consumer Access to OTC PSE Products: Schedule V and Behind-the-Counter Status

Schedule V

- Oklahoma has classified PSE as a Schedule V controlled substance. Under this law, products containing PSE can only be sold through a retail pharmacy as follows:
  - Must be housed behind a pharmacy counter and dispensed by a licensed pharmacist or pharmacy technician
  - Any person purchasing must produce a photo ID proving they are at least 18 years of age
  - Purchasers must sign a written log
  - No person shall purchase more than 9 grams of PSE in a 30 day period
  - Combination ingredient liquid products are exempt
- This law affects the following SPHCP products:
  - Claritin D 12 hr (all skus)
  - Claritin D 24 hr (all skus)
  - Drixoral Cold & Allergy (all skus)
  - Drixoral Allergy Sinus (all skus)
  - Drixoral Cold & Flu (all skus)
  - Drixoral Nasal Decongestant (all skus)
  - Coricidin-D
  - Chlor-Trimeton D 4 hr

Schedule V

- Arkansas has classified PSE as a Schedule V controlled substance. Under this law, products containing PSE can only be sold through a retail pharmacy as follows:
  - Must be housed behind a pharmacy counter and dispensed by a licensed pharmacist or pharmacy technician
  - Any person purchasing must produce a photo ID proving they are at least 18 years of age
  - Purchasers must sign a written log
  - No person shall purchase more than 9 grams of PSE in a 30 day period
  - No person shall possess more than 9 grams of PSE
- Product must be sold in blister packs of not more than 3 grams of PSE as calculated on the ***base***. Each blister cell can contain not more than 2 dosage units.
- Product cannot contain more than 96 tablets, gelcaps, or capsules per package.
- Liquid products, liquid capsules and liquid gel capsules are exempt.
- This law affects all SPHCP PSE products.

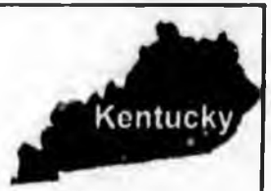
Schedule V

Effective 60 days from enactment or July 1 2005, whichever comes sooner.

- Iowa has classified PSE as a Schedule V controlled substance. Under this law, products containing PSE can be sold only through a retail pharmacy as follows:
  - Must be housed in a locked cabinet behind a pharmacy counter and dispensed by a licensed pharmacist or pharmacy technician
  - Consumer must produce a photo ID
  - Purchasers must sign a written log
  - No person shall purchase more than 7.5 grams of PSE in a 30 day period
- Liquid products, liquid capsules and gel capsules can be sold in stores that do not have pharmacies only if the following criteria all are met:
  - Package contains no more than 360 mg PSE (0.36 grams) ***AND***
  - Product is stored behind a counter or in a locked cabinet ***AND***
  - Only 0.36 grams of these products can be purchased in a 24-hour period
- This law affects all SPHCP PSE products.

Some States Have Passed Legislation That Restricts Consumer Access to OTC PSE Products: Schedule V and Behind-the-Counter Status

Schedule V



Effective 90 days after the General Assembly adjourns.
Estimated effective date: June 15, 2005

- Kentucky has classified PSE as a Schedule V controlled substance. Under this law, products containing PSE can only be sold through a retail pharmacy as follows:
  - Must be housed behind a pharmacy counter and dispensed by a licensed pharmacist or pharmacy technician
  - Any person purchasing a PSE product must produce a photo ID proving they are at least 18 years of age
  - Purchasers must sign a written log
  - No person shall purchase more than 9 grams of PSE in a 30 day period (no reference of base vs. salt)
- Transaction limit of 3 packages per transaction
- Liquids, liquid capsules, and gel capsules are exempt.

Modified Schedule V

Emergency Rule: October 14, 2004

- OR state legislature was not in session
- Governor directed the Board of Pharmacy to implement an "Emergency Rule"
- Single ingredient PSE products can be sold only from behind the pharmacy counter. They cannot be sold in stores that do not have a pharmacy.
- A variation on a true Schedule V: Combination PSE products can be sold only from behind a pharmacy counter, customer service counter, or other store counter where only store personnel have access to the product.
- Transaction limit of 9 grams (calculated on the salt)
- Certain liquid and pediatric products are exempt.
- Purchasers of these restricted products are required to show a photo identification. (School-issued IDs are unacceptable, since the new rule does not impose an age limit on these products.)
- Retailers were given 30 days in which to comply. If they are not in compliance, they will receive a warning notice and then must be in full compliance within 30 days from the date of the notice.
- The emergency rule will remain in effect for 180 days. During that time the Pharmacy Board intends to establish a stakeholder working group to develop the permanent rule

Some States Have Passed Legislation That Is More Restrictive Than Federal Regulations

- Prohibits the retail sale of any package that contains more than 3 grams of PSE
  - Washington: Calculated on the "salt" (sulfate) (PSE "salt" contains only about 70% of PSE "base")
  - North Dakota: Calculated on HCl
- SPHCP products affected:
  - Claritin D 12 hr 30ct
  - Claritin D 24 hr 15 ct
  - Drixoral Cold & Allergy 30ct
- In order to assist retailers in complying with the law, SPHCP does not ship these items to stores or distribution centers in North Dakota.
- Based upon an exemption granted in August 2004 by the Washington State Board of Pharmacy, SPHCP is able to ship these products to stores and distribution centers in Washington State.
- Washington
  - Limit of 3 packages per transaction
  - Certain pediatric products are exempt
- North Dakota
  - Limit of 2 packages per transaction
  - Age restriction of 18+
  - Liquid and pediatric products are exempt

Single Ingredient PSE

- Must be kept behind the counter ***or*** within 10 ft of check-out counter with an unobstructed view ***or*** under use of an anti-theft device (e.g. EAS tags)
- Transaction restriction of 2 pkgs or 6 gms (as calculated on the salt)

Combination Products

- Transaction limit of 3 pkgs or 9 grams of PSE (calculated on the "salt")
  - PSE "salt" contains only about 70% of PSE "base"
- Pediatric products are exempt
- This prohibits the sale of 3 or more packages of the following SPHCP products:
  - Claritin D 12 hr 30ct
  - Claritin D 24 15ct
  - Drixoral Cold & Allergy 30ct

***Note**: MS legislature is still in session as of 03/14/05. Legislation can still change during this session.*

Effective July 1, 2005:

All PSE Products

- 3 grams of PSE per package limit (calculated on the ***salt***)
- 2 packages or 6 grams per transaction limit
- 9 gram purchase and acquisition limit per 30-day period
- 24 gram possession limit (calculated on the ***salt***)
- Photo ID required for all PSE transactions (no age restriction cited)
- Law goes into effect July 1, 2005

Single Ingredient PSE Products

- Product must be kept behind-the-counter ***or*** in a locked display case so that the product is not accessible to consumers without employee assistance.

Combination Products

- Product can be merchandised on the retail shelves if it is placed within 30 feet of a cashier ***or*** if the product is under video surveillance
- If neither of the above criteria can be met, the product must be kept behind-the-counter ***or*** in a locked display case so that it is not accessible to consumers without employee assistance.

Some States Have Passed Legislation That Is More Restrictive Than Federal Regulations

Note: *SD legislature is still in session as of 03/14/05. Legislation can still change during this session.*

Effective July 1, 2005:

<u>All PSE Products</u>

- 2 package limit per transaction
- Retailer must post signs alerting consumers of this transaction limit
- Pre-empts all county and municipal ordinances that would attempt to enact more stringent provisions

<u>Single Ingredient PSE Products</u>

- Product can remain on the retail shelves only if it is displayed in conjunction with an anti-theft device system, such as EAS tags (Electronic Article Surveillance)
- In the absence of an anti-theft device system, the product must be shelved behind-the-counter ***or*** in a locked display case so that the product is not accessible to consumers without employee assistance.
- Pediatric, liquid, liquid cap, and gel cap single ingredient PSE products must be displayed in accordance with the combination product restrictions, outlined below.

<u>Combination PSE Products</u>

- Product can remain on the retail shelves if it is displayed in in conjunction with an anti-theft device system, such as EAS tags (Electronic Article Surveillance)
- In the absence of an anti-theft device system, the product must be within 20 feet and within an unobstructed view of an employee-manned counter.

- Legislation passed Aug 24, 2004
- Single ingredient PSE products must be kept behind the counter or in a locked case.
- 3-gram limit of PSE per package (calculated on the ***salt***). SPHCP products affected:
  - Claritin D 12 hr 30ct
  - Claritin D 24 hr 15 ct
  - Drixoral Cold & Allergy 30ct
- 2 package limit of all products containing pseudoephedrine
- Includes additional retail merchandising restrictions. To maintain consumer access to combo products at shelf, retailers must choose 2 of the following. The first option must be implemented by 1/1/05, the second option by 7/1/05:

- EAS tagged product
  - If a retailer chooses this as the first option for implementation, they must ensure that 50% of all PSE units are tagged by 1/1/05, and that 100% of PSE units are tagged by 7/1/05
- Merchandise PSE combo products within 30 feet and in direct line of sight of a cash register or store counter staffed by one or more employees
- Provide 24-hour video surveillance
- Implement shelving units that allow only 1 package to be removed at a time, with a 15- second delay between packages

- Liquid PSE products are exempt

Effective July 1, 2005:

<u>All Non-Liquid PSE Products</u>

- Prohibits the retail sale of any package that contains more than 3 grams of PSE base
- Solid dosage form product must be sold in blister packs.
- Powder must be sold in unit dose packets or pouches.

<u>Retail Merchandising Restrictions</u>

Product can remain on the retails shelves if one of the following provisions is met:

- Product must be displayed within 30 feet of a staffed check-out ***and*** the store must employ a reliable alarm system to prevent theft (e.g. EAS tags) ***OR***
- The product must be merchandised in an area that is monitored by a constant video surveillance system.
- If neither of the above criteria can be met, product must be shelved behind-the-counter ***or*** in a locked display case so that the product is not accessible to consumers without employee assistance.

Some States Have Passed Legislation That Is More Restrictive Than Federal Regulations

- Legislation passed May, 2004
- Single ingredient products that contain 60 mg or more of PSE per tablet must be kept behind the pharmacy or customer service counter.
- 3 pkg limit on all products that contain PSE.
- 9 gram transaction limit. There is no reference to the basis of the 9 gram calculation (i.e. base vs. salt).
- Pediatric products are exempt.

- Transaction limit of 2 blister packages (up to 6 grams of PSE) per transaction. Does not specify base vs. salt.
- Retailers cannot "knowingly or intentionally sell" more than 6 grams of PSE to the same individual within a 7-day period.
- Products must be placed in direct sight of store personnel and not more than 20 feet away from a cash register.
- Retailers must develop and implement a training program to be read and signed by all store personnel.
- All manufacturers, wholesalers, and retailers not currently licensed by the Board of Pharmacy must obtain a precursor license to sell PSE products.
- The regulations were published in the December 30,2004 issue of the "New Mexico Register".

Some States Have Passed Legislation That Differs From Federal Regulations

- Transaction limit of 24 grams/transaction (Does not specify calculation on base vs. salt)
- Illegal to possess> 24 grams (Does not specify calculation on base vs. salt)

- Transaction limit of 3 pkgs and 9 grams
- Does not specify base vs. salt in calculation
- Pediatric products are exempt from the 9 gram transactional limit

Some States Have Passed Possession Restrictions But Not Transaction Restrictions

- Georgia: Possession limit of 9 grams (calculated on salts and isomers) ***or*** 300 tablets
- Indiana : Possession limit of 10 grams (calculated on salts and isomers)
- Louisiana: Possession limit of 12 grams (calculated on salts and isomers)
  Certain pediatric products are exempt
- Michigan: Possession limit of 12 grams (no reference to base vs. salts and isomers)
  Pediatric products are exempt
- Nebraska: Possession with the intent to manufacture methamphetamine is prohibited
  Sale or distribution of PSE with knowledge that it will be used for meth production is prohibited
- Texas: Possession limit of 9 grams (no reference to calculation on base vs. salt) ***or*** 3 pkgs ***or*** 300 tablets.
  Applies only to possession in conjunction with possession of other specifically listed chemicals such as anhydrous ammonia.
- Utah: Possession limit of 12 grams (calculated on salts and isomers)

Schering-Plough's Position on Effective Legislation Regarding PSE

Schering-Plough's Position on Effective Legislation

Schering-Plough and the member companies of CHPA advocate a comprehensive approach to combating the methamphetamine problem:

- *Support federal preemption bill which includes "safe harbor packaging" that places a 3 gram limit of PSE base per package. (All SGP products are in compliance with this federal provision.)*

- *Implement MethWatch to curtail the sale of PSE for illicit use*

- *Place retail sales limits on methamphetamine precursors*
  - *2 package / 6 gram sales limit of base PSE per transaction*

- *Increase criminal penalties for those producing and selling methamphetamines*

Schering-Plough's Position on Effective Legislation (continued...)

- *Provide grants at the local level to fund environmental clean-up associated with meth labs*

- *Provide grants for education, prevention, and treatment of methamphetamine abuse.*

  - *CHPA and The Partnership for a Drug Free America (PDFA) have launched two successful pilot programs in St. Louis and Phoenix.*

- *Enact stronger laws protecting drug-endangered children.*

- *Provide federal funding for DEA enforcement of methamphetamine laws. Increase funding for law enforcement efforts through the Office of National Drug Control Policy (ONDCP) Youth Anti-Drug media campaign.*

A Case Study in Success: MethWatch

A Case Study in Success: MethWatch

Kansas retailers have partnered with law enforcement to implement a multi-pronged program called "MethWatch," which reportedly has resulted in a significant reduction in meth lab seizures since its implementation in mid-2001. SPCHC supports CHPA's efforts to extend this program nationally.

Program Elements

- *Product is placed in consistently staffed areas*
  - *in view of customer service counter*
  - *in view of pharmacy*
  - *at check-out counter*
  - *in aisles with video surveillance*
  - *at end of aisle in high-traffic area*
- *Limit number of packages on shelf*
- *Use MethWatch shelf tags, door decals, cash register decals*
- *Limit number of packages per purchase*

A Case Study in Success: MethWatch

Additional Retailer Involvement

- *Report suspicious transactions to law enforcement*
- *Educate consumers by providing them with MethWatch information*
- *Train employees to administer the program*

Key Benefits to Retailers

- *Safer stores*
- *Better consumer relations*
- *Reduced theft*
- *Increased employee awareness*
- *Better relations with local law enforcement*
- *Unifying communities in working towards reducing drug abuse*

Metrics

- *Major KS retailer adopted MethWatch and reportedly saw > 85% theft reduction.*
- *Meth lab seizures reportedly have decreased by 23% since 2001.*
- *WA state reports 50% reduction of meth busts since MethWatch.*

Q & A

Q & A

What is the status of legislation in the 30 states not covered in this presentation?

To our knowledge, there are no enacted state laws in these states which restrict the otherwise legitimate retail sale of PSE-containing products. There may be localities within a state that have enacted restrictive ordinances or there may be pending bills or regulation but we do not cover these, if any in this document.

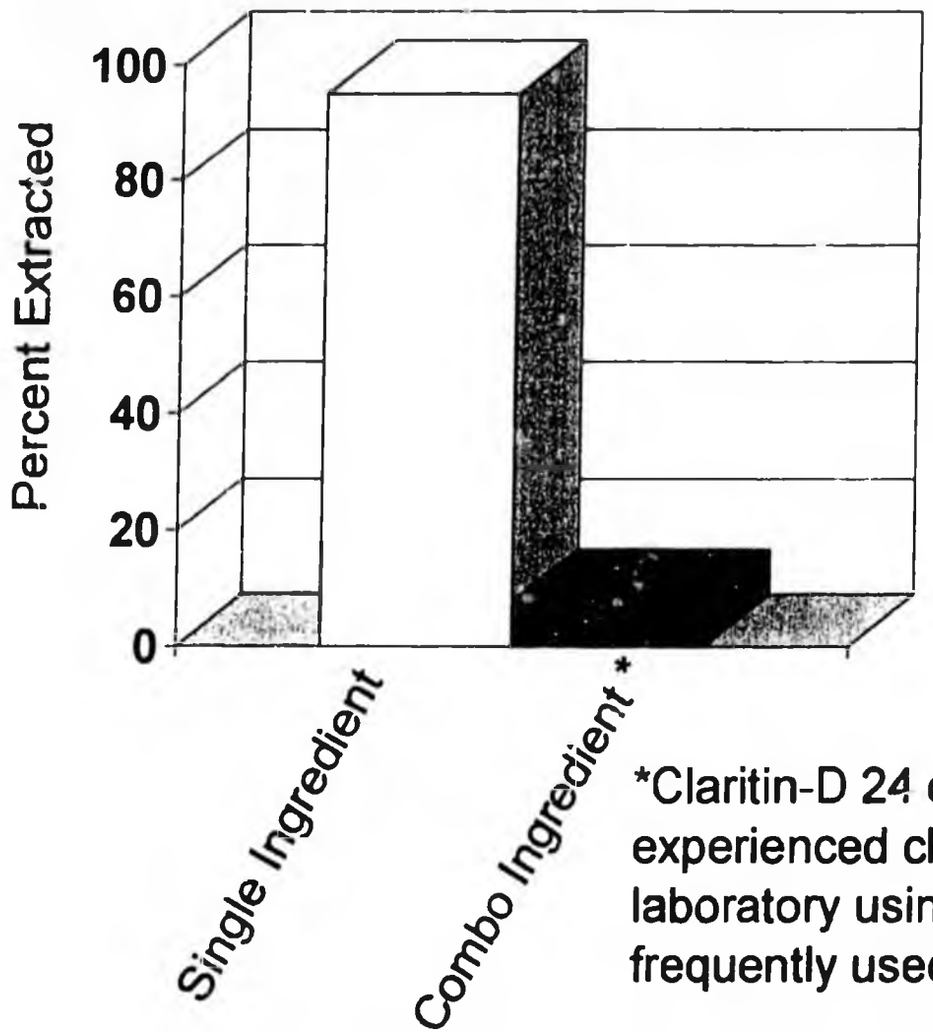
Are there plans to reformulate Schering-Plough products which contain PSE?

We do not share or comment on our future product plans.

Will Schering-Plough accept returns of its products containing PSE from customers?

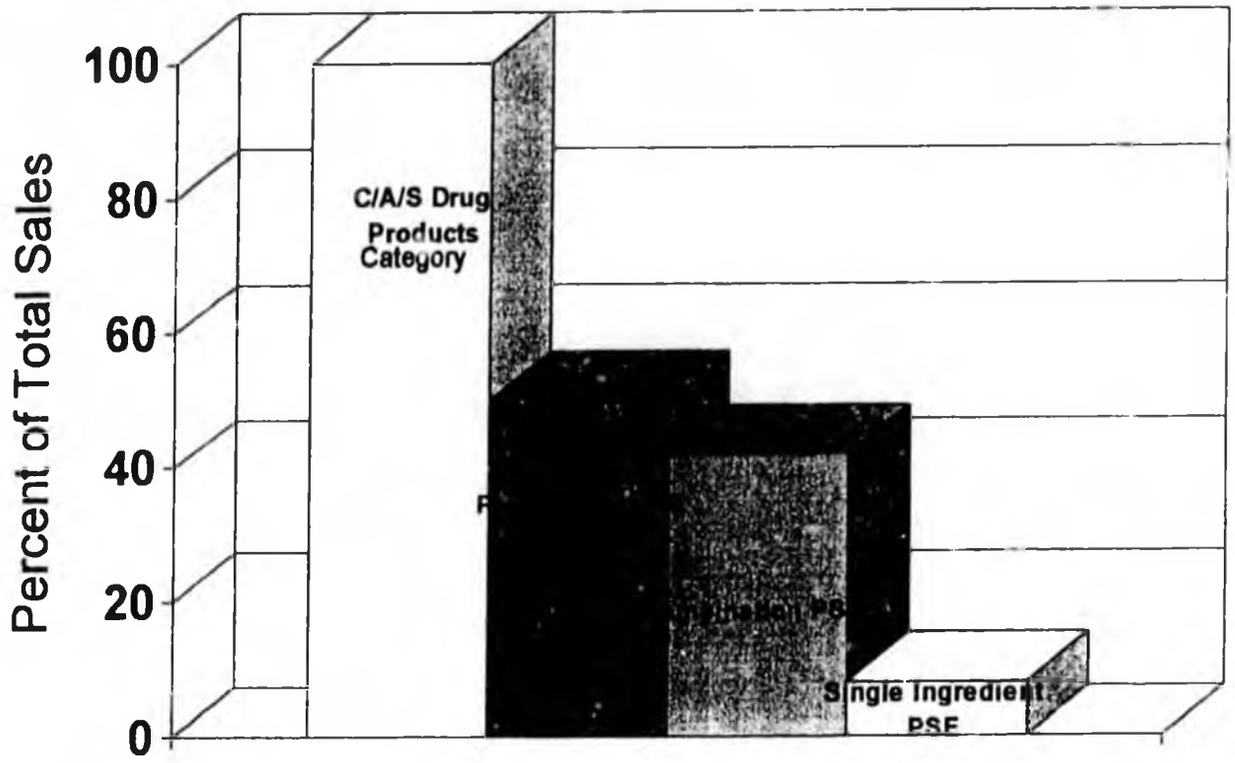
Our sales representatives will work with customers impacted by state regulations to effectively manage inventory on SPHCP products containing PSE. Refer to the SPHCP return goods policy. Any product requires an approved return goods authorization prior to being returned. Specific questions can be directed to the SPHCP Customer Support Department at 1-800-898-8326.

Extraction from Combination Tablets Yields Far Lower Levels of Pseudoephedrine than Single Ingredient Products



*Claritin-D 24 extracted by an experienced chemist in a pharmaceutical laboratory using the "UncleFester" method frequently used by meth cooks

Single Ingredient Pseudoephedrine Products are Small Part of Cold/Allergy/Sinus OTC Market but Are Predominant Products Found in Meth Labs



IRI Market Information, January 2005

Combination Pseudoephedrine Products are **not** found in Meth Lab Seizures*

- Eight states thoroughly investigated
  - AZ, CA, GA, IL, NY, OK, TN, TX
- Interviews with local, state, and federal law enforcement officials
- Findings
  - Single ingredient pseudoephedrine products predominantly found in meth labs
  - Combination products in general not found and no Claritin-D products found

*Investigation conducted by national DEA Investigative consulting firm, February 2005

House Bill 272 impacts the following products by requiring that they be placed behind the pharmacy counter. Customers would be required to sign a log and show identification in order to purchase these products:

Single-entity PSE products
(Note: Some products are examples of store brand)

Suphedrine MX Strength
Sudafed Tablets 30 MG
Suphedrine Decongenstant
Sudafed 12 Hour
Sudafed 12 Hour Caplets
Suphedrine
Suphedrine 12 Hour Caplets
Sudafed 24 Hour
Suphedrine 12 Hour Caplets
Contac 12 Hour Cold Caplets
Contac 12 Hour Caplets
Cold Caps 12 Hour

Single-entity PSE products – Liquid and Gel Tabs
(Note: Some products are examples of store brand)

Pedia Care Infant Drops
Sudafed Children's Decongestant
Dimetapp 12 Hour Non-Drowsy
Childrens Suphedrine Grape
Sudafed Nasal Decongestant Childrens
Elixsure Children's Decongestant

Mulitple/ Compound PSE Products
(NOTE: Products listed more than once indicate varying formulations; Some products are examples of store brands)

Alka Seltezer Plus Cold Tabs
Claritin D Allergy Tabs (X 3 strengths)
Nyquil Cold Medicine (capsules, gelcaps, liquid)
ND Allergy Congestant
Advil Cold and Sinus
Tylenol Cold Severe Congestion
Aphedrid Tabs
Theraflu Max Strength Nighttime
ND Allergy Congestion Tab 24 Hour
Tylenol Flu Gelcaps
Aphedrid Cold & Allergy Tab
Tylenol Cold ND MS
Theraflu Max Strength Packets
Theraflu Nighttime Flu
Drixoral Cold & Allergy
Advil Cold and Sinus
Tylenol Cold MS Caplet
Aleve Cold and Sinus
Suphedrine MS Tablets
Sudafed Non Drying Sinus
ND Allergy Congestion Tab 24 Hour
Actifed Tablets
Contac Day & Night Cold & Flu
Theraflu Flu Cold & Cough
Flu Cold & Cough Nite Time
Tylenol Sinus ND Severe Congestion
Theraflu Non-Drowsy Flu & Congestion
Sudafed Sinus
Theraflu
Tylenol Allergy Sinus
Alavert Allergy Sinus
Coricidin D Tablet
Tylenol Cold ND Caplet
Alavert Allergy
Tylenol Max STR Sinus
Suphedrine ND Liquid Sinus Caps
Theraflu Cold & Sore Throat
Theraflu Nite Time Flu & Cough
Primatene
Advil Flu & Body Ache
Sudafed Sever Cold & Flu
Benadryl Allergy Sinus Headache
P RLVR Allergy Sinus Max

Attachment A.

Tylenol MS St Sinus
Benadryl D Allergy Sinus FSTMLT
Tylenol Allergy Sinus
Contac Severe Max STR Cold & Flu
Contac Severe Cold Max Strength
Suphedrine MS Sin Caps
Pain Reliever Sinus Caps
Alka Seltzer Plus Cold & Cough
Tylenol Sinus ND MS
MS Flu Cold & Cough ND
Profen IB Cold Sinus CPLT
Motrin Cold & Sinus
Sudafed Sinus Nighttime Max STR
Aleve Sinus & Headache
Benadryl Cold Caplets
Pain Reliever Cold Severe Caps
Comtrex Non-Drowsy Cold & Cough
Benadryl D Allergy Sinus
Flu Cold & Cough Original
Benadryl Severe Allergy & Sinus Headache
Pain Relief Sinus Allergy Caps
Tylenol Child Cold & Cough Chew
Suphedrine MS Cough & Cold
Tylenol Sinus
Triaminic Soft Chew Cold & Cough
Tylenol Max STR Sinus
Sudafed Sinus Nighttime
Tylenol Allergy Sinus
Sudafed Sinus & Cold Liquid Caps
Sudafed Sinus Tablets
Theraflu Severe Cold & Congestion NT
Theraflu Caplets
Child Aspirin FR Cold & Cough
Sudafed Severe Cold & Flu
Alka Seltzer Plus Cold
Contac Severe Cold & Flu Caplets
Tylenol M S Sinus
Advil Cold & Sinus
Sudafed Severe Cold & Flu
Tric Nite Time Max Strength
Tylenol Allergy Sinus DN MS
Sudafed Max Strength Sinus
Tylenol Allergy Sinus
Suphedrine Cold Allergy
Allerest Tablets Max Strength
Benadryl Allergy Sinus Headache
Suphedrine Severe Cold Caplets
Primatene
Tylenol Allergy Sinus
Suphedrine MS Sinus Tabs
Alka Seltzer Plus Nighttime
Triaminic Softchew Throat & Cough
Advil Allergy Sinus
Severe Cold and Flu Caplets
Comtrex Nighttime Cold & Cough
Sinutab Max Strength Non-Drowsy
Comtrex Deep Chest Cold
Advil Allergy Sinus
Comtrex Day & Nite Cold & Flu Therapy
Diph Headache Allergy Sinus CP
Profen IB Cold & Sinus CPLT
Tavist Allergy Sinus Headache
Suphedrine Severe Cold MS Capsules
Triacting MS Cough & Cold Cherry
Pain Reliever Cold COM MS Capsules
Tylenol Sinus Nite & Day Severe Congestion
Sinus Caplets Non-Drowsy
Pain Relief ND Multi Caplets
Triacting MS Chest Congestion
Claritin D 24 Hour Allergy
Claritin D 12 Hour Allergy
NA Flu Day & Night Combo
NA Cold Day & Night Combo
Sinus Day & Night Caplet
Tylenol Cold Severe Congestion
Vicks Baby Rub
Advil Multi Symptom Cold
Advil Multi-Symptom Cold
Triacting MS Cold & Allergy

Multiple/ Compound PSE Products – Liquid and Gel Tabs
(NOTE: Products listed more than once indicate varying formulations; Some products are examples of store brands)

Robitussin Cough Syrup (X 4 strengths/ flavors)
Dayquil Liquicaps
Tylenol Infant Cold Drops
Children's Tylenol Cold Cough
Vicks Dayquil
Pediacare Decongestant Plus Cough
Dayquil Liquid
Tylenol Flu MS Day/ Night
Children's Motrin Cold
Nighttime Liquid Cherry
Nighttime Liquid Original
Dimetapp DM Elixir
Dimetapp Decongestant Cough Infant Drops
Tussin CF
Tylenol Cold ND Geltabs
Daytime Liquid Caps
Robitussin Flu
Nighttime Liquid Original
Robitussin Pedia Cough & Cold
Tylenol Childrens Flu Formula
Nighttime Liquid Cherry
Pedia Care Cough & Cold
Robitussin Cough & Cold
Tylenol Flu Night Time
Tylenol Infant Cold Decongestant Drops
Advil Cold and Sinus
Nighttime Liquid Caps
Vicks Dayquil/ Nyquil Liquicaps
Sudafed Cold & Cough Liquid Caps
Dimetapp Elixir
Vicks Formula 44E
Vicks Dayquil ND Cold Flu
Robitussin PE
Vicks Formula 44M
Vicks Children's Nyquil Cold & Cough
Children's Tylenol Cold Nighttime
Dimetapp Cough Plus Cold
Robitussin Cough, Cold & Flu
Robitussin Allergy & Cough
ND Day Time Liquid
Robitussin Cold Severe Congestion
Vicks Nyquil Cold & Flu
Sudafed Cold & Cough Liquid Caps
Nyquil Original Twin Pack
Dimetapp Nighttime Flu
Vicks Formula 44D
Childrens Advil Cold
Children's Benadryl Allergy Cold
Robitussin PM Cough and Cold
Robitussin Pediatric Night
Children's Motrin Cold Dye Free
Nyquil Twin Pack Cherry
Robitussin Syrup PE
Benadryl D Allergy Sinus Liquid
Robitussin Maximum Strength
Pediacare Nite Rest
Nighttime Original
Vicks Formula 44M
Tussin MS Cough & Cold EXL
Sinus Pain Relief Gelcaps
Pediacare Cough Plus Cold
Tussin Pediatric
Sudafed Children Cold & Cough
Infant Cold Drops Cherry
Dibromm Elixir Grape
Dibromm DM Elixir Grape
Robitussin
Dimetapp Pediatric
Vicks Pediatric Formula 44E
Dibromm Elixir Grape
Triacting Sorethroat Grape
Robitussin Cough & Cold
Childs Cold Liquid Grape
Daytime Cold & Flu Softgels
Sinus Max Strength Geltabs NA
Vicks Dayquil Twin
Night Time Cold & Flu Softgels
Pediatric Relief Infant Drops
Childrens Pain Reliever Flu
Suphedrine Cough & Cold Liquid Gel
Children's Tylenol Cold
Ibuprofen Cold Suspension
Dayquil Sinus Liquicaps
Dimetapp Cold & Fever
Children's Advil Allergy Sinus
Tylenol Cold & Flu Daytime
Dimetapp Elixir

SAFEWAY INC.

CHER GOTTSTEIN FOODS CO.

6401 A Street
Anchorage Alaska 99518

Voice: (907)339-7704

Fax: (907)339-7793

FAX

TO: Senator Seekins

FROM: Glenn Peterson

DATE: April 26th

Number of pages including cover sheet 4

Remarks: Urgent For your review Reply ASAP Please Comment

ALASKA STATE LEGISLATURE
SENATOR GRETCHEN GUESS

Sponsor Statement

Senate Bill 149:

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

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

The following are the provisions of the bill.

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

Thank you for your consideration.

January-May: State Capitol • Juneau, AK 99801-1182 • (907) 465-2435 • Fax (907) 465-6615
June-December: 716 W. 4th Avenue • Anchorage, AK 99501• (907) 269-0120• Fax (907) 269-0122
Email: Senator_Gretchen_Guess@legis.state.ak.us Website: www.GretchenGuess.com

24-LS0809\Y.2
Bannister
4/18/05

AMENDMENT

OFFERED IN THE SENATE BY SENATOR GUESS

TO: SSSB 149

Page 5, line 1:

Delete "or (2)"

Page 5, lines 1 - 2:

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

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

Page 5, lines 28 - 29:

Delete "within three business days after receiving the request"

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

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

Delete "within three business days"

Insert "immediately"

Page 8, line 18 - 19:

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

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

LEGAL SERVICES

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

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

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

MEMORANDUM April 19, 2005

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

TO: Senator Gretchen Guess
Attn: Meagan

FROM: Theresa Bannister
Legislative Counsel

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

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

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

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

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

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

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

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

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

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

Sec. 45.48.090 defines terms for Article 1.

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

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

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

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

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

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

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

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

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

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

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

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

Sec. 45.48.210 establishes certain exemptions for Article 2.

Sec. 45.48.220 defines terms for Article 2.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Sec. 45.48.590 defines terms for Article 5.

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

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

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

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

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

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

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

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

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

Sec. 45.48.690 defines terms for Article 6.

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

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

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

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

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

Sec. 45.48.990 defines terms for this chapter.

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

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

Section 3. Adds a transition provision for Article 4.

If I may be of further assistance, please advise.

TLB:med
05-272.med

FISCAL NOTE

STATE OF ALASKA
2005 LEGISLATIVE SESSION

Fiscal Note Number: 1
Bill Version: CSSSSB 149(L&C)
(S) Publish Date: 4/22/05

Revision Date/Time (Note if correction):
Dept. Affected: LAW
Title "An Act relating to breaches of security involving personal information; and relating to consumer report..."
RDU CIVIL
Component Commercial & Fair Business
Sponsor Senator Guess
Requester Senate Labor and Commerce
Component No.

Expenditures/Revenues (Thousands of Dollars)

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

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

FUND SOURCE (Thousands of Dollars)

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

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

POSITIONS

Full-time						
Part-time						
Temporary						

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

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

Article 2 ads a section that allows consumers to place a security freeze on his or her credit report. When a security freeze is in place, a credit reporting agency may not release information from the consumer's credit report to third parties unless requested by the consumer. There are several exemptions for access required to correct technical information, and for some agencies like the child

Prepared by: Kathryn Daughhetee, Director
Phone 465-3673
Division Administrative Services Division
Date/Time 4/9/05 2:53 PM
Approved by: Kathryn Daughhetee for David Márquez, Attorney General
Date 4/9/2005
Agency Department of Law

STATE OF ALASKA
2005 LEGISLATIVE SESSION

BILL NO. CSSSSB 149(L&C)

ANALYSIS CONTINUATION

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

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

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

FISCAL NOTE

STATE OF ALASKA
2005 LEGISLATIVE SESSION

Fiscal Note Number: 2
Bill Version: CSSSSB 149(L&C)
(S) Publish Date: 4/22/05

Revision Date/Time (Note if correction):
Dept. Affected: Commerce
Title: Protection of Personal Information
RDU: Executive Admin and Dev (119)
Component: Administrative Services
Sponsor: Guess
Requester: Labor & Commerce
Component No.: 1028

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 1156 - Receipt Supported Services						
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 20(budget proposal:

POSITIONS

Full-time						
Part-time						
Temporary						

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

SSSB 149 establishes requirements to deal with personal information on information systems if a breach of security should occur. This indeterminate fiscal note is submitted because financial impact to the department would occur only if and when a breach occurs. There are approximately 500,000 records in the department's automated systems that store personal information such as: social security numbers, date of birth, etc. For example, there are approximately 126,000 professional licensing records; 175,000 business licensing records; 2,000 investment accounts, and more. Under this bill, all individuals in our information systems would need to be notified if a breach occurs. Additionally, business practices would be changed concerning collection, storage, and transmitting of personal information (relating to the use of SSNs). Significant costs may be generated by adding new security measures to our automated systems. Business practices relating to information collected, stored, and transmitted on paper will also be affected.

Prepared by: JoEllen Hanrahan, Director
Phone: (907) 465-2505
Division: Administrative Services
Date/Time: 4/21/05 12:14 PM
Approved by: Edgar Blatchford, Commissioner
Date: 4/21/2005
Agency: Commerce, Community, and Economic Development

Consumers Union

Publisher of Consumer Reports

Freeze Identity Thieves Out of Consumers' Credit Files:

Support State Credit Report Security Freeze Laws

Credit card companies, merchants, credit bureaus and other businesses do not adequately safeguard consumers' private financial information, making it relatively easy for thieves to steal this data and use it to take out new credit or to rack up charges on existing accounts. As a result, identity theft is one of the fastest growing financial crimes. Nearly 10 million Americans fall victim each year, and the Identity Theft Resource Center reports that victims spend an average of $1,495 and 600 hours to restore their credit histories and their good names. Identity theft also costs U.S. businesses nearly $48 billion annually.

Consumers need additional tools to help prevent identity theft before it happens. Many states are considering legislation that would allow people to lock identity thieves out of their credit files with a security freeze. With a security freeze in place, a consumer's credit report and credit score cannot be shared with any potential creditors unless the consumer decides to unlock the files by contacting the credit bureaus and providing a security code.

A security freeze can help prevent identity theft. Most businesses will not issue new credit or loans to an individual without first reviewing his or her credit report or credit score. If an individual's credit file is frozen and an imposter applies for credit in that individual's name, a creditor likely would deny the imposter's application, preventing an instance of identity theft. In addition, if a request for credit is made on a frozen account, then the credit bureau would be required to notify the consumer about the attempted fraud.

Under a state security freeze law, people who choose to freeze access to their credit report may temporarily lift the freeze for new loans and credit they apply for themselves. When a consumer initially activates the freeze, the credit bureau will issue a unique PIN to the consumer that can be used to "thaw" or lift the security freeze for a particular creditor. Credit bureaus must release the report within three business days of such a request, and are permitted and encouraged to develop faster methods of releasing credit reports on request of the consumer. In addition, existing creditors will continue to have access to an individual's credit report.

State security freeze laws would give consumers the right to decide for themselves whether or not to place a security freeze on their reports.

Frequently Asked Questions

How is a security freeze different from fraud alerts or blocking of information generated by a thief?

A security freeze is a mechanism to prevent identity theft. Only a security freeze allows the consumer to control who has access to his or her credit file. The federal Fair Credit Reporting Act allows identity theft victims to block the reporting of specific information in their credit reports that is the result of identity theft. But fraud blocking is a way to begin to undo damage after it has been done. Fraud blocking does not prevent identity theft. Fraud blocking does not prevent the release of a credit report; it only limits certain fraud-related information from being included in the report after the consumer discovers that information. Similarly, a fraud alert does not prevent a credit report from being issued. Under the federal Fair Credit Reporting Act, when a fraud alert is attached to a credit file, creditors must take additional steps to verify a credit applicant's identity before extending credit. The fraud alert, however, does not prevent the potential creditor from seeing the report, and it does not prevent the credit bureau from selling or sharing the credit report.

A security freeze grants each consumer the right to prevent the credit bureau from issuing his or her credit report for the purpose of issuing new credit. It freezes access to the report except for circumstances such as review of existing accounts, other limited purposes, or the express permission of the consumer.

Would anyone have access to a consumer's credit file if it is frozen?

Yes, these proposed state bills include a few necessary exemptions to the freeze. Security freezes 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, such as law enforcement agencies and certain governmental agencies that need them for investigations and other statutory responsibilities.

Do states have the right to enact security freeze legislation under federal law?

A state law establishing a security freeze right should not be preempted by the federal Fair Credit Reporting Act. No provision of federal law preempts the ability of a state to restrict when a credit reporting agency allows access to a credit report. Federal law addresses the contents of credit files, not who can see them. Federal law also requires credit bureaus, upon the request of a consumer to: (1) 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) block the reporting of any information in a consumer's file that the consumer identifies as information resulting from an identity theft. States are preempted from imposing requirements regarding the same conduct required by certain specific provisions of federal law, such as these provisions. States are not preempted from other steps to prevent or mitigate identity theft. States should be free to enact security freeze legislation.

Which states already have security freezes?

California, Louisiana, Texas, and Vermont have security freeze laws, the Texas and Vermont statutes are limited to victims of identity theft. The California and Louisiana laws allow consumers who have not been victims of identity theft to control who gets access to their credit files for credit granting purposes.

G:\Groups\Credit & Finance\Gail\Wallet\2005\Security Freeze Factsheetwlogo.doc

IDENTITY THEFT FACT SHEET

Source: FTC's NCPW 2005. Quiz – Identity Theft: When Fact Becomes Fiction

1. ID theft is the fastest growing white-collar crime in the U.S. 27 million Americans have been victims of the crime in the past five years, nearly 10 million people last year.
2. Identity thieves can get personal information from you by:
   - Stealing your wallet or purse
   - Stealing your mail
   - Rummaging through your trash, and
   - Using personal information they find on the Internet about you.

   For additional information on how ID thieves can steal your identity, go to: www.consumer.gov/idtheft/understanding_idt.html#2.
3. If you are getting rid of your computer, it is not enough to delete files using mouse and keyboard commands. Use a "wipe" utility program to overwrite the entire hard drive. This makes files unrecoverable
4. ID thieves that obtain your personal information can: (1) call your credit card issuer and change the mailing address on your card; (b) open a new credit card account or bank account in your name; (c) file for bankruptcy under your name to avoid paying off debts they've incurred; and (d) counterfeit checks or drain your bank account.
5. Here are some ways for you to minimize your risk of becoming a victim of ID theft::
   - Don't give out personal information by email, Internet, phone or mail unless you initiated contact and you are certain you know who you are dealing with
   - Don't carry your social security card with you
   - Carry only the identification information and credit/debit cards that you actually need
   - Password protect your credit card, bank and phone accounts.
   - For additional tips, go to: www.consumer.gov/idtheft/protect_against_idt.html#5.
6. If you are a victim of ID theft, place a fraud alert on your credit report. This will help prevent If thieves from opening additional accounts in your name.
7. If you think someone has stolen your personal information or identification, do the following:
   - Immediately close all your credit card or bank accounts
   - Place a fraud alert with any one of the three national consumer reporting companies
   - Contact the Social Security Administration to get a new Social Security number
   - Alert issuing agencies for your driver's license and other identification documents
8. If you have high speed Internet connection, such as DSL or cable modem, get a firewall program to prevent uninvited guests from accessing your computer.
9. Signs you could be a victim of ID theft:
   - Fail to receive bills or other mail
   - Receive credit cards for which you did not apply
   - Are denied credit for no apparent reason
   - Get calls or letters from debt collectors or businesses about merchandise or services you didn't buy
10. Don't tape computer and website passwords to your computer. Safeguard these passwords. Also, when creating passwords, use a combination of letters (upper and lower case), numbers and symbols.

IDENTITY THEFT IN ALASKA

Source: FTC's Consumer Sentinel Complaint Statistics and Trends for Alaska, for the periods January 1 – December 31, 2004, (pg. 17 of 66) & January 1 – December 31, 2003 (pg. 17 of 66)
http://www.consumer.gov/sentinel/pubs/Top10Fraud2004.pdf

Fraud complaints from Alaska consumers:

- 1,143 in 2004
- 1,165 in 2003

Identity theft complaints from Alaska victims:

- 433 in 2004
- 231 in 2003

Ranking ID theft by category from Alaska victims in 2004 – Identity Theft Complaints from Alaska Victims = 433

Rank	Type	# of Victims	Percentage*
1	Credit card fraud	127	29%
2	Phone or utilities fraud	78	18%
3	Bank fraud**	59	14%
4	Gov't documents or benefits fraud	33	8%
5	Employment-related fraud	30	7%
6	Loan fraud	18	4%
	Other	129	30%
	Attempted ID theft	31	7%

* Percentages are based on 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.

** Includes fraud involving checking and savings accounts and electronic fund transfers.

Ranking ID theft by category from Alaska victims in 2003 – Identity Theft Complaints from Alaska Victims = 231

Rank	Type	# of Victims	Percentage*
1	Credit card fraud	80	35%
2	Phone or utilities fraud	35	15%
3	Bank fraud**	32	14%
4	Employment-related fraud	23	10%
5	Gov't documents or benefits fraud	17	7%
6	Loan fraud	15	6%
	Other	64	28%
	Attempted ID theft	18	8%

* Percentages are based on 231 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.

** Includes fraud involving checking and savings accounts and electronic fund transfers.

IDENTITY THEFT
Data Clearinghouse

Identity Theft Victim Complaint Data

Figures and Trends In Alaska

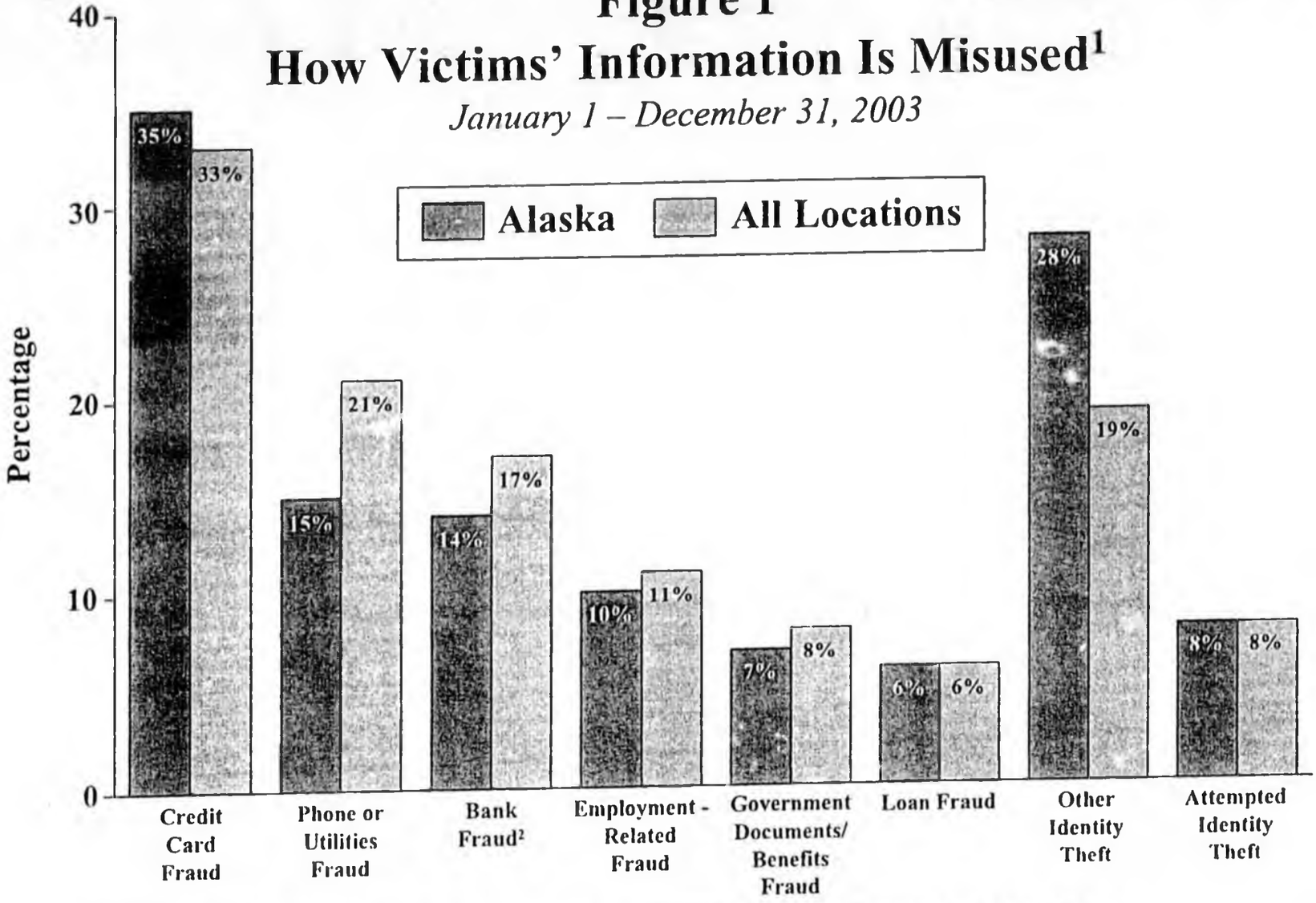
January 1- December 31, 2003

Federal Trade Commission
Washington, DC

IDENTITY THEFT Data Clearinghouse

Figure 1
How Victims' Information Is Misused[1]

January 1 – December 31, 2003



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

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

Federal Trade Commission
Created January 22, 2004

Figure 2

IDENTITY THEFT Data Clearinghouse

How Victims' Information Is Misused[1]

January 1 – December 31, 2003

Total Number of Identity Theft Victims:
Alaska = 231
All Locations = 214,905

Credit Card Fraud

Theft Subtypes	*Alaska*	*All Locations*
New Accounts	19.0%	19.2%
Existing Accounts	14.3	12.0
Unspecified	1.3	1.4
Total	35%	33%

Phone or Utilities Fraud

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

Bank Fraud[2]

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

Employment-Related Fraud

Theft Subtype	*Alaska*	*All Locations*
Employment-Related Fraud	10.0%	11.1%

Government Documents or Benefits Fraud

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

Loan Fraud

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

Other Identity Theft

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

Attempted Identity Theft

Theft Subtype	*Alaska*	*All Locations*
Attempted Identity Theft	7.8%	8.0%

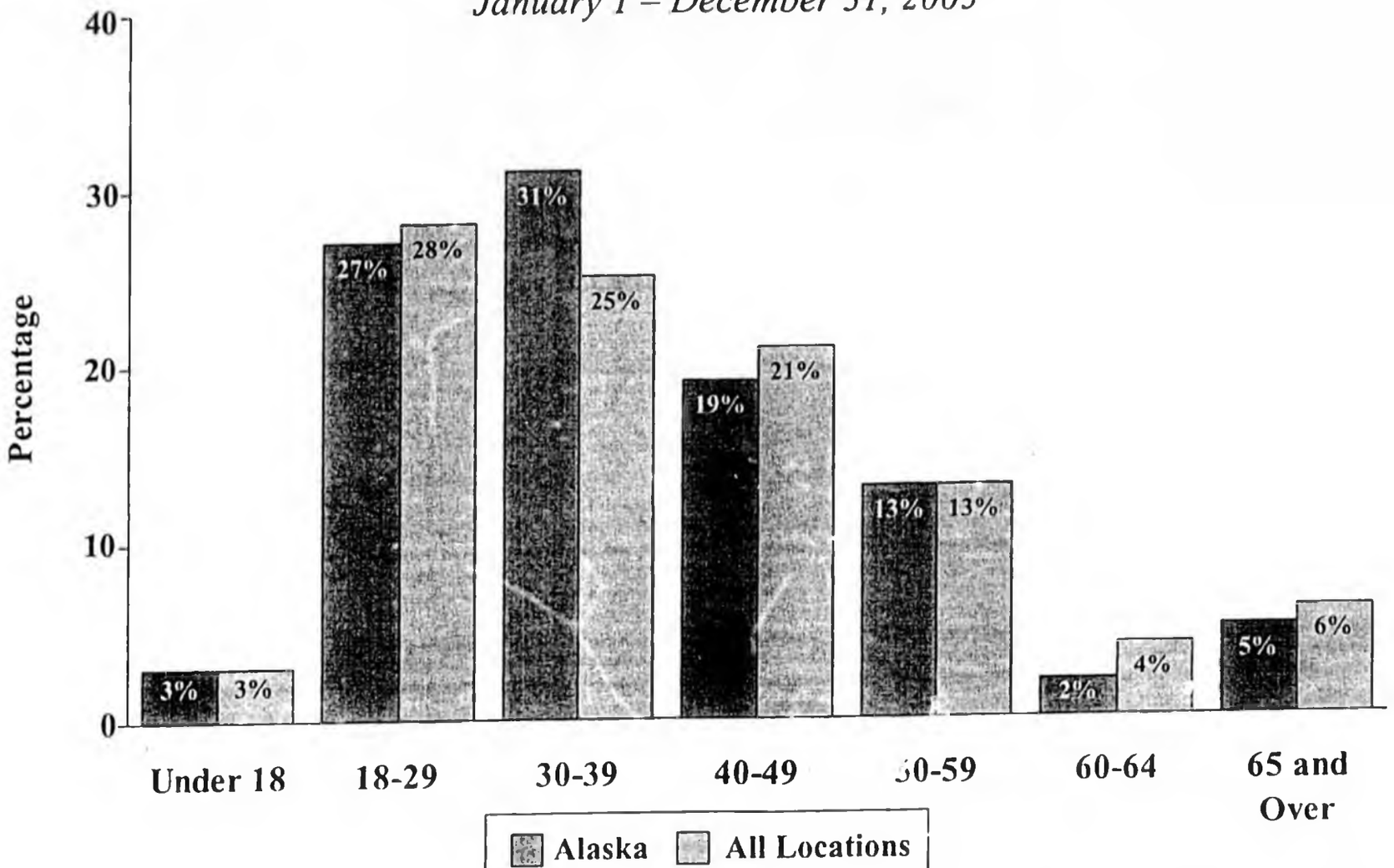
[1]Percentages are based on the total number of victims reporting: 231 from Alaska and 214,905 from all locations. Percentages add to more than 100 because approximately 17% of victims from Alaska and 19% of victims from all locations reported experiencing more than one type of identity theft. All victims reported experiencing at least one type of identity theft.
[2]Includes fraud involving checking and saving accounts and electronic fund transfers.

Federal Trade Commission
Created January 22, 2004

IDENTITY THEFT
Data Clearinghouse

Figure 3
Complaints by Victim Age[1]

January 1 – December 31, 2003



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

Federal Trade Commission
Created January 22, 2004

Figure 4a

IDENTITY THEFT Data Clearinghouse

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

January 1 – December 31, 2003

Rank	Victim State	Victims Per 100,000 Population	Number of Victims	Rank	Victim State	Victims Per 100,000 Population	Number of Victims
1	Arizona	122.4	6,832	26	Kansas	50.6	1,378
2	Nevada	113.4	2,541	27	Rhode Island	49.9	537
3	California	111.2	39,452	28	Minnesota	49.7	2,517
4	Texas	93.3	20,634	29	Oklahoma	48.1	1,689
5	Florida	83.0	14,119	30	Ohio	48.0	5,494
6	New York	82.4	15,821	31	Tennessee	47.6	2,782
7	Oregon	81.7	2,909	32	Arkansas	47.5	1,294
8	Colorado	81.3	3,698	33	South Carolina	45.7	1,895
9	Illinois	77.4	9,792	34	Nebraska	44.9	781
10	Washington	77.3	4,741	35	Wisconsin	42.5	2,325
11	Maryland	74.9	4,124	36	Louisiana	41.7	1,875
12	Georgia	70.5	6,127	37	Alabama	40.5	1,823
13	New Mexico	70.3	1,317	38	New Hampshire	38.8	500
14	New Jersey	68.9	5,948	39	Mississippi	37.6	1,084
15	North Carolina	65.9	5,537	40	Idaho	36.1	493
16	Michigan	65.1	6,566	41	Alaska	35.6	231
17	Missouri	61.3	3,496	42	Wyoming	34.3	172
18	Indiana	59.1	3,660	43	Kentucky	32.3	1,332
19	Virginia	58.2	4,297	44	Montana	30.7	282
20	Delaware	57.7	472	45	Iowa	30.6	900
21	Massachusetts	56.5	3,634	46	West Virginia	28.1	508
22	Utah	56.4	1,326	47	Maine	27.0	353
23	Connecticut	54.9	1,913	48	Vermont	25.7	159
24	Pennsylvania	52.9	6,545	49	North Dakota	20.0	127
25	Hawaii	51.6	649	50	South Dakota	19.6	150

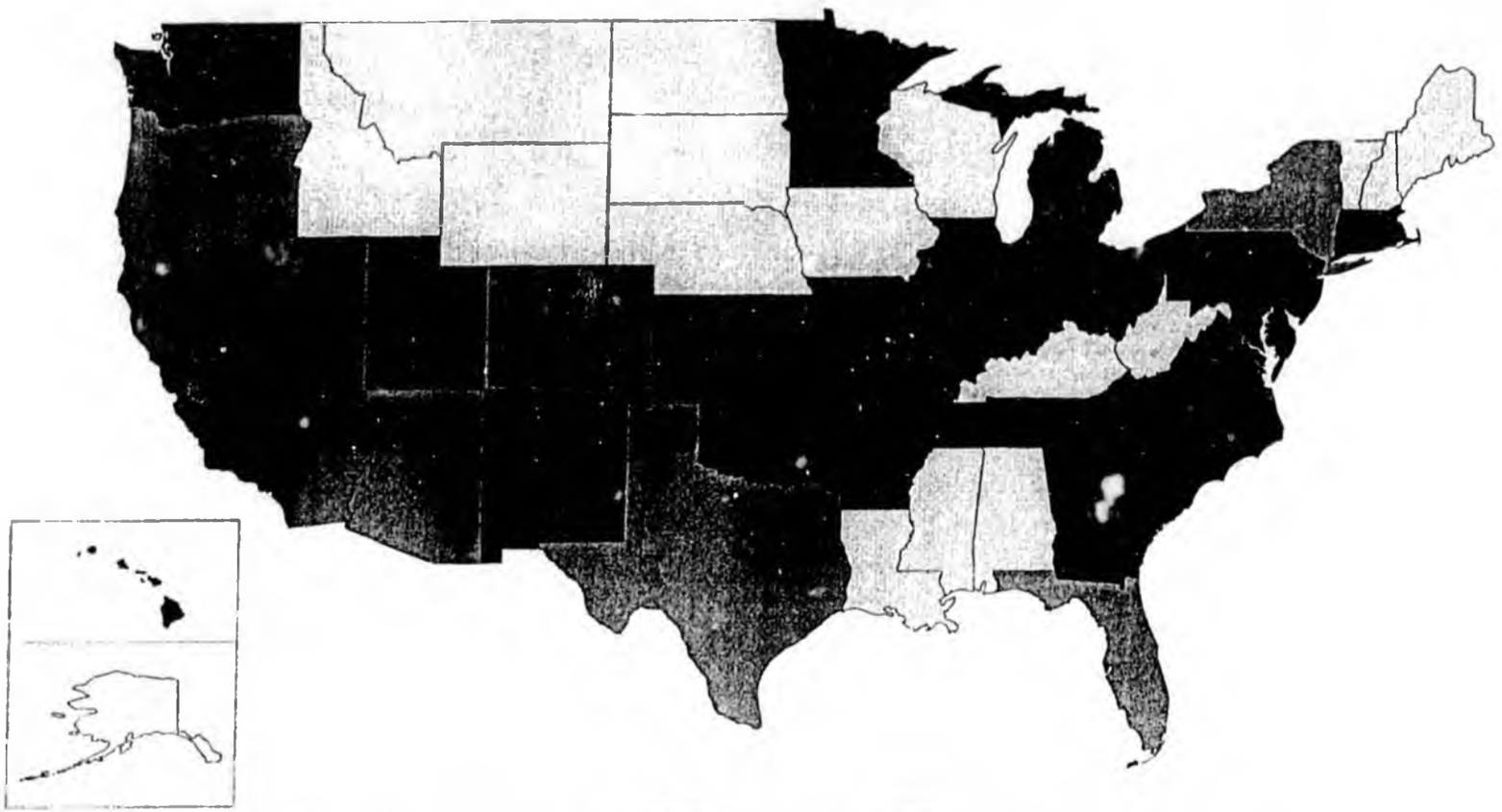
[1]Per 100,000 unit of population estimates are based on the 2003 U.S. Census population estimates (Table NST-EST2003-01 - Annual Estimates of the Population for the United States and States, and for Puerto Rico: April 1, 2000 to July 1, 2003). Numbers for the District of Columbia are: 917 victims and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

Federal Trade Commission
Created January 22, 2004

IDENTITY THEFT
Data Clearinghouse

Figure 4b
Identity Theft Victims by State (Per 100,000 Population)[1]

January 1 – December 31, 2003



Less Than 45 | 45-80 | More Than 80

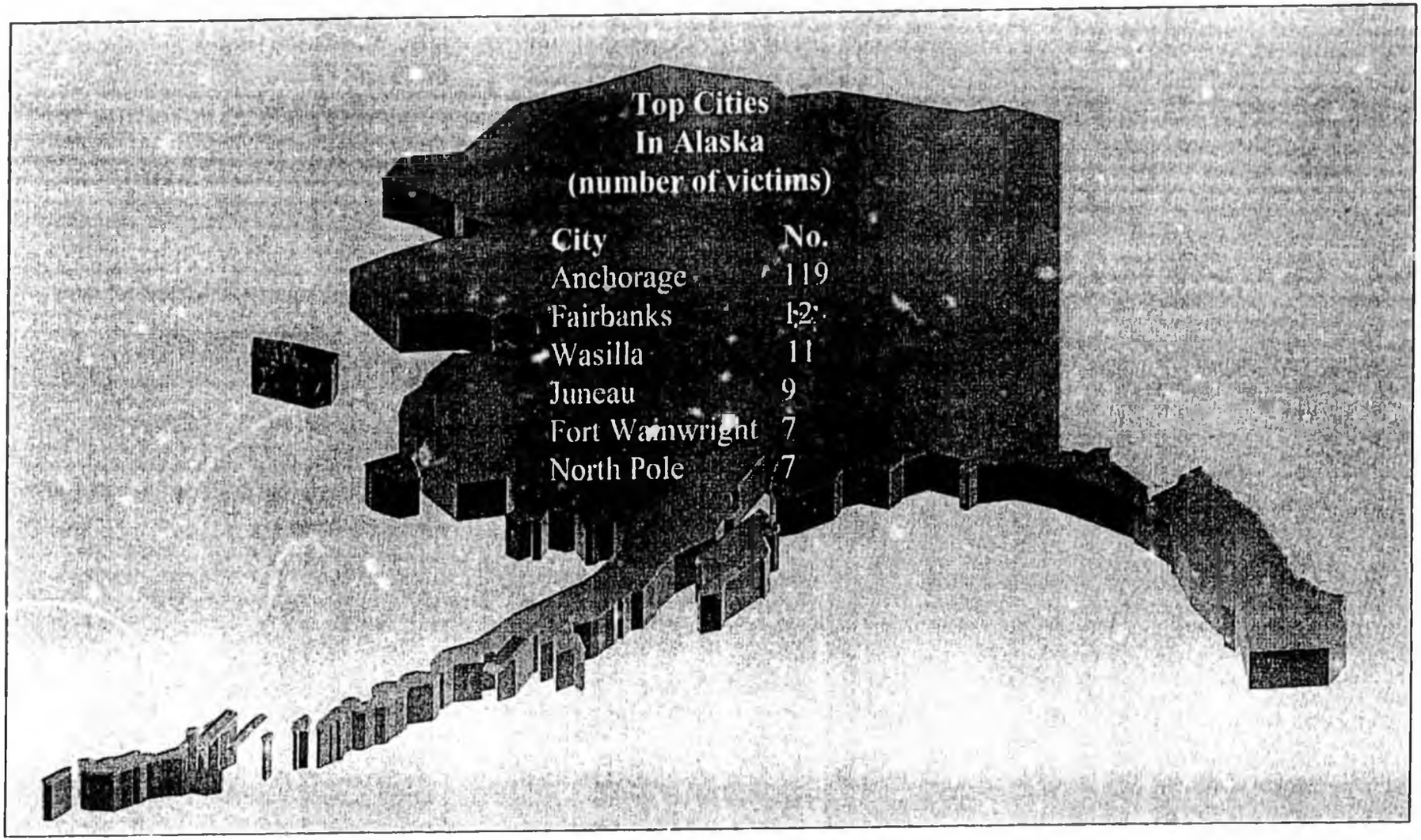
[1]Per 100,000 unit of population estimates are based on the 2003 U.S. Census population estimates (Table NST-EST2003-01 - Annual Estimates of the Population for the United States and States, and for Puerto Rico: April 1, 2000 to July 1, 2003). Numbers for the District of Columbia are: 917 victims and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

Federal Trade Commission
Created January 22, 2004

IDENTITY THEFT Data Clearinghouse

Figure 5
Top Cities in Alaska[1]

January 1 – December 31, 2003



Federal Trade Commission
Created January 22, 2004

[1]99.1% of the 231 victims reporting from Alaska indicated their city of residence.

Fact Sheet 17(g): Criminal Identity Theft

Privacy Right CLEARINGHOU

Privacy Rights Clearinghouse / UCAN and Identity Theft Resource Center
May 2001. Revised May 2002.

Identity Theft Resource Center
P.O. Box 26833
San Diego, CA 92126
(858) 693-7935
Web: www.idtheftcenter.org
E-mail: itrc@idtheftcenter.org

3100 - 5th Ave., Suite B
San Diego, CA 92103
Voice: (619) 298-3396
Fax: (619) 298-5681
Web: www.privacyrights.or
Contact Us:
www.privacyright .org/inquiryfor

HOME

Criminal Identity Theft: What to Do if It Happens to You

Note: Congress recently enacted the Fair and Accurate Credit Transactions Act of 2003 (FACTA) into law, which will amend the Fair Credit Reporting Act (FCRA). This law has provisions that apply to Identity Theft. For more information about FACTA, see our Fact Sheet 6(a) *FACTA, the Fair and Accurate Credit Transactions Act: Consumers Win Some, Lose Some* at www.privacyrights.org/fs/fs6a-facta.htm

What is criminal identity theft? Criminal identity theft occurs when an imposter gives another person's name and personal information such as a drivers' license, date of birth, or Social Security number (SSN) to a law enforcement officer during an investigation or upon arrest. Or the imposter may present to law enforcement a counterfeit license containing another person's data.

Frequently, but not always, the imposter fraudulently obtained a driver's license or identification card in the victim's name and provides that identification document to law enforcement. Or the imposter, without showing any photo identification, uses the name of a friend or relative. In many cases, the imposter is cited for a traffic violation or for a misdemeanor violation and is released from the arrest. The imposter signs the citation and promises to appear in court. If the imposter does not appear in court, the magistrate may issue a bench warrant, but the warrant of arrest will be under the victim's name.

The identity theft victim may not know there is a warrant of arrest issued under his/her name. The victim may unexpectedly be detained pursuant to a routine traffic stop and then subsequently arrested and taken to county jail (booked) because of the outstanding bench warrant.

In some cases the imposter will appear in court for the traffic or misdemeanor violation and plead guilty without the victim being aware of this event. In other cases, the imposter is arrested and booked at the county jail for a felony such as a drunk driving or other serious public offense. The imposter provides the victim's name and personal information. This information is then recorded in the countywide data base and is usually transferred to the State's criminal records data base and possibly to the national data bases, the National Crime Information Center (NCIC)

Some identity theft victims, unaware of the earlier criminal activity by the imposter, may learn of the impersonation when the victim is denied employment or terminated from employment. In these cases, the employer conducted a background investigation and had relied upon the criminal history found under the victim's name. Note that the employer is legally obligated to inform the victim of the reason for the rejection of employment. (See Federal Trade Commission information about this requirement at www.ftc.gov/bcp/conline/pubs/buspubs/credempl.htm.)

Unfortunately, as with financial identity theft, the burden of clearing one's name within the criminal justice system is primarily on the victim. The victim must act quickly and assertively to minimize the damage. Yet, the responsibility to correct the erroneous data in the various criminal justice computer systems is with the officials working within the criminal justice system. There are no established procedures for clearing one's wrongful criminal record.

This guide. The purpose of this guide is to provide information on the steps you must take to clear your name. Be aware that the procedures to correct the record within the criminal justice data bases are likely to be somewhat different from state to state, and even from jurisdiction to jurisdiction. This publication gives you an outline of steps to take.

Organizing your case. In dealing with the authorities, it is vital that you keep a detailed log of all conversations, including dates, names, phone numbers, and e-mail addresses. Note the time spent and any expenses incurred, as you may some day be able to request restitution for damages from the courts. Confirm conversations in writing, especially ones that directly deal with clearing criminal records. Send correspondence by certified mail, return receipt requested. Keep copies of all letters and documents sent by mail for your files.

If you must correspond by e-mail, ask the recipient to verify receipt of the letter with the original message attached. However, we must remind you that electronic messages are not secure and should be used sparingly. Never send anything by e-mail that you would not want publicly published.

We recommend using our Fact Sheet 17(b), "Organizing Your Case," to help you track your efforts. Web: www.idtheftcenter.org/vg106.shtml. Attorney Mari Frank also offers identity theft prevention and survival tools , (800) 725-0807 (www.identitytheft.org).

Criminal records data bases. When an individual is first "booked" or a warrant of arrest is issued, that person's name is likely to be entered into the county data base and the state's criminal records data base. In California, this system is called the Criminal Identification Index (CII).

In the situation of criminal identity theft, the name and other identifying information such as Social Security number that appear in the data bases are that of the victim. The information is also likely to be entered into the Federal Bureau of Investigation's (FBI) National Crime Information Center (NCIC) data base (www.fbi.gov). Victims of criminal identity theft should assume that information is maintained in local, state, and federal criminal history files.

This presents a problem for the victim. The usual method of query by law enforcement into the various criminal justice data bases is by name, date of birth, and/or drivers' license number. Yet, law enforcement relies on the accuracy of such information for their investigations.

Once the victim's name is recorded on a criminal record data base, it will be unlikely that the victim's name will be totally removed from the official record. Should the imposters' true

identity be determined, the victim should request a "key name" switch within the various criminal justice data bases. This means that the record will reflect the imposter's true name as the *primary* name and the victim's name will appear as an *alias* (aka). Law enforcement insists on this record-keeping system because it reflects more accurately the criminal event. The dilemma for law enforcement - and for the victim -- is when the imposter's identity has not been determined.

The following are general steps you must take to clear your name of the erroneous criminal records attributed to you. Please note that these procedures are likely to vary somewhat from jurisdiction to jurisdiction.

1. What is the first step the victim of criminal identity theft should take? Contact the arresting or citing law enforcement agency -- that is, the police or sheriff's department that originally arrested the person using your identity, or the court agency that issued the warrant for the arrest. Explain that this is a case of misidentification and that someone is using your personal information. Insist that you are the victim.

2a. Working with the arresting law enforcement agency: File an impersonation report. The law enforcement agency should first confirm your identity. This can be done by the police department taking a full set of your fingerprints, your photograph, and copying any photo identification documents such as a driver's license, passport, or U.S. legal presence documents.

Once your identity has been established, the law enforcement agency should retrieve the booking record of the criminal event that you dispute. This will include the booking prints and booking photograph or the citation which may or may not have a thumbprint impression. Request that the law enforcement agency compare the prints and/or photographs to establish your innocence.

Subsequently, the law enforcement agency should recall any warrants and issue a "clearance letter" or certificate of release (if you were arrested/booked) which you will need to keep in your possession at all times. Also, request that the law enforcement agency file with the district attorney's office and/or court of jurisdiction the follow-up investigation establishing your innocence which will entail an amended complaint being issued.

Request that the law enforcement agency change *all* records from your name to the imposter's true identity (*if* the true identity of the imposter is known). Some but not all of the levels that must be cleared include city, county, state, and federal data bases.

2b. Working with the court: You will need to determine the specific law(s) in your state that enable you to clear your name in the court records. In California, this is Penal Code Section 851.8, "Determination of Factual Innocence." Ask if something similar to Penal Code Section 851.8 is appropriate in your situation. A judge or magistrate will be required to make this determination.

The declaration should say that you are factually innocent of charges based upon the follow-up impersonation investigation by the law enforcement agency, or declarations, affidavits, or other material and relevant information. This action will change the name on the arrest records and the warrant of arrest to that of the imposter (if the true identity of the imposter is known). Your name will then be known as an alias of the imposter. The court should be requested to provide written verification for you to carry.

The following is a description of the process you are likely to encounter when working with the court to clear your name of the erroneous criminal records that exist in your name. We recommend that you first file an impersonation report with the law enforcement agency of jurisdiction and allow that agency to conduct their follow-up investigation and submit their

findings to the court. However, depending upon the law enforcement agency's readiness for investigating this type of crime (criminal identity theft) or the county's prescribed protocols, you may need to proceed to the court to expedite this process.

If you discovered that there is an arrest warrant or criminal conviction, you may visit the courthouse in the jurisdiction where the arrest was made to schedule a hearing. The office that you visit within the courthouse will depend on whether the warrant is for a felony or misdemeanor crime and/or traffic violation.

It is best to call the courthouse before making the trip so you can verify the specific office, the hours they are open to the public, and what documentation you need to bring with you. Also, obtain the warrant number and/or case number ("docket") of the court. Most likely you will be asked to bring photo identification documents such as a driver's license, passport, or U.S. legal presence documents.

Tell the clerk there is a docket and/or warrant in your name and you dispute the criminal event that appears in your name. Depending upon the court of jurisdiction's protocols, the clerk may copy your identification documents(s) and obtain other pertinent information from you. You will likely be instructed to have your fingerprints taken, which might be done at the District Attorney's office, sheriff's office, or at the courthouse itself.

Arrangements will be made to schedule an "identity hearing" with the goal of obtaining a determination of factual innocence. At that hearing a judge will examine the evidence, whether it is proof you obtained on your own or subsequent police reports. If the court determines that you indeed are the wrong person named in the case/warrant, you will be issued a certificate that declares your innocence in this case.

For this and any other "certificates of clearance" that you obtain, make several copies. Carry one with you at all times. File another at home in a secure place. Give others to relatives and/or friends who can be contacted in situations where you might have forgotten yours. If you are a California resident, see also step 8 below.

Remember, this whole process can be complex. It involves the arresting agency, the court, and the administrators of the various criminal justice data base systems including the motor vehicle data bases. In the best-case scenario you might be able to completely separate your name from the imposter. In most cases, your name will remain a known alias of the imposter indefinitely.

3. What if the victim of identity theft lives in one county and the criminal event including the arrest warrant, traffic citation, or criminal conviction originated from another county or state? Go to the police or sheriff department in your *own* jurisdiction or residency and request they take an impersonation report. Obtain a copy of the report and report number. Ask them to take the report under the appropriate Penal Code Section for either identity theft or false personation. You can visit the Federal Trade Commission web site to determine whether your state has enacted an identity theft statute (www.consumer.gov/idtheft).

In California, the law enforcement agency in the victim's own jurisdiction is now required by law (Penal Code Section 530.6) to take an impersonation report. It may begin an investigation or refer the matter to the law enforcement agency where the suspected crime was committed for an investigation of the facts.

In states other than California that might not have a "local jurisdiction" law such as Penal Code 530.6, request your local law enforcement to take a "courtesy report." Mail the report, your fingerprints, your photograph, and any photo identification documents such as a driver's license, passport, or U.S. legal presence documents to the police department in

the jurisdiction where the arrest warrant, traffic citation, or criminal conviction originated. Include any information you may have about the imposter, including but not limited to photograph, physical description, fingerprints, known alias and addresses.

The best method to track and resolve your case is to establish direct communication with the assigned detective or investigator. Ask this person what additional steps you need to go through to obtain a letter of clearance from their agency. Also, consider that you may be requested to sign an affidavit under the penalty of perjury that you did not give any individual permission or authority to use your name, personal identifiers including birth date, driver's license number, and Social Security number. You may also be called to testify in court if the imposter is identified and prosecuted.

You should also ask your local law enforcement agency if it can query your name through various law enforcement data bases (see item number 2a above) to see if there are any outstanding warrants, arrests, traffic violations, or convictions, that you do not yet know about. In some states, this step may be against system policies and/or may be unlawful - California, for example. But in such situations, you can ask law enforcement if they will determine simply *if* a record exists under the victim's name/identity, even though they may be prohibited from releasing this data to you, the victim.

4. Should the victim contact the Department (Bureau) of Motor Vehicles? Determine if your driver's license has been compromised in your state, or the state where the imposter appears to be committing crimes in your name. Order a certified copy of your drivers' license record for your own review of possible discrepancies. The imposter might have fraudulently obtained a duplicate license under your name and license number but has his/her photograph on the license. Or the imposter may have applied for an original license in a particular state while you live in another state. Ask if your license record can be "flagged" for possible fraud. A directory of DMVs in all 50 states can be found at www.aamva.org, the American Association of Motor Vehicle Administrators.

In California, if you can substantiate that your license number has been used fraudulently, you are entitled to a new license number. Check with your local DMV for their policy and procedures. The California DMV's toll-free fraud assistance phone number is (866) 658-5758. Its e-mail address is dlfraud@dmv.ca.gov. Its website is www.dmv.ca.gov/consumer/fraud.htm.

5. What if law enforcement determines the victim's innocence but doesn't know the true name of the imposter? In the event that the imposter's true name is not yet known, request the "key name," or primary name, be switched from your name to the name "John Doe" with your name noted as an alias.

6. What if the police agency does not believe that an imposter committed the crimes and arrests the victim? The first step is to ask the police to compare the arrest information - physical description, fingerprints, mug shots - to you. This should help prove your innocence. You may have to establish an alibi for the criminal event committed by the imposter. Check your date book: Can employment records establish your innocence? Do you have any receipts that prove where you were at the time of the criminal event. Is there someone who can vouch for your presence elsewhere? If this fails, you should give serious consideration to hiring a criminal defense attorney.

7. What if no fingerprints were taken by the arresting officer when the imposter was arrested? This often happens, especially with traffic violations and some misdemeanors like shoplifting. If the citation(s) does not contain a thumbprint, the law enforcement agency can compare your handwriting or signature to that of the citation. Or a vehicle records check can establish that you were not the registered owner of the vehicle that was associated with the citation. (Caution: Some imposters have registered vehicles using the victim's name.) Or the traffic officer that issued the citation may be asked to look at a photo

line-up to establish that you were not the person cited.

8. Are there any agencies that might help the victim? In California, Senate Bill 129, passed into law in 2000, established the nation's first Office of Privacy Protection within the State Department of Consumer Affairs. It serves as the central clearinghouse where California consumers can file complaints and seek advice about identity theft and other privacy related issues.

In 2000, the California Legislature passed another law to assist victims of criminal identity theft, AB 1862. This law establishes an Identity Theft Registry within the California Department of Justice as a companion data base to the Criminal Identification Index (CII), discussed above. Bona fide victims of criminal identity theft can register information about their case with this data base. If they are wrongfully arrested for the crimes of their imposter, they can direct the arresting officer to the data base, accessible by a toll-free telephone number. If the victim applies for a job and knows that a background check will be conducted, he/she can instruct the employer to access the registry in order to learn that the applicant is *not* the individual committing the crime(s).

Information about these legislative bills can be found at www.leginfo.ca.gov. You can obtain information about California statutes (the Motor Vehicles Code or the Penal Code, for example) at www.leginfo.ca.gov/calaw.html.

The toll-free number for the Calfornia Department of Justice's Identity Theft Registry is (888) 880-0240. The program can also be contacted by e-mail, IEP.CommandCenter@doi.ca.gov. The California Office of Privacy Protection has a guide for registering with the Department of Justice at http://www.privacy.ca.gov/cover/identitytheft.htm called *How to Use the California Identity Theft Registry* with applicable forms. Additional information about the Identity Theft Registry can be found at the California Attorney General's web site at www.ag.ca.gov/idtheft/general.htm.

If you are aware of agencies and organizations in other states that provide assistance to victims of criminal identity theft, please contact the Privacy Rights Clearinghouse through our inquiry form at www.privacyrights.org/inquiryform.html.

9. Should the victim hire an attorney? Competent legal counsel can be invaluable in helping you to clear your name. We have talked with several victims who were unable to attract the attention of law enforcement and court personnel *until* an attorney (a criminal defense attorney) contacted them. We have also spoken with victims who have been able to navigate the criminal justice system without legal help. However, it took them considerable time and they felt vulnerable to being arrested for the crimes committed by the imposter.

10. Should the victim change their Social Security number or driver's license number? Not for most situations. Changing your Social Security number may cause more problems than it solves because you start with fresh records. You no longer have a financial history, work history, or even college records. A clean slate is considered negative by most lenders. These records are all linked by your old Social Security number. (See Fact Sheet 17(L), "Should I Change My Social Security Number," at www.idtheftcenter.org/vg113.shtml)

If your driver's license number was used fraudulently by an imposter in a scheme to issue bogus checks to businesses, the license number may have been recorded and flagged by one of the various check cashing verification companies, for example, Telecheck. This may result in your check cashing privileges being denied. In this case, we recommend requesting a new license number. Be sure to contact the appropriate check verification

service to clear the erroneous record.

11. In addition to working with law enforcement and the court system, are there any other steps the victim should take to clear his/her name? Yes. You must contact any information brokers who may have purchased your wrongful criminal records from the courts and/or law enforcement agencies.

Just like consumer reporting agencies compile credit data on consumers for the purpose of selling credit reports, information brokers compile criminal record information on individuals. They sell such information to employment background checkers, private investigators, attorneys, debt collectors, and others. Information brokers purchase such records from courts and law enforcement agencies throughout the country. Your wrongful criminal record is likely to have found its way to one or more of these data bases. The problem is that it may be very difficult to determine which information brokers have obtained the erroneous information and who they may have sold it to.

You should start by asking the court administrator who they sell their data to. Similarly, ask the law enforcement agency who they sell arrest data to, if anyone, and who else might have access to that data. You will want to immediately contact these entities in writing and request that they remove the erroneous information from their records. Also ask them who, if anyone, they have sold the information to, or who else has access to their data base. Do not be surprised if these companies are less than cooperative. If you encounter resistance, you may need to hire an attorney.

The information broker industry is, for all practical purposes, not regulated by federal or state law. There are no *legally-mandated* standards that they must comply with. Their trade association, the Individual Reference Services Group, has established a *voluntary* set of privacy principles (see www.lrsg.com) in conjunction with the Federal Trade Commission (www.ftc.gov). Unfortunately, these guidelines do not give victims of criminal identity theft meaningful access to the records about them.

12. What additional considerations should I be aware of regarding employment? You may have learned about your wrongful criminal record from an employer who conducted a background check on you, and who has decided *not* to hire you because of the criminal record that was found. That employer is *obligated* to give you a copy of the report *and* tell you the name of the investigative company that compiled the report. This is a requirement of the federal Fair Credit Reporting Act, discussed in the next section.

Once you have learned the name of the company that conducted the background check, you should contact them and ask which information broker data base(s) they used in compiling the report. Then you must contact those companies to remove the erroneous data. Again, this is a situation in which the assistance of a competent attorney is likely to be invaluable.

If you are a victim of criminal identity theft, and if wrongful criminal records are preventing you from obtaining employment, you might want to request a criminal record clearance search through your state Department of Justice criminal records unit. In California, the fee is $25.You would fill out an application and submit fingerprints to the California Department of Justice. Your local police department can assist you in preparing a set of prints that is acceptable to the DOJ.

The DOJ then will conduct a criminal records search based on your fingerprints. If no matches are found, you will receive a letter from the DOJ stating that you have no criminal record based upon a fingerprint search. This could assist you in employment situations where wrongful criminal records are a barrier to finding a job. For more information about the California DOJ's criminal records search, visit their web site,

www.ag.ca.gov/ag/publications/directory.pdf. (Look for "Criminal History Records" in the index.) Or call (916) 227-3832. For links to the Attorneys General offices (DOJ) in the 50 states, visit the web site of the National Association of Attorneys General, www.naag.org.

13. Are there any precautions individuals can take to prevent becoming a victim of criminal identity theft? There is no "early detection" system to alert victims of criminal identity theft. However, there are some things that you can do as precautions. Besides ordering your credit history from the three credit bureaus each year, periodically obtain a copy of your driver's license record from your local DMV. Also, order a copy of your Personal Earnings and Benefits Estimate Statement from the Social Security Administration. Information about obtaining these documents can be found in Fact Sheets 17 and 17a at www.privacyrights.org. These fact sheets discuss credit-related identity theft.

Most victims learn of the perils of criminal identity theft by indirect means. These include notice of citation(s) from the courts, collection agency calls, and notice of warrant(s) of arrest. During a routine traffic stop, a police officer might inform the victim that their license was suspended or revoked. Or the victim might be arrested for crimes committed by the imposter.

We know of individuals who have been refused employment because of criminal identity theft. They learned of their wrongful criminal record from information obtained by the employer on the background check. Federal law requires employers to notify job applicants if they have been refused the job because of information on the background check. (For more information about the federal Fair Credit Reporting Act and "consumer investigative reports," see www.ftc.gov/bcp/conline/pubs/buspubs/credempl.htm.)

We have learned of several instances where employers did *not* comply with this law, and left the criminal identity theft victims in the dark about their wrongful criminal records. If you have repeatedly been rejected for employment, you might want to conduct a background check on yourself. There are two ways to do this. First, you could hire an investigative firm that specializes in employment checks to conduct the search. Many such companies can be found in the Yellow Pages under "Investigators." Be sure to check for proper credentials such as a state-issued private investigator license. Ask if the investigator is a member of a professional or trade association. Costs and investigative methods vary, so do some comparative shopping.

In California you can contact the referral services of two professional associations to obtain names of private investigators who specialize in employment background checks: the California Association of Licensed Investigators, at (800) 350-2254, and the California Institute for Professional Investigators, at (800) 400-2474. If you live in another state, find out if there is a private investigators professional association that makes referrals.

For information about private investigative services in other states, visit the web sites of the National Association of Legal Investigators (www.nalionline.org/sponsors_associations.html) and the National Association of Security and Investigative Regulators (www.nasir.org/licensing.htm).

Or second, you can use one of the online information broker services to conduct your own background check. These include: www.privacyscan.com, www.mybackgroundcheck.com, www.ussearch.com, www.uslocate.com, www.whoishe.com, among others. Be aware, however, that professional employment investigators are skilled in conducting background checks. They may be able to find information that you are not able to uncover on your own.

Some additional action steps:

We hope that the above steps will help guide you in dealing with the struggles of criminal identity theft. Remember that the preceding steps to correct the record within the criminal justice system will be different from state to state, and even from county to county. If you become a victim of criminal identity theft, we recommend that you file a complaint with the Federal Trade Commission so they may more accurately monitor such crimes. This may be done online at www.consumer.gov/idtheft.

Please also share your experience with us. We are compiling information from around the country on the steps victims must take to clear their names from wrongful criminal records. This guide has focused on procedures victims must take in California. We want to expand this guide to include information useful to victims in other states. Contact us at www.privacyrights.org/inquiryform.html or itrc@idtheftcenter.org.

You might want to advocate for the improvement of laws regulating employment background checks and the information broker industry. We recommend that the Fair Credit Reporting Act be amended to improve employer disclosure requirements to those whose backgrounds they are investigating. (FCRA, 15 USC sec. 1681, text available at www.ftc.gov) Victims of criminal identity theft should not be left unaware of the reason they are being denied employment. The following are two suggested amendments.

> The FCRA should be amended to require that job applicants be given the results of background checks in *every* instance -- not just when the employer uses the report to make an adverse decision about them. For example, the employer could say that they did not use the results of the background check when making the adverse employment decision, but, rather, that the individual did not have the requisite skills, or that the job pool had other individuals with higher qualifications.
>
> Right now, compliance with the FCRA is only required when the employer hires a third party, such as a private investigative firm, to conduct background checks. For employers who conduct their own investigations, the disclosure requirements of the FCRA do not apply. The laws in many states also contain this loophole. In this day and age of Internet access to public records data and to information brokers, employers can go online and do their own investigations. Several such online information brokers are listed in step 13 above. The FCRA and equivalent state laws should be amended to require that such employers disclose the results of background checks that they perform themselves and provide the source of the information to the job applicants. In California, the Investigative Consumer Reporting Act has been amended to include such requirements (AB 655, 2001 Legislative session, California Civil Code 1786).

For additional information on the problem of criminal identity theft, see the PRC's June 2000 presentation on "The Growing Problem of Wrongful Criminal Records" on its web site at www.privacyrights.org/ar/wcr.htm.

This publication was written by Linda Foley, Director, Identity Theft Resource Center; Beth Givens, Director, Privacy Rights Clearinghouse; and Paul Satkowski, state investigator.
 Their mailing information is at the beginning of this guide. We thank Paul Johnsen (San Diego County District Attorney's office), Bronti Kelly (victim advocate), and Mari Frank, Esq. for their insights and advice.

HOME TOP

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

April 4th, 2005

AkPIRG Statement of Support for:

SB 149: Identity Theft Protections

The Alaska Public Interest Research Group (AkPIRG), an Alaska membership organization dedicated to protecting consumers, urges quick passage of SB 149. This bill is an appropriate response to the ChoicePoint Inc. security breach that occurred in February, and will greatly enhance consumer protection in regard to Identity Theft. Consumers were alarmed to find out that nearly 150,000 people across the nation had their personal information stolen and were at high risk for identity theft. Yet only California had laws on the books that mandated ChoicePoint Inc to even notify those who fell victim.

The total included some 251 Alaskans. This bill will help better protect those individuals and all Alaskans if and when a similar security breach occurs in the future, and it will protect Alaskans from the increasing array of sophisticated identity thieves.

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

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

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

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

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

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

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

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

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

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

Sincerely,

Steve Cleary
AkPIRG Executive Director

Consumers Union

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

April 1, 2005

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

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

Dear Senator Guess:

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

Security freeze

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

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

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

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

Federal law is inadequate to prevent identity theft

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

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

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

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

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

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

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

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

Notice of security breach

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

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

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

Very truly yours,

Gail Hillebrand

Gail Hillebrand

VIDEO Professor

March 28, 2005

Rep. John Coghill
Alaska State Legislature

Dear Rep. John Coghill,

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

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

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

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

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

Identity thieves are predators of the worst kind.

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

Yours truly,

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

AARP Alaska

April 26, 2005

The Honorable Ralph Seekins, Chair
Senate Judiciary Committee
Alaska State Capitol, Room 125
Juneau, AK 99801-1182

RE: SB 149 (Guess)--Support

Dear Chair Seekins:

On behalf of the members of AARP in Alaska, we encourage you and your colleagues on the Senate Judiciary Committee to support SB 149, authored by your Committee member Senator Gretchen Guess.

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

SB 149 will mandate that any company that has had its customer financial information stolen must notify those customers that they could be victimized.

SB 149 also requires the three companies that have credit information on all of us to offer security freeze protection. Security freeze protections allow the consumer to determine which companies will be allowed credit information which can be used for lines of credit. This will provide an effective tool to prevent false applications for credit because of stolen information/identity theft.

SB 149 addresses a variety of issues associated with identity theft in a very comprehensive manner. Millions of Americans have been negatively impacted by identity theft that has cost billions of dollars and hundreds of hours clearing up their

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

records. Even small amounts of losses can be devastating to older citizens who are living on fixed incomes.

This issue needs to be addressed and SB 149 is one good way to help Alaskans.

We urge an "AYE" vote on SB 149.

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

Thank you for your consideration.

Sincerely,

Marie Darlin

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

CC: Vice-Chair Charlie Huggins
Senator Gene Therriault
Senator Hollis French
Senator Gretchen Guess

Fax Cover Sheet

Alaska State Office
907.341.2270 fax
907.341.2277 voice
ak@aarp.org

3601 "C" Street,
Suite 1420

Anchorage, AK
99503

TO:	SENATOR RALPH SEEKINS	**FROM:**	PAT LUBY
COMPANY:		**DATE:**	
FAX NUMBER:	907-465-5241	**# PAGES:**	

HB

155

SENATE COMMITTEE REPORT

DATE: 3/22/05

FURTHER: Finance

DATE TURNED
IN TO OFFICE:_____

Judiciary Committee considered CS FOR HOUSE BILL NO. 155(JUD)

HB 155 YOUTH COURTS AND CRIMINAL FINES

"An Act relating to funding for youth courts; and relating to separately accounting for fines imposed on and collected from defendants.

and recommends:

[ ] be **replaced** with _____ **CS** _____ (_____)

[ ] adopt **previous** _____ **CS** _____ (_____)

[ ] attached amendment(s)

[ ] adopt Letter of Intent by _____ Committee

[ ] further referral to _____ Committee

CS Senate Bill:
[ ] Same Title
[ ] New Title

SCS House Bill:
[ ] Same Title
[ ] Technical Title Change
[ ] New Title w/ SCR #_____

NEW FISCAL NOTE(S):

Department	Date	Fiscal	Indet.	Zero	FN#

PREVIOUS FISCAL NOTE(S):

Department	Date	Fiscal	Indet.	Zero	FN#

[ ] **APPROPRIATION - no fiscal note**

SIGNATURES AND RECOMMENDATIONS:	DO PASS	DO NOT PASS	NO REC	AMEND
	X			
	X			
	X			
	X			
CHAIR:	✓			

REPRESENTATIVE RALPH SAMUELS

HOUSE DISTRICT 29

CS HB 155 (JUD)

SPONSOR STATEMENT

"An Act relating to funding for youth courts; and relating to separately accounting for fines imposed on and collected from defendants."

HB 155 would create a separate accounting mechanism for fines collected by the Alaska Court system in criminal judgments and would authorize the legislature to appropriate up to 25% of those collected fines either directly to local youth courts or to the United Youth Courts of Alaska for distribution to local youth courts.

Currently youth courts operate in fourteen communities throughout Alaska: Anchorage, Delta Junction, Fairbanks, Homer, Juneau, Kake, Kenai, Ketchikan, Kodiak, Kotzebue, Mat-Su, Nome, Sitka and Wrangell. The Anchorage Youth Court, established in 1989, is the oldest of the programs. In the first two quarters of the current fiscal year, there have been 471 youth offenders referred to these programs, and 8,833 hours of community service and $7,502.00 in restitution ordered.

Since 1989, 4,049 cases have been referred to the Anchorage Youth Court alone. These youth offenders have completed a total of 85,576 community work service hours and paid $68,300.00 in restitution to victims. These programs, while unique in their own ways, are working. A 2002 Urban Institute study found that only 6% of offenders going through the Anchorage Youth Court re-offend - by far the best percentage of any court in the study.

First time offenders not held accountable for their illegal acts results in more frequent and serious juvenile crimes in the future. Youth courts provide an effective avenue to intervene early with young offenders and set them on the right track to deter them from becoming adult offenders.

HB 155 will provide a way for the legislature to annually allocate funds to support this effective, worthwhile, and cost efficient program.

Email: Representative_Ralph_Samuels@legis.state.ak.us

Session: Alaska State Capitol, Juneau, Alaska 99801-1182 • Phone: (907) 465-2095 Fax: (907) 465-3810

Interim: 716 W. 4th Ave., Anchorage, Alaska 99501-2133 • Phone: (907) 269-0240 Fax: (907) 269-0242

FISCAL NOTE

STATE OF ALASKA
2005 LEGISLATIVE SESSION

Fiscal Note Number: 1
Bill Version: CSHB 155(JUD)
(H) Publish Date: 3/3/05

Revision Date/Time (Note if correction):
Dept. Affected: LAW
Title "An Act relating to youth courts and to the recommended use of criminal fines to fund activities..."
RDU CRIMINAL
Component Criminal Justice Litigation
Sponsor Representative Samuels
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 12.55.035 in the Code of Criminal Procedure by adding a requirement that fines collected shall be separately accounted for as general fund program receipts. The Department of Law already accounts for the receipts this way. Additionally, the bill allows the legislature to appropriate 25% of the criminal fines collected to fund youth courts in Alaska. The Department of Law also relies on these funds to help pay for its Collections unit in the Civil Division. The FY 2005 level of that appropriation is $306,800 and our FY 2006 funding request is $324,800. Based on FY 2004 actuals, approximately $1.2 million in fines was collected by the unit, so at least for now, sufficient funds appear to be available to satisfy a 25% appropriation without jeopardizing the Department of Law's funding. We therefore do not anticipate a fiscal impact from passage of this legislation.

Prepared by: Kathryn Daughhetee, Director
Phone 465-3673
Division Administrative Services Division
Date/Time 3/1/05 1:48 PM
Approved by: K. Daughhetee for Scott Nordstrand, Acting Attorney General
Date 3/1/2005
Agency Department of Law

(Revised 9/23/2004 OMB)

FISCAL NOTE

STATE OF ALASKA
2005 LEGISLATIVE SESSION

Fiscal Note Number: 2
Bill Version: CSHB 155(JUD)
(H) Publish Date: 3/3/05

Revision Date/Time (Note if correction): 3/1/05 5:30 p.m.
Dept. Affected: Health & Social Services

Title: RELATING TO YOUTH COURTS AND CRIMINAL FINES
RDU: Juvenile Justice
Component: Probation Services

Sponsor: SAMUELS
Requester: HOUSE (JUD)
Component No.: 2134

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	36.8	36.8	36.8	36.8	36.8	36.8
Travel						
Contractual						
Supplies						
Equipment						
Land & Structures						
Grants & Claims						
Miscellaneous						
TOTAL OPERATING	**36.8**	**36.8**	**36.8**	**36.8**	**36.8**	**36.8**
CAPITAL EXPENDITURES						
CHANGE IN REVENUES (0)						

FUND SOURCE (Thousands of Dollars)

1002 Federal Receipts						
1003 GF Match						
1004 GF	36.8	36.8	36.8	36.8	36.8	36.8
1037 GF/Mental Health						
Other(Specify Type-do not abbreviate)						
Other(Specify Type-do not abbreviate)						
TOTAL	**36.8**	**36.8**	**36.8**	**36.8**	**36.8**	**36.8**

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

POSITIONS

Full-time						
Part-time	1	1	1	1	1	1
Temporary						

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

This fiscal note is based on the assumption that the Legislature wants to appropriate 25% of the fines collected from the Alaska Court System to help fund youth courts in Alaska as this legislation would allow.

Currently, an Associate Coordinator position within the Director's Office of the Division of Juvenile Justice manages the youth court grants that currently exist. On this fiscal note, the Division is reflecting the proposed appropriation of a .5 FTE at this same level. Based on the estimated 35 additional grants that would be incurred for this Division, it has been determined that an additional part-time position would need to be established to absorb the additional workload.

Prepared by: Patty Ware
Phone 465-2112
Division: Juvenile Justice
Date/Time 03/01/2005
Approved by: Joel S. Gilbertson, Commissioner
Date 03/02/2005
Agency: Department of Health and Social Services

FISCAL NOTE

STATE OF ALASKA
2005 LEGISLATIVE SESSION

Fiscal Note Number: 3
Bill Version: CSHB 155(JUD)
(H) Publish Date: 3/16/05
Revision Date/Time (Note if correction):
Dept. Affected: Health & Social Services

Title: RELATING TO YOUTH COURTS AND CRIMINAL FINES
RDU: Juvenile Justice
Component: Probation Services

Sponsor: SAMUELS
Requester: HOUSE (FIN)
Component No.: 2134

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 (0)						

FUND SOURCE (Thousands of Dollars)

1002 Federal Receipts						
1003 GF Match						
1004 GF						
1037 GF/Mental Health						
Other(Specify Type-do not abbreviate)						
Other(Specify Type-dc not abbreviate)						
TOTAL	0.0	0.0	0.0	0.0	0.0	0.0

Estimate of any current year (FY2005) cost:
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 fiscal note is based on the assumption that the Legislature wants to appropriate 25% of the fines collected from the Alaska Court System to help fund youth courts in Alaska as this legislation would allow.

On this fiscal note, the Division is reflecting A $0.0 impact in FY06 and an indeterminate amount for the following fiscal years.

Prepared by: Patty Ware, Director
Phone 465-2112
Division: Juvenile Justice
Date/Time 03/11/2005
Approved by: Joel S. Gilbertson, Commissioner
Date 03/14/2005
Agency: Department of Health and Social Services

(Revised 9/23/2004 OMB)