SENATE STAFF ANALYSIS AND ECONOMIC IMPACT STATEMENT

(This document is based on the provisions contained in the legislation as of the latest date listed below.)

BILL: CS/ CS/SB 1072

SPONSOR: Appropriations Subcommittee on Criminal Justice and Criminal Justice and Senator Crist

SUBJECT: Criminal Use/Personal ID Information

DATE: April 10, 2003 REVISED: _____ _____ _____ _____

	ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
1.	Erickson	Cannon	CJ	Favorable/CS
2.	Noble	Sadberry	ACJ	Favorable/CS
3.			AP	
4.				
5.				
6.				

I. Summary:

The bill amends s. 817.568, F.S., to provide that it is a second degree felony with a mandatory minimum sentence of 3-years imprisonment, for a person to willfully and without authorization fraudulently use personal identification information of an individual without first obtaining that individual's consent.

Currently, the monetary amount that triggers this offense is $75,000 or more. This bill provides that the second degree felony applies if the pecuniary benefit, the value of the services received, the payment sought to be avoided, or the amount of the injury or fraud is $5000 or more or if the person fraudulently uses the personal identification information of 10 or more individuals without their consent. If the amount is $50,000 or more or if the person fraudulently uses the personal identification information of 20 or more individuals without their consent, it is a first degree felony. A mandatory sentence of 5 years applies if the amount is $50,000 to less than $100,000. A mandatory minimum sentence of 10 years applies if the amount is $100,000 or more or if the person fraudulently uses the personal identification information of 30 or more individuals without their consent.

The bill also enhances penalties for identity theft if the offense was committed using the personal identification information of a child. It further enhances penalties if the offense was committed using the personal identification information of a person who is under 18 years of age, over whom the offender has custodial authority.

The bill requires out-of-state corporations who provide electronic communication services or remote computing services to comply with subpoenas or other court orders issued by a Florida court. The bill also requires Florida providers of electronic communication services or remote

computing services to comply with subpoenas or other court orders issued by a court of another state. In addition, the bill creates a new hearsay exception in the Florida evidence code.

The bill substantially amends ss. 817.568, 921.0022, 934.23 and creates 92.605, F.S.

II. Present Situation:

A. Identity Theft: Description, Mode, Information Stolen

The Office of Statewide Prosecution (webpage) provides the following information regarding the offense of "identity theft" or "identity fraud."

> What is Identity Theft or Identity Fraud?
>
> Identity theft or identity fraud (true name fraud) is the criminal act of taking a victim's identity for the purpose of obtaining credit, credit cards from banks and/or retailers, stealing money from the victim's existing accounts, applying for loans in the victim's name, establishing accounts with utility companies, leasing automobiles and residences, filing bankruptcy, and/or even obtaining employment. Identity thieves often steal thousands of dollars from unsuspecting victims, in the victim's own name, without the victim knowing about the fraud for months or sometimes years. Recently, identity thieves have used unsuspecting victim's identities to commit crimes ranging from traffic infractions to felonies.
>
> How Does Identity Theft Occur?
>
> All that is needed is a little information, such as your social security number, birth date, address, phone number, or any other information which can be discovered. Armed with this identifying information, and possibly a false driver's license with the identity thief's picture in place of yours, the identity thief can apply in person for instant credit, or through the mail by posing as you. Often, an identity thief will provide their own address, (claiming to have moved) in an effort to prolong the fraud. Negligent credit grantors, in their rush to issue credit, do not verify information or addresses. As such, once the imposter opens the first account, they can use this new account, along with the other identifying information, to bolster their credibility and obtain even more credit in your name. These criminal actions result in a proliferation of the fraud, and the thief is well on his/her way to getting rich and ruining your credit and good name.
>
> Where Does the Information About You Come From?
>
> Many places- your doctor, accountant, lawyer, dentist, school, place of employment, health insurance carrier, and many others have your identifying information. If some criminally minded person is employed at one of these places, (or is just visiting) and decides to use or steal this information to assume your identity, you would probably not find out about it until after the damage had been done. Further, if this information is not disposed of with a shredder, a "dumpster-diver" could retrieve the information, and

assume your identity without ever having to enter any of the above-mentioned places. You should also be aware that you do not need to lose your wallet or have anything tangible stolen, in order for someone to steal your identity. By simply failing to shred your confidential information, utility bills, credit card slips and other documents, it is easy for an identity thief to "dumpster dive" your garbage, and retrieve your most personal identifying information. In addition, if an identity thief were to obtain your credit report illegally, they would have all the information necessary to become you. You should also know that much of your identifying information is readily available on the Internet, or even at your local courthouse, where it is accessible by the filing of a public records request.

B. Identity Theft National and Florida Statistics

The Federal Trade Commission reports national and state-specific data on the crime of identity theft, compiled from the Consumer Sentinel and Identity Theft Clearinghouse databases. *See National and State Trends in Fraud and Identity Theft/January-December 2002* (last updated January 1, 2003). The number one complaint received was identity theft (43 percent). *Id*. at p. 11. Florida had 80.2 identity theft complaints per 100,000 population (number of complaints: 12,816), which ranked it third in the nation (behind California and Texas). *Id*. Florida had 68.2 victims per 100,000 population (number of victims: 10,898), which ranked it fourth in the nation (behind California, Texas, and New York). *Id*.

Credit card fraud led the list of identity theft types reported in Florida complaints (48 percent or 5,188 complaints) (followed by phone or utilities fraud, bank fraud, loan fraud, government documents or benefits fraud, employment-related fraud, other, and attempted identity theft). *Id*., at p. 22. The top Florida identity theft victim location was Miami (1,836 victims) (followed by Orlando, Tampa, Jacksonville, and Fort Lauderdale). *Id.*

C. Florida's Identity Theft Law

Section 817.568, F.S., provides punishment for the crime of identity theft or identity fraud. There are several identity theft crimes in s. 817.568, F.S. The crime relevant to this analysis is set forth in s. 817.568(2)(b), F.S. This paragraph provides that it is a second degree felony for a person to willfully and without authorization fraudulently use personal identification information concerning an individual without first obtaining that individual's consent, if the pecuniary benefit, the value of the services received, the payment sought to be avoided, or the amount of the injury or fraud is $75,000 or more. This offense is ranked in Level 5 of the offense severity ranking chart of the Criminal Punishment Code.

This offense is similar to an identity theft offense punishable under New Jersey law, in which the monetary amount that triggers the offense is $75,000 or more. *See* N.J. Stat. Ann. § 2C:21-17.

III. Effect of Proposed Changes:

Criminal Use of Personal Identification Information:

The bill amends s. 817.568, F.S., to provide that it is a second degree felony with a mandatory minimum sentence of 3-years imprisonment, for a person to willfully and without authorization fraudulently use personal identification information of an individual without first obtaining that individual's consent. This penalty applies if the pecuniary benefit, the value of the services received, the payment sought to be avoided, or the amount of the injury or fraud is $5000 or more or if the person fraudulently uses the personal identification information of 10 or more individuals without their consent. Currently, the monetary amount that triggers this offense is $75,000 or more.

If the amount is $50,000 or more or if the person fraudulently uses the personal identification information of 20 or more individuals without their consent, it is a first degree felony. A mandatory sentence of 5 years applies if the amount is $50,000 to less than $100,000. A mandatory minimum sentence of 10 years applies if the amount is $100,000 or more or if the person fraudulently uses the personal identification information of 30 or more individuals without their consent.

The bill also changes the definition of "personal identification information" to include a bank account or credit card number.

The bill describes how mandatory sentencing under this section is to occur in relation to other specified penalty or sentencing laws. It provides that if an offense prohibited under this section was committed using the personal identification of a person under the age of 18, the offense severity level must be increased to level 8. If the child involved was the offender's natural child or any child over whom the defendant has custodial authority, the offense severity shall be increased to level 9.

The bill also amends s. 921.0022(3)(e), F.S., to correct the Criminal Punishment Code offense severity ranking chart to reflect changes to the second degree felony offense of criminal use of personal identification information.

Disclosure of Customer Communications or Records:

The bill amends section 934.23, F. S. to define that a "court of competent jurisdiction" means a court having jurisdiction over the investigation or otherwise authorized by law.

Production of Records:

The bill creates section 92.605, F. S. which relates to the production of records by Florida corporations and out-of-state corporations and is identical to section 3 of House Bill 1161. The analysis for that bill states the following:

The newly created section applies to a subpoena, court order or search warrant issued in compliance with the federal Electronic Communications Privacy Act which allows a search for records that are in the actual or constructive possession of an out-of-state corporation that

provides electronic communication services[1] or remote computing services[2] to the public, when those records would reveal:

- the identity of the customers using those services,
- data stored by the customers,
- the customers' usage of those services, or
- the recipients or destinations of communications sent to or from those customers.

The bill provides that when properly served[3] with a subpoena, court order, or search warrant issued by a Florida court, an out-of-state corporation subject to this section shall provide to the applicant[4] all records sought pursuant to the subpoena, court order or search warrant within 10 days or within the time indicated, including records located outside the state of Florida. The bill provides that the corporation can be required to produce the records sooner if the applicant shows that the delay would cause an adverse result. The bill also allows the judge to authorize an extension of time upon a showing of good cause by the corporation. If the corporation seeks to quash the subpoena, court order or warrant, it must seek relief from the court ordering production within 10 days of the order. The corporation must verify the authenticity of records it produces by providing an affidavit.

Florida corporation: The bill requires a Florida corporation that provides electronic communication services or remote computing services to the public to comply with a subpoena, court order or warrant issued by another state in the same manner as if the order had been issued by a Florida court. The bill provides that a cause of action does not arise against any corporation subject to this section for providing records, information facilities or assistance in accordance with the terms of the subpoena, court order or warrant subject to this section.

Admissibility of Records – Hearsay Exception:

The bill provides that in a criminal court proceeding, out-of-state records of regularly conducted business activity[5] or a copy of such a records, shall not be excluded as hearsay evidence if an out-of-state certification[6] attests that:

---

[1] "Electronic communication service" means "any service which provides to users thereof the ability to send or receive wire or electronic communications". 18 U.S.C § 2510 The term does not apply to corporations that do not provide those services to the public. This term is defined in the same manner in s. 934.02(14), F.S.

[2] "Remote computing service" means "the provision to the public of computer storage or processing services by means of an electronic communications system". 18 U.S.C. § 2711. This term is defined in the same manner in s. 934.02(19), F.S.

[3] The bill defines the term "properly served" to mean "delivery by hand or in a manner reasonably allowing for proof of delivery if delivered by United States mail, overnight-delivery service, or facsimile to a person or entity properly registered to do business in any state."

[4] The bill defines the term "applicant" to mean "a law enforcement officer who is seeking a court order or subpoena or who is issued a search warrant or anyone who is authorized to issue a subpoena under the Florida Rules of Criminal Procedure. Rule 3.361 authorizes the clerk of the court or any attorney of record in an action to issue a subpoena.

[5] The bill defines the term" out-of-state record of regularly conducted business activity" to mean "a memorandum, report, record, or data compilation, in any form, of acts, events, conditions, opinions, or diagnoses, maintained in another state or country."

[6] The bill defines the term "out-of-state certification" to mean "a written declaration made and signed in another state or country by the custodian of an out-of-state record of regularly conducted business activity or another

1. Such record was made at or near the time of the occurrence of the matters set forth by, or from information transmitted by, a person with knowledge of those matters.
2. Such record was kept in the course of a regularly conducted business activity.
3. The business activity made such a record as a regular practice.
4. If such records is not the original, it is a duplicate of the original, unless the source of information or the method or circumstances of preparation indicate lack of trustworthiness.

This provision is apparently not intended to apply only to records of electronic communication services or remote computing services but to apply to out-of-state records of any "business". The term business is defined as any "business, institution, association, profession, occupation or calling of any kind, whether or not conducted for profit." The bill also provides that no evidence in such records in the form of opinion or diagnosis is admissible unless such opinion or diagnosis would be admissible if the person whose opinion is recorded were to testify to the opinion.

These provisions are similar to the hearsay exception contained in s. 90.803(6)(a) of the Florida Evidence Code relating to business records with the exception that the required live testimony of the custodian or other qualified witness is replaced with the requirement of out-of-state certification. The Federal Evidence Code contains a similar provision, allowing records of regularly conducted business activity to be admitted based on a written certification.[7] This provision is also similar to the hearsay exception contained in s. 92.60, F.S. which relates to business records kept in a foreign country.

The bill requires a party intending to offer evidence of an out-of-state record of regularly conducted business to provide notice to the other parties as soon after the arraignment as possible or 60 days prior to trial. A party opposing the admission of such records must file a motion and the matter must be determined by the court before the trial. Failure to oppose the admission of the records constitutes a waiver unless the court grants relief from the waiver upon a finding of good cause.

The bill provides that in a criminal case, the content of any electronic communication may be obtained under this section only by court order or by the issuance of a search warrant, unless otherwise provided under the Electronic Communications Privacy Act or other provision of law.

The bill provides an effective date of July 1, 2003.

IV. Constitutional Issues:

A. Municipality/County Mandates Restrictions:

None.

---

qualified person that, if falsely made, would subject the declarant to criminal penalty under the laws of another state or country".

[7] Federal Rule of Evidence 803(6).

B. Public Records/Open Meetings Issues:

None.

C. Trust Funds Restrictions:

None.

V. Economic Impact and Fiscal Note:

A. Tax/Fee Issues:

None.

B. Private Sector Impact:

None.

C. Government Sector Impact:

According to the Office of Economic and Demographic Research, the bill will have an insignificant impact on the need for prison beds.

VI. Technical Deficiencies:

None.

VII. Related Issues:

None.

VIII. Amendments:

None.