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.)

Prepared By: Judiciary Committee

BILL:	CS/SB 978
SPONSOR:	Judiciary Committee and Senator Campbell
SUBJECT:	Unlawful Use of Personal Identification Information
DATE:	April 14, 2005 REVISED:

	ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
1.	Chinn	Maclure	JU	**Fav/CS**
2.			CM	
3.			CJ	
4.			JA	
5.				
6.				

I. Summary:

Committee Substitute for Senate Bill 978 amends s. 817.568, F.S., related to identity theft, to provide that any person who willfully and fraudulently uses or possesses with the intent to use personal identification information concerning a deceased individual commits a third-degree felony. The committee substitute also provides for enhanced penalties and the imposition of three, five, or ten-year minimum mandatory sentences depending on the value of the pecuniary benefit or injury or the number of deceased individuals whose personal identification information is used. The committee substitute creates a third-degree felony offense for willfully and fraudulently creating, using, or possessing with the intent to use counterfeit or fictitious personal identification information for the purpose of committing a fraud upon another person.

The committee substitute also provides for the reclassification of an identity theft offense that involves misrepresenting oneself to be a law enforcement officer, or an employee of a bank, credit card company, credit counseling company, or a credit reporting agency, or any person who wrongfully represents that he or she is seeking to assist the victim with a problem with the victim's credit history. This will have the effect of increasing the maximum sentence that can be imposed for these offenses.

The committee substitute also requires a person who maintains computerized personal identification information for another person or business entity to notify the person or business entity for whom computerized records are maintained when there is a breach of security in the system.

This committee substitute amends section 817.568, Florida Statutes, and creates section 817.5681, Florida Statutes.

II. Present Situation:

Criminal Use of Personal Identification Information – Identity Theft

Section 817.568, F.S., provides that any person who willfully and without authorization fraudulently uses, or possesses with intent to fraudulently use, personal identification information[1] concerning an individual without first obtaining that individual's consent commits a third-degree felony. This offense is commonly known as "identity theft." The section also provides for enhanced penalties for identity theft as follows:

- If the value of the pecuniary benefit, services received, or injury is $5,000 or more or if the person fraudulently uses the personal identification information of 10 or more individuals without their consent, the offense is a second-degree felony and the judge must impose a three-year minimum mandatory term of imprisonment.
- If the value of the pecuniary benefit, services received, or injury is $50,000 or more or if the person uses the personal identification information of 20 or more individuals, the offense is a first-degree felony and the judge must impose a five-year minimum mandatory sentence.
- If the value of the pecuniary benefit, services received, or injury is $100,000 or more or if the person uses the personal identification information of 30 or more individuals, the offense is a first-degree felony and the judge must impose a ten-year minimum mandatory sentence.

This section also provides penalties for the offense of harassment[2] by use of personal identification information as well as using a public record to commit identity theft.[3] Further, the section provides penalties if identity theft is committed using the personal identification information of an individual less than 18 years of age.[4]

Disclosure of Breach of Security

There is currently no provision in the Florida Statutes that requires a person who maintains computerized data for another person or business entity to notify the person or business entity for whom computerized data is maintained when there is a breach in security in the system.

[1] s. 817.568(1)(f), F.S., defines "personal identification information" to mean any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any: 1) Name, social security number, date of birth, official state-issued or United States-issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, or Medicaid or food stamp account number, or bank account or credit card number; 2) Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation; 3) Unique electronic identification number, address, or routing code; or 4) Telecommunication identifying information or access device.

[2] s. 817.568(1)(c), F.S., defines "harass" as engaging in conduct directed at a specific person that is intended to cause substantial emotional distress to such person and serves no legitimate purpose.

[3] s. 817.568(4) and (5), F.S.

[4] s. 817.568(6) and (7), F.S.

III. Effect of Proposed Changes:

Criminal Use of Personal Identification Information

The committee substitute amends the definition of the term "personal identification information" under s. 817.568, F.S., to include: a postal or e-mail address; telephone number; mother's maiden name; debit card number; personal identification number or code assigned to the holder of a debit card by the issuer to permit authorized electronic use of such card; medical records; or other number or information that can be used to access a person's financial resources.

The committee substitute also provides that any person who willfully and fraudulently uses or possesses with intent to fraudulently use personal identification information concerning a *deceased individual* commits a third-degree felony.[5] Penalties for this violation are as follows:

- If the value of the pecuniary benefit, services received, or injury is $5,000 or more or if the person fraudulently uses the personal identification information of 10 or more but fewer than 20 deceased individuals, the offense is a second-degree felony and the judge must impose a three-year minimum mandatory term of imprisonment.
- If the value of the pecuniary benefit, services received, or injury is $50,000 or more or if the person uses the personal identification information of 20 or more but fewer than 30 deceased individuals, the offense is a first-degree felony and the judge must impose a five year minimum mandatory sentence.
- If the value of the pecuniary benefit, services received or injury is $100,000 or more or if the person uses the personal identification information of 30 or more deceased individuals, the offense is a first-degree felony and the judge must impose of a ten year minimum mandatory sentence.[6]

The committee substitute provides that any person who willfully and fraudulently creates, uses, or possesses with intent to use, counterfeit or fictitious personal identification information either concerning a fictitious individual or concerning a real individual without first obtaining that real individual's consent, intending to use such counterfeit or fictitious personal identification information for the purpose of committing or facilitating the commission of a fraud against another person, commits a third-degree felony.[7]

The committee substitute further provides that any person who commits an offense prohibited by s. 817.568, F.S., for the purpose of obtaining or using personal identification information to misrepresent himself or herself to be a law enforcement officer, an employee or representative of a bank, credit card company, credit counseling company or a credit reporting agency, or any person who wrongfully represents that he or she is seeking to assist the victim with a problem with the victim's credit history shall have the offense reclassified as follows:

[5] Proposed s. 817.568(8)(a), F.S.
[6] Proposed s. 817.568(8)(b)-(c), F.S.
[7] Page 4, lines 14-19 provide that "counterfeit or fictitious personal identification information" means "any counterfeit, fictitious, or fabricated information in the similitude of the data outlined [in the definition of personal identification information] that, although not truthful or accurate, would in the context lead a reasonably prudent person to credit its truthfulness and accuracy."

- A misdemeanor offense is reclassified to a third-degree felony;
- A third-degree felony offense is reclassified to a second-degree felony;
- A second-degree felony offense is reclassified to a first-degree felony; and
- A first-degree felony offense is reclassified to a life felony.

The committee substitute also authorizes a prosecutor to move the sentencing court to reduce or suspend the sentence of any person who is convicted of a violation of s. 817.568, F.S., who provides substantial assistance in the identification, arrest, or conviction of any of that person's accomplices, accessories, coconspirators, principals, or of any other person engaged in fraudulent possession or use of personal identification information. The committee substitute requires that the arresting agency be given an opportunity to be heard in aggravation or mitigation in reference to this motion and allows the motion to be filed and heard in camera upon good cause shown.

Disclosure of Breach of Security

The committee substitute creates s. 817.5681, F.S., to provide that any person who conducts business in Florida, and that maintains computerized data that includes personal information, must disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of Florida whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. With certain specified exceptions, disclosure must be made within 30 days following discovery of the breach. The committee substitute provides that any person who fails to make the required disclosure within this time is liable for the an administrative fine in the amount of $1,000 for each day the breach goes undisclosed for up to 30 days. The person is liable for up to $50,000 for each 30-day period the breach goes undisclosed up to 180 days. If disclosure is not made within 180 days, the person is subject to an administrative fine of up to $500,000. The disclosure required must be made by all persons in the state in possession of computerized data, but the administrative sanctions described above do not apply in the case of computerized information in the custody of any governmental agency or subdivision. However, if the governmental agency or subdivision has entered into a contract with a contractor or third party administrator to provide governmental services, the contractor or third party administrator is a person to whom the administrative sanctions would apply, although that contractor or third party administrator found in violation of the non-disclosure restrictions would not have an action for contribution or set-off available against the employing agency or subdivision.

Further, the committee substitute provides that any person that maintains computerized data that includes personal information, on behalf of another business entity, must notify the business entity for whom the information is maintained of any breach of the security of the data within 72 hours of the discovery, if the personal information is reasonably believed to have been acquired by an unauthorized person. The administrative fines described above apply to a person who fails to disclose a security breach under this provision. The committee substitute defines the terms "breach of the security of the system," "personal information," and "unauthorized person." The committee substitute specifies what type of notice must be provided.

This committee substitute provides an effective date of July 1, 2005.

IV. Constitutional Issues:

A. Municipality/County Mandates Restrictions:

None.

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:

The committee substitute requires that a person who conducts business in Florida and maintains computerized data that includes personal information must disclose a breach of the security system to a resident of Florida whose unencrypted personal information was acquired by an unauthorized person. The disclosure must be made within specified time limits. Notice must either be written notice, electronic notice which complies with federal law, or substitute notice including e-mail notice or conspicuous posting on a website if the person demonstrates that the cost of providing notice would exceed $250,000 or the affected class of person to be notified exceeds 500,000. This obligation will have an indeterminate fiscal impact on the private sector. However, the committee substitute could provide added protection from identity theft for residents.

C. Government Sector Impact:

On February 22, 2005, the Criminal Justice Impact Conference decided that the portions of the committee substitute relating to criminal penalties would have an indeterminate effect, but expected minimal impact on the prison population of the Department of Corrections.

VI. Technical Deficiencies:

None.

VII. Related Issues:

None.

VIII. Summary of Amendments:

None.