

FULL ANALYSIS

I. SUBSTANTIVE ANALYSIS

A. HOUSE PRINCIPLES ANALYSIS:

Provide limited government – The bill creates new felony offenses by requiring a business to disclose a security breach which results in personal information being acquired by an unauthorized person in certain circumstances.

Promote personal responsibility – The bill creates sanctions for potentially injurious behavior.

B. EFFECT OF PROPOSED CHANGES:

Criminal Use of Personal Identification Information – Identity Theft: Fla. Stat. § 817.568 currently provides that “[a]ny person who willfully and without authorization fraudulently uses, or possesses with intent to fraudulently use, personal identification information¹ 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 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 ten 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 of a ten year minimum mandatory sentence.

This section also provides penalties for the offense of harassment² 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 eighteen years of age.⁴

HB 481 amends the definition of the term “personal identification information” 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.

¹ Fla. Stat. § 817.568(f) defines “personal identification information” as “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, 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 The term “harass means to engage in conduct directed at a specific person that is intended to cause substantial emotional distress to such person and serves no legitimate purpose. Fla. Stat. § 817.568(1)(c) (2004).

³ 817.568(4) and (5), F.S.

⁴ s. 817.568(6) and (7), F.S.

The bill 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. The bill also provides for enhanced penalties 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.

The bill provides that any person who willfully and fraudulently creates or 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.⁵

The bill further provides that any person who commits an offense prohibited by section 817.568, F.S. and for the purpose of obtaining or using personal identification information misrepresents 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:

- In the case of a misdemeanor, the offense is reclassified as a third degree felony.
- In the case of a third degree felony, the offense is reclassified as a second degree felony.
- In the case of a second degree felony, the offense is reclassified as a first degree felony.
- In the case of a first degree felony, the offense is reclassified as a life felony.

The bill 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 the section and who provides substantial assistance in the identification, arrest, or conviction of any of that person's accomplices, accessories, coconspirators, or principals or of any other person engaged in fraudulent possession or use of personal identification information. The bill 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 bill creates Fla. Stat. § 817.5681 to require that a person who conducts business in Florida and maintains personal information in a computerized data system to disclose a breach in the security of the data to any resident of this State subject to certain exceptions. When a disclosure is required, it must be made without unreasonable delay, and no later than forty-five days following the determination that unencrypted personal information was acquired, or reasonably

⁵ The bill also defines the term "counterfeit or fictitious personal identification information" to mean "any counterfeit, fictitious, or fabricated information in the similitude of the data outlined [in the definition of personal identification information which], although not truthful or accurate, would in context lead a reasonably prudent person to credit its truthfulness and accuracy."

believed to have been acquired, by an unauthorized person and the acquired information materially compromises the security, confidentiality, or integrity of personal information.

The bill provides that any person who fails to make the required disclosure within forty-five days 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 of 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 bill 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 10 days of the determination that a breach has occurred, 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 bill defines the terms "breach," "breach of the security of the system", "personal information," "unauthorized person," and "person." The bill specifies what type of notice must be provided.

C. SECTION DIRECTORY:

Section 1 amends Fla. Stat. § 817.568 relating to criminal use of personal identification information.

Section 2 creates Fla. Stat. § 817.5681 requiring disclosure of security breach in certain circumstances.

Section 3 provides effective date of July 1, 2005.

II. FISCAL ANALYSIS & ECONOMIC IMPACT STATEMENT

A. FISCAL IMPACT ON STATE GOVERNMENT:

1. Revenues:

None.

2. Expenditures:

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

B. FISCAL IMPACT ON LOCAL GOVERNMENTS:

1. Revenues:

None.

2. Expenditures:

None.

C. DIRECT ECONOMIC IMPACT ON PRIVATE SECTOR:

The bill 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.

D. FISCAL COMMENTS:

None.

III. COMMENTS

A. CONSTITUTIONAL ISSUES:

1. Applicability of Municipality/County Mandates Provision:

Not applicable because this bill does not appear to: require the counties or cities to spend funds or take an action requiring the expenditure of funds; reduce the authority that cities or counties have to raise revenues in the aggregate; or reduce the percentage of a state tax shared with cities or counties.

2. Other:

None.

B. RULE-MAKING AUTHORITY:

None.

C. DRAFTING ISSUES OR OTHER COMMENTS:

None.

IV. AMENDMENTS/COMMITTEE SUBSTITUTE & COMBINED BILL CHANGES

The original version of HB 481 amended the Florida Deceptive and Unfair Trade Practices Act contained within Fla. Stat. Chapter 501 to provide civil penalties for several activities. However, on March 16, 2005, the Committee on Criminal Justice adopted a strike-all amendment and reported the bill favorably with a CS. This amendment removed any reference to Chapter 501.

Further, the original bill amended Fla. Stat. § 817.568 to provide that any person who willfully and without authorization discloses, sells or transfers personal identification information concerning an individual without first obtaining that individual's consent commits a third degree felony. This provision did not require proof of any fraudulent intent in the disclosure of the information and would have prohibited a broad range of common activities. The strike-all amendment removed this language as well.

The amendment also created a new section of statute to require disclosure of a security breach which results in personal information being acquired by an unauthorized person in certain circumstances.

On April 6, 2005, the Business Regulation Committee adopted an amendment changing the language in Section 2 of the bill and reported the amendment favorably with a CS. This amendment made the following changes:

- When a disclosure is required, it must be made without unreasonable delay, and no later than forty-five days following the determination that unencrypted personal information was acquired, or reasonably believed to have been acquired, by an unauthorized person, rather than within thirty days as provided in the original bill.
- 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 ten days of the determination that a breach has occurred, rather than within seventy-two hours as provided in the original bill.
- A clause was added stating that the notification required by this section cannot be delayed by more than ninety days by a law enforcement agency unless an extension is ordered by a court of competent jurisdiction.
- Definitions for “breach” and “person” were added in addition to a clause specifically stating what the term “personal information” does not include.

The staff analysis was updated to reflect both the strike-all amendment and the amendment to Section 2 of the bill.