HOUSE OF REPRESENTATIVES STAFF ANALYSIS

BILL #: HB 129 CS Consumer Protection
SPONSOR(S): Vana and others
TIED BILLS: **IDEN./SIM. BILLS:** SB 284

REFERENCE	ACTION	ANALYST	STAFF DIRECTOR
1) Civil Justice Committee	5 Y, 0 N, w/CS	Billmeier	Billmeier
2) Agriculture Committee	8 Y, 0 N, w/CS	Reese	Reese
3) Governmental Operations Committee	6 Y, 0 N	Williamson	Everhart
4) Justice Appropriations Committee	8 Y, 0 N, w/CS	Sneed	DeBeaugrine
5) Justice Council			

SUMMARY ANALYSIS

HB 129 w/CS makes it a violation of the Florida Deceptive and Unfair Trade Practices Act (FDUTPA) for a person to intentionally use deceptive practices to obtain another person's address, telephone number or social security number and use it to engage in commercial solicitation. Through FDUTPA, a broad range of civil penalties and remedies are available. This bill imposes a civil penalty not to exceed $15,000 for a person who engages in a deceptive and unfair trade practice by fraudulently misrepresenting himself as affiliated with a law enforcement agency, firefighting agency or public utility.

This bill amends s. 817.568, F.S., relating to the criminal use of personal identification information (i.e., identity theft) by broadening the term "personal identification information" to include a postal or e-mail address, telephone number, debit card number, medical records and other information that can be used to access a person's financial resources. Any person who willfully and fraudulently uses, or possesses with intent to use, personal identification information concerning a deceased individual, commits a third degree felony, and may be subject to a 3, 5, or 10 year minimum mandatory sentence depending on the value of the pecuniary benefit, the injury or the number of deceased individuals whose personal identification information is used. The bill creates a new 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 fraud.

HB 129 w/CS reclassifies an identity theft offense in which a person misrepresents himself as a law enforcement officer; employee of a bank, credit card company, credit counseling company, credit reporting agency; or one who seeks to assist a victim with a problem with the victim's credit history. This will result in an increase in the maximum sentence imposed.

This bill creates s. 817.5681, F.S., relating to security breaches of confidential personal information in third-party possession. This section requires 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 affected Florida residents, subject to certain exceptions. The bill imposes a $50,000 fine for failing to disclose a potential security breach that materially compromises the security, confidentiality, or integrity of the information.

This bill places certain restrictions on the accumulating or reporting of consumer's drug test results.

The Criminal Justice Estimating Conference has not yet met to determine the prison bed impact of this bill, However, staff of the Division of Economic and Demographic Research has indicated that this bill will likely have an indeterminate minimal impact.

This bill provides an effective date of July 1, 2005.

FULL ANALYSIS

I. SUBSTANTIVE ANALYSIS

A. HOUSE PRINCIPLES ANALYSIS:

Promote personal responsibility – This bill creates civil penalties against persons who pretend to be affiliated with law enforcement agencies, public utilities, or firefighting agencies. It provides increased civil penalties for persons who violate laws relating to identity theft. The bill requires a business to disclose a security breach which results in personal information being acquired by an unauthorized person in certain circumstances.

Provide limited government – The bill creates new felony offenses.

B. EFFECT OF PROPOSED CHANGES:

Background

The Florida Deceptive and Unfair Trade Practices Act

The Florida Deceptive and Unfair Trade Practices Act (FDUPTA)[1] provides that "unfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful." The FDUTPA provides that it should be construed with "due consideration and great weight… given to the interpretations of the Federal Trade Commission and the federal courts relating to s. 5(a)(1) of the Federal Trade Commission Act, 15 U.S.C. s. 45(a)(1).[2]"

Willful violations occur when the person knew or should have known that his or her conduct was unfair or deceptive[3]. A person willfully violating the provisions of the FDUTPA is liable for a civil penalty of not more than $10,000 per violation[4]. This penalty increases to $15,000 for each violation if the willful violation victimizes or attempts to victimize senior citizens or handicapped persons[5]. Individuals aggrieved by a violation of this act may seek to obtain a declaratory judgment that an act or practice violates this act and to enjoin a person from continuing the deceptive or unfair act[6]. An individual harmed by a person who has violated this act may also seek actual damages from that person, plus attorney's fees and court costs[7]. The state attorneys and the Department of Legal Affairs are the enforcing authorities for the FDUPTA[8] and the act specifies the actions that the enforcing authority may bring[9].

The First District Court of Appeal has described the FDUTPA as follows:

> [The FDUTPA] is designed to protect not only the rights of litigants, but also the rights of the consuming public at large. When addressing a deceptive or unfair trade practice claim, the issue is not whether the plaintiff actually relied on the alleged practice, but whether the practice was likely to deceive a consumer acting reasonably in the same circumstances. A deceptive or unfair trade practice constitutes a somewhat unique tortuous act because, although it is similar

[1] s. 501.201, F.S.
[2] s. 501.204, F.S.
[3] s. 501.2075, F.S.
[4] Id.
[5] s. 501.2077, F.S.
[6] s. 501.211, F.S.
[7] Id.
[8] s. 501.203(3), F.S.
[9] s. 501.207, F.S.

to a claim of fraud, it is different in that, unlike fraud, a party asserting a deceptive trade practice claim need not show actual reliance on the representation or omission at issue.

State Office of Atty. Gen. v. Wyndham Intern, Inc., 869 So. 2d 592, 598 (Fla. 1st DCA 2004)(citing Davis v. Powertel, Inc., 776 So. 2d 971, 974 (Fla. 1st DCA 2000). "An unfair practice under the federal statute has been defined as one that 'offends established public policy' and one that is 'immoral, unethical, oppressive, unscrupulous or substantially injurious to consumers.[10]"

Privacy Protection under Federal Law

Federal law provides some privacy protections to individuals. The Gramm-Leach-Bliley Financial Services Act covers privacy considerations for customers' personal financial information applicable to all financial companies[11]. These laws balance the right to privacy with a financial company's need to provide information for normal business purposes. Companies involved in financial activities must send their customers privacy notices.

The federal act requires financial institutions to provide clear disclosure at the beginning of a customer relationship and not less than annually thereafter, of their privacy policy regarding sharing of nonpublic personal information with affiliates and third parties. The company must disclose how or whether it intends to share personal financial information. The act also gives a person the right to stop (opt out of) some sharing of nonpublic personal information. The act prohibits disclosures of account numbers or credit card account information to third parties for use in telemarketing, direct mail marketing or other marketing through electronic mail and provides criminal penalties. A person has the right to opt out of some information sharing with companies that are part of the same corporate group as the person's financial company (or affiliates), or not part of the same corporate group as the person's financial company (or non-affiliates).

Criminal Use of Personal Identification Information – Identity Theft

S. 817.568, F.S., currently provides that "[a]ny person who willfully and without authorization fraudulently uses, or possesses with intent to fraudulently use, personal identification information[12] concerning an individual without first obtaining that individual's consent, commits" a third degree felony. This offense is commonly known as "identity theft".

Effect of Bill

The bill provides that any person who uses deceptive practices or means to obtain another person's address, telephone number, or social security number and uses it to engage in "commercial solicitation" commits an unfair or deceptive act or practice or unfair method of competition under the FDUTPA. A violator is subject to the civil penalties provided under the FDUTPA. The term "commercial solicitation" is not defined in the bill or in statute.

The bill provides a $15,000 civil penalty per violation for engaging in a deceptive and unfair trade practice with the intent to deceive another person into believing that he or she is affiliated with a law enforcement agency, firefighting agency, or public utility.

---

[10] Samuels v. King Motor Co. of Fort Lauderdale, 782 So. 2d 489, 499 (Fla. 4th DCA 2001)(citations omitted).

[11] 15 U.S.C. ss. 6821-6827

[12] s. 817.568(f), F.S., 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."

Current law provides that a person using personal identification information, such as social security numbers, driver's license numbers, passport numbers, and credit card numbers, for fraudulent purposes, commits a third degree felony, punishable by up to 5 years in prison[13]. The bill creates a new and unnumbered section providing that a person who violates or fails to comply with any provision of s. 817.568, F.S., commits an unfair or deceptive act or practice or unfair method of competition in violation of the FDUTPA. A violator would be subject to civil penalties under the FDUTPA in addition to the criminal penalties.

Current law makes violations of certain federal laws and Federal Trade Commission rules a violation of the FDUTPA[14]; however, current statutes only reference federal laws and rules as of July 1, 2001. This bill updates the year to 2005 in various provisions of the FDUTPA in order to capture within the act any changes in relevant rules or statutes made between 2001 and 2005.

The bill provides a broad range of remedies that the court can grant to accomplish the purposes of the act. It permits the court to enter orders to appoint receivers, freeze assets, reimburse consumers or government entities, to limit the application of contracts to avoid unconscionable results, to order a defendant to divest itself of any interest in any enterprise, to impose restrictions on future activities, or grant "legal, equitable, or other appropriate relief." The bill permits the court to enter orders "to bring actions in the name of and on behalf of the defendant enterprise." This change will allow courts to enter orders permitting receivers to bring actions in the name of a defendant enterprise.

This bill amends s. 817.568, F.S., providing the following enhanced penalties for "identity theft":

- 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 harassment[15] by use of personal identification information as well as using a public record to commit identity theft[16]. Further, the section provides penalties if identity theft is committed using the personal identification information of an individual less than 18 years of age[17].

CS/HB 129 amends the definition of the term "personal identification information" to include: a postal or email 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.

[13] s. 817.568, F.S.
[14] See e.g. s. 501.203(3), F.S.
[15] 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. s. 817.568(1)(c) (2004).
[16] s. 817.568(4) and (5), F.S.
[17] 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.[18]

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:

- A misdemeanor is reclassified to a third degree felony.
- A third degree felony is reclassified to a second degree felony.
- A second degree felony is reclassified to a first degree felony.
- A first degree felony 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 s. 817.5681, F.S., 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 believed to have been acquired, by an unauthorized person and the acquired information materially compromises the security, confidentiality, or integrity of personal information.

[18] 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."

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

This bill contains a severability clause, and a July 1, 2005 effective date.

C. SECTION DIRECTORY:

Section 1. Creates s. 501.165, F.S., relating to obtaining personal information for commercial solicitation.

Section 2. Amends s. 501.2075, F.S., providing an exception to a civil penalty.

Section 3. Creates s. 501.2076, F.S., relating to misrepresenting one’s affiliation with a law enforcement agency, firefighter agency, or public utility.

Section 4. Provides that a violation of s. 817.568, F.S., is also a violation of ch. 501, part II, F.S.

Section 5 and 6. Amends ss. 501.203 and 501.204, F.S., updating obsolete dates.

Section 7. Amends s. 501.207, F.S., allowing the court to enter orders to bring actions on behalf of a defendant enterprise.

Section 8 and 9. Amends s. 817.568 and creates s. 817.5681, F.S., relating to the criminal use of personal identification information or confidential personal information.

Section 10. Places certain restrictions on accumulating or reporting a consumer’s drug test results.

Section 11. Provides a severability clause.

Section 12. Provides an effective date of July 1, 2005.

II. FISCAL ANALYSIS & ECONOMIC IMPACT STATEMENT

A. FISCAL IMPACT ON STATE GOVERNMENT:

1. Revenues:

   This bill could generate additional revenue in fines and civil penalties, but the amount is indeterminate.

2. Expenditures:

   The bill also specifies violations relating to the FDUTPA that may be enforced by the Attorney General or the state attorneys. The cost is indeterminate because the number of cases that may arise is unknown. Another cost of this bill may involve the impact of the enhanced criminal penalties. The Criminal Justice Estimating Conference has not yet met to determine the prison bed impact of this bill on the Department of Corrections. However, staff from the Division of Economic and Demographic Research has determined that due to the relatively small number of expected offenses, HB 129 w/CS would have an indeterminate minimal prison bed impact.

B. FISCAL IMPACT ON LOCAL GOVERNMENTS:

1. Revenues:

   None.

2. Expenditures:

   There appears to be no expected fiscal impact for local government.

C. DIRECT ECONOMIC IMPACT ON PRIVATE SECTOR:

There appears to be no expected fiscal impact for the private sector.

D. FISCAL COMMENTS:

None.

III. COMMENTS

A. CONSTITUTIONAL ISSUES:

1. Applicability of Municipality/County Mandates Provision:

   This bill does not require counties or municipalities to take an action requiring the expenditure of funds, does not reduce the authority that counties or municipalities have to raise revenue in the aggregate, and does not reduce the percentage of state tax shared with counties or municipalities.

2. Other:

   None.

B. RULE-MAKING AUTHORITY:

None.

C. DRAFTING ISSUES OR OTHER COMMENTS:

None.

IV. AMENDMENTS/COMMITTEE SUBSTITUTE & COMBINED BILL CHANGES

Civil Justice Committee
The Civil Justice Committee considered the bill on February 9, 2005. The committee adopted an amendment to permit transfers of personal information if the third party agrees to abide by the transferring entity's privacy policy. It provided that a person or entity can transfer personal information for the purpose of allowing a third party to make commercial solicitations on behalf of the transferring person or entity. The bill was reported favorably as a committee substitute.

Agriculture Committee
On March 16, 2005, the Agriculture Committee adopted a "strike all" amendment to conform HB 129 w/CS to its Senate companion, SB 284. Section 501.166, F.S., is created to prohibit the sale or transfer of personal customer information to a third party if the information is protected from disclosure by law, contract, or a published privacy policy, unless the purchaser or transferee agrees to abide by the contract or published privacy policy. The prohibition applies to any customer who resides in this state at the time of the sale or transfer. The bill was reported favorably as a committee substitute.

Justice Appropriations Committee
On April 15, 2005, the Justice Appropriations Committee adopted two amendments.

The first one was a "strike all" amendment. The amendment removed all references to s. 501.166 and s 501.167, F.S., relating to computerized information and amended s. 501.2077, F.S. by adding provisions for unfair or deceptive practices that affect handicapped persons or certain senior citizens. It also amended ss. 817.568 and 817.5681, F.S., by clarifying definitions relating to "personal identification information", created additional criminal offenses and provided minimum mandatory prison sentences and/or fines for violations, and authorized the Department of Legal Affairs to institute certain proceedings involving fines. In addition, the amendment placed certain restrictions on accumulating and reporting consumer drug test results.

The second amendment removed the provisions in the "strike all" amendment amending s. 501.2077, F.S., related to unfair or deceptive practices against handicapped persons or senior citizens.

The bill was reported favorably as a committee substitute.