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 284
SPONSOR:	Judiciary Committee, Senator Aronberg and others
SUBJECT:	Consumer Protection
DATE:	April 15, 2005 REVISED:

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

I. Summary:

Committee Substitute for Senate Bill 284 prohibits the use of deceptive practices or means to obtain certain personal information for commercial solicitation purposes. In addition, the committee substitute revises the Florida Deceptive and Unfair Trade Practices Act (FDUTPA or the "act") to provide the following:

- Creates a section making it a violation of the act to falsely represent oneself as being affiliated with law enforcement, a firefighting agency, or public utility for the purpose of engaging in a deceptive and unfair trade practice, and an increased penalty is provided for this action;[1]
- Updates provisions of the act from the year 2001 to the year 2005 to capture within the act any changes in Federal Trade Commission (FTC) rules and associated interpretations, changes in statutes, rules, regulations, ordinances, and decisions in federal courts; and
- Makes it an unfair and deceptive act to cause handicapped persons or certain senior citizens over the age of 70 to waive their right to a jury trial or to waive or limit their right to any benefit or protection conferred on them.

The committee substitute requires a person who maintains computerized personal identification information to disclose a breach of security of the system if personal identification information is believed to have been acquired by an unauthorized individual. In addition, the proposed language requires a person who maintains computerized personal identification information for another

[1] Proposed s. 501.2076, F.S., would increase the maximum civil penalty for this violation to $15,000, while current s. 501.2075, F.S., provides a maximum civil penalty of $10,000 for a violation of part II, ch. 501, F.S.

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.

The committee substitute provides that the criminal use of personal identification information in violation of s. 817.568, F.S., is also a violation of the FDUTPA, which would allow a victim of identity theft to bring a civil action *or* a state attorney or the Department of Legal Affairs to bring a civil action on behalf of the victim.

The committee substitute 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 10-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.

This committee substitute creates an unnumbered section of the Florida Statutes, and creates the following sections of the Florida Statutes: 501.165, 501.167, and 501.2076. This committee substitute amends the following sections of the Florida Statutes: 501.203, 501.204, 501.207, 501.2075, 501.2077, and 817.568.

II. Present Situation:

Consumer Protection

Part I of ch. 501, F.S., prohibits certain acts that may bring harm to Florida consumers, such as tampering with consumer goods,[2] and regulates various industries that directly interact with consumers, such as telemarketers[3] and health studios.[4] Part II of ch. 501, F.S., the Florida Deceptive and Unfair Trade Practices Act (FDUTPA), provides remedies and penalties for "[u]nfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce."[5] Remedies for acts prohibited by FDUTPA may include an action to enjoin a person from committing such acts[6] as well as the

[2] s. 501.001, F.S.
[3] s. 501.059, F.S
[4] ss. 501.012-510.519, F.S.
[5] s. 501.204, F.S.
[6] s. 501.207(1)(b), F.S.

imposition of a civil penalty of not more than $10,000.[7] For violations involving senior citizens over age 60 or handicapped persons, the penalty for a violation under FDUTPA is increased to $15,000 per violation.[8] Actions for violation under this part may be brought by a state attorney or the Department of Legal Affairs[9] or by a consumer.[10]

It is also the public policy of this state to protect the public from those impersonating certain public officers. It is a third-degree felony if any person "deliberately impersonates or falsely acts as a public officer or tribunal, public employee or utility employee, including, but not limited to, marshals, judges, prosecutors, sheriffs, deputies, court personnel, or any law enforcement authority in connection with or relating to any legal process affecting persons and property, or otherwise takes any action under color of law against persons or property."[11] It is also a third-degree felony if any person "falsely assumes or pretends to be the State Fire Marshal, an agent of the Division of State Fire Marshal, a firefighter as defined in s. 112.81, F.S., or a firesafety inspector and … acts as such to require a person to aid or assist him or her in any matter relating to the duties of the State Fire Marshal, an agent of the division, a firefighter, or a firesafety inspector."[12]

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[13] 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

[7] s. 501.2075, F.S.
[8] s. 501.2077, F.S.
[9] s. 501.207, F.S.
[10] s. 501.211, F.S.
[11] s. 843.0855(2), F.S.
[12] s. 633.151, F.S.
[13] 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.

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

Federal Consumer Protection and Privacy Laws

Federal law provides some privacy protections to individuals. The Gramm-Leach-Bliley Act covers privacy considerations for consumers' personal financial information. Companies involved in financial activities must send their customers privacy notices, including such companies as:[17]

- Banks, savings and loans, and credit unions;
- Insurance companies;
- Securities and commodities brokerage firms;
- Retailers that directly issue their own credit cards;
- Mortgage brokers;
- Automobile dealerships that extend or arrange financing or leasing;
- Check cashers and payday lenders;
- Financial advisors and credit counseling services; and
- Sellers of money orders or travelers checks.

The company must disclose whether, and if so how, it intends to share personal financial information. Federal privacy laws also give a person the right to opt-out of some sharing of personal financial information with companies that are part of the same corporate group as the financial company (or affiliates) or not part of the same corporate group as your financial company (or non-affiliates).

A person, however, cannot opt-out and completely stop the flow of all personal financial information. The law permits financial companies to share certain information without giving the person the right to opt-out where the companies need to provide information for normal business purposes. The financial company may provide to non-affiliates: information to firms that help promote and market that company's products, records of transactions to firms that provide data processing and mailing services for the company, information in response to a court order, and payment history on loans and credit cards to credit bureaus.[18]

---

[14] 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.
[15] s. 817.568(4) and (5), F.S.
[16] s. 817.568(6) and (7), F.S.
[17] "Privacy Choices for Your Personal Financial Information," Federal Trade Commission, *available at* http://www.ftc.gov/bcp/conline/pubs/credit/privchoices.htm.
[18] *Id.*

Florida Consumer Protection and Privacy Laws

The Florida Constitution provides a right to privacy solely from governmental intrusion.[19] The privacy of an insurance consumer's nonpublic personal financial and health information is protected by rules based on the Privacy of Consumer Financial and Health Information Regulation, adopted September 26, 2000, by the National Association of Insurance Commissioners and adopted by the Florida Department of Insurance, now the Florida Department of Financial Services (DFS).[20] These rules must be consistent with, and not more restrictive than, the standards contained in Title V of the Gramm-Leach-Bliley Act of 1999. The rules adopted by DFS describe an insurance company's privacy obligation to the consumer and how the consumer may opt-out of certain disclosures by an insurance company to affiliated and non-affiliated third parties, but it does not address the sale or transfer of the nonpublic personal financial and health information.[21]

Disclosure of Breach of Security

There is currently no provision in the Florida Statutes that requires a person that 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.

III. Effect of Proposed Changes:

Consumer Protection

Committee Substitute for Senate Bill 284 provides that any person who intentionally uses a deceptive practice or means to obtain another person's address, telephone number, or social security number and uses it to engage in commercial solicitation, or provides it to another person for purposes of commercial solicitation, commits an unfair or deceptive act or practice or unfair method of competition in violation of part II of ch. 501, F.S., which is the Florida Deceptive and Unfair Trade Practices Act (FDUTPA or the "act").

The committee substitute creates a provision to prescribe that falsely representing oneself as being affiliated with law enforcement, a firefighting agency, or public utility for the purpose of engaging in a deceptive and unfair trade practice is a violation of the FDUTPA.[22] Currently, the maximum civil penalty for most violations under the act is $10,000, but the committee substitute creates an exception to this general cap and provides that the maximum civil penalty for this particular violation is $15,000.

An increased maximum civil penalty of $15,000 for violations under the act is already present in s. 501.2077, F.S., relating to violations of FDUTPA where the victim is 60 years old or older or handicapped. The committee substitute adds to existing law to provide that it is a violation of FDUTPA to cause an elderly person over the age of 70, and whose ability to perform normal activities of daily living is impaired, or a handicapped person to waive that person's right to a

[19] s. 23, Art. I, State Constitution.
[20] s. 626.9651, F.S.
[21] chs. 4-128, F.A.C., Privacy of Consumer Financial and Health Information.
[22] Proposed s. 501.2076, F.S.

jury trial or to waive or limit that person's right to any befit or protection conferred on that person.[23]

The proposed language provides an unnumbered section that would make any violation of s. 817.568, F.S., relating to criminal use of personal identification information, a violation of the FDUTPA. By enacting this provision, the committee substitute would allow a victim of identity theft *or* a state attorney or the Department of Legal Affairs, on behalf of a victim, to bring a civil action against a defendant.

Current law provides that a court may order a number of different actions upon motion of an enforcing authority or an interested party to an action brought under s. 501.207, F.S. The committee substitute would add language to subsection (3) regarding the court's appointment of a general or special magistrate or receiver in a bankruptcy and the court's authority to enter orders with respect to the appointee's ability "to bring actions in the name of and on behalf of the defendant enterprise," thereby allowing receivers to bring actions against other companies that may be involved in an unfair trade practice.

The committee substitute updates provisions of the FDUTPA with the year "2005" to capture within the act any changes made between 2001 and 2005 in any Federal Trade Commission (FTC) rules, any court or FTC interpretations regarding the standards of unfairness and deception, or any changes in law, statute, rule, regulation, or ordinance which proscribe unfair methods of competition, or unfair, deceptive, or unconscionable acts or practices.[24]

Disclosure of Breach of Security

The committee substitute creates s. 501.167, 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. Disclosure must be made in the "most expedient time possible" and without unreasonable delay, but the committee substitute does not specify exact time frames for disclosure.[25] Further, the committee substitute provides that any person who 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, if the personal information is reasonably believed to have been acquired by an unauthorized person. Notification of affected individuals may be delayed if law enforcement officials determine that notification will impede a criminal investigation.

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 and allows a person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information to follow its own procedures as long as they are consistent with the requirements of the proposed language.

[23] Proposed s. 501.2077(3), F.S.
[24] Amended sections include ss. 501.203(3) and 501.204(2), F.S.
[25] Page 3, lines 30-31.

Additionally, the committee substitute provides for exceptions to notification after an investigation reveals no harm has resulted from the breach of security, for notification of consumer reporting agencies, and for a violation under this section to be a violation of FDUTPA.

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.[26] 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 court 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 court 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 court must impose of a 10-year minimum mandatory sentence.[27]

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.[28]

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

[26] Proposed s. 817.568(8)(a), F.S.
[27] Proposed s. 817.568(8)(b)-(c), F.S.
[28] Page 13, lines 13-18, provides 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."

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 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.

The committee substitute also provides a severability clause, providing that if any provision of the act is held invalid, the invalidity shall not affect other provisions of the act.

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. 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:

The committee substitute specifies that violations under 817.568, F.S., would now also be violations under the Florida Deceptive and Unfair Trade Practices Act (FDUTPA). This would allow the Attorney General or the state attorneys to enforce violations of identity theft under FDUTPA. A projected financial impact resulting from the prosecution of these violations has not been determined because the number of cases that may arise is unknown.

VI. Technical Deficiencies:

None.

VII. Related Issues:

The committee substitute provides that any person who violates the identity theft statute, s. 817.568, F.S., commits a deceptive and unfair trade practice in violation of part II of ch. 501, F.S., and is subject to the penalties and remedies available for the violation. However, part II of ch. 501, F.S., applies to unfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices *in the conduct of any trade or commerce*. Trade or commerce is defined to apply to acts relating to the advertising, soliciting, providing, offering, or distributing of any good or service. Generally, the Florida Deceptive and Unfair Trade Practices Act are used to penalize business entities for deceptive activities. As a result, it is not clear that violation of a statute which prohibits identity theft, which would not be related to the advertising, soliciting, providing, offering, or distributing of a good or service and would not be committed by a business entity, would fit in the overall scope of the act. It does not appear that every offense of identity theft could be categorized as a deceptive and unfair trade practice.

VIII. Summary of Amendments:

None.