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/SB 1580

SPONSOR: Banking and Insurance Committee and Senator Aronberg and others

SUBJECT: Consumer Protection

DATE: April 3, 2003 REVISED: _____ _____ _____ _____

	ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
1.	Johnson	Deffenbaugh	BI	Favorable/CS
2.			CJ	
3.			ACJ	
4.			AP	
5.			RC	
6.				

I. Summary:

The committee substitute provides greater protections for consumers by creating penalties and remedies for certain deceptive or unfair trade acts under the Florida Deceptive and Unfair Trade Practices Act. The committee substitute provides that the following activities are violations under the act:

- Engaging in a deceptive and unfair trade practice with the intent deceive to deceive others in believing that they are affiliated with a law enforcement agency, firefighting agency, or public utility;
- Using deceptive practices to obtain personal information to engage in commercial solicitation;
- Selling or transferring any database that contains personal customer information of a bankrupt person if the bankrupt person, through contract or published privacy policy, agreed or stated that such information would not be disclosed; and
- Violating or failing to comply with the identity theft provisions under s. 817.568, F.S.

This bill creates the following sections of the Florida Statutes: 501.165, 501.166, and 501.2076. The bill amends section 501.2075 of the Florida Statutes.

II. Present Situation:

Identity Theft and Fraud

In recent years, the Internet marketplace has been growing at a phenomenal rate. Advances in technology have enhanced the capacity of online companies to collect, store, transfer, and

analyze vast amounts of data from and about the consumers who visit their web sites. This increase in the collection and use of data has raised public awareness and consumer concerns about online privacy. Consumer concerns about privacy include the misuse of information, including the risk of identity theft and unwanted intrusions in their daily lives. The Internet has become an appealing place for criminals to obtain personal identifying data, such as passwords, or even banking or other financial information for consumers, since many consumers conduct business transactions via the Internet.

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.[1] The number one complaint received was identity theft (43 percent). 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). 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).

The U.S. Department of Justice prosecutes cases of identity theft and fraud under a variety of federal statutes, including the Identity Theft and Assumption Deterrence Act of 1998.[2] This act provides that it is a federal crime to knowingly transfer or use, without lawful authority, a means of identification of another person with the intent to commit any unlawful activity that constitutes a violation of federal law or any applicable state law. Schemes to commit identity theft or fraud may also involve violations of other statutes, such as identification fraud, credit card fraud, computer fraud, mail fraud, wire fraud, or financial institution fraud.

According to the National Conference of State Legislators, 45 states, including Florida, have enacted laws to address identity theft. Section 817.568, F.S., provides criminal penalties for the criminal use of personal identification information.

"Pretexting" is the practice of obtaining personal financial information by fraud. For a price, an "information broker" or "pretexter" will call banks and other financial institutions under the pretext of being a customer to obtain the customer's account numbers and balances, as well as other personal information. Since the provisions of the Gramm-Leach Bliley Act outlawing "pretexting" went into effect in 1999, the Federal Trade Commission has increased its enforcement efforts to stop the misuse of sensitive financial information.[3] The act provides for civil remedies to be enforced by the FTC, and for criminal penalties enforced by the Department of Justice in cases where the "pretexter" knowingly or intentionally violated or attempted to violate the law.

Federal and State Privacy Laws

- 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. These laws balance the right to privacy

[1] *National and State Trends in Fraud and Identity Theft/January-December 2002* (Last updated January 1, 2003).
[2] 18 U.S.C 1028.
[3] 15 U.S.C sections 6821-6827.

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 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 your 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. Among other things, the financial company can provide to non-affiliates:

- Information about you to firms that help promote and market the company's own products or products offered under a joint agreement between two financial companies;
- Records of your transactions – such as your loan payments, credit card or debit card purchases, and checking and savings account statements – to firms that provide data processing and mailing services for your company;
- Information about you in response to a court order; and
- Your payment history on loans and credit cards to credit bureaus.[4]

Section 626.9651, F.S., provides that the privacy of a consumer's nonpublic personal financial and health information is protected by rules based on the Privacy of Consumer Financial and Health Information Model Regulation, adopted September 26, 2000, by the National Association of Insurance Commissioners (NAIC) and adopted by the Department of Insurance, now the Florida Department of Financial Services. 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 the department delineate an insurer'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.[5] According to the NAIC, 36 states have enacted laws or rules to meet the privacy standards of the Gramm-Leach-Bliley Act. The NAIC Insurance Information Privacy Protection Model Regulation establishes an affirmative consent for the disclosure of insurance consumers' personal information, including financial and health information.

[4] *Id.*
[5] Chapter 4-128, F.A.C., Privacy of Consumer Financial and Health Information.

Bankruptcy and the Sale or Transfer of Customer Information

The Federal Bankruptcy Code is codified in Title 11 of the United States Code. The word "person" is specifically defined and includes an individual, partnership, or corporation.[6] Four of the code's principal chapters (7, 11, 12, and 13) are briefly outlined below:

- Chapter 7 bankruptcy is a liquidation proceeding available to consumers and businesses. The debtor's assets that are not exempt from creditors are collected and liquidated (reduced to money), and the proceeds are distributed to creditors. A consumer debtor receives a complete discharge from debt under Chapter 7, except for certain debts that are prohibited from discharge by the Bankruptcy Code.
- Chapter 11 bankruptcy provides a procedure by which an individual or a business can reorganize its debts while continuing to operate. The vast majority of Chapter 11 cases are filed by businesses. The debtor, often with participation from creditors, creates a plan to repay part or all of its debts.
- Chapter 12 allows a family farmer to file for bankruptcy, reorganize the farm's business affairs, repay all or part of the farm's debts, and continue operating.
- Chapter 13, often called wage-earner bankruptcy, is used primarily by individual consumers to reorganize their financial affairs under a repayment plan that must be completed within 3 or 5 years. To be eligible for Chapter 13 relief, a consumer must have regular income and may not have more than a certain amount of debt, as set forth in the Bankruptcy Code.[7]

Florida law defines "person" to include, among other things, individuals, partnerships, estates, trusts, corporations, and all other groups or combinations.[8] Florida has several provisions found in ch. 222, F.S., addressing specific exemptions from a bankruptcy proceeding, including the homestead, personal property, and wages.[9] An additional bankruptcy provision is found in s. 55.145, F.S., which describes how a debtor may petition the court to have the bankruptcy discharged.

Sale or Transfer of Customer Information

The enforcement of privacy policies in a bankruptcy proceeding is a growing concern with federal and state regulators. Companies that promise confidentiality may decide to sell or transfer personal information they have collected. Toysmart, a failed Internet retailer of children toys, collected detailed personal information about its visitors, including name, address, billing information, shopping preference, and family profiles. Toysmart posted a privacy policy at its website which stated that information collected from customers would never be shared with third parties. In May 2000, Toysmart announced it was closing its operations and selling its assets. The Federal Trade Commission discovered that Toysmart was offering its customer list for sale in violation of its own privacy policy. The FTC alleged that Toysmart engaged in deceptive acts

[6] 11 U.S.C. s. 101(41).
[7] United States Trustee Program, Bankruptcy Fact Sheets & Consumer Notices, *Overview of Bankruptcy Chapters*, *available at* http://www.usdoj.gov/ust/pdfs/fs01.pdf.
[8] Section 1.01(3), F.S.
[9] Section 222.01, F.S., Designation of homestead by owner before levy; s. 222.061, F.S., Method of exempting personal property; inventory; s. 222.11, F.S., Exemption of wages from garnishment.

or practices in violation of Section 5 of the Federal Trade Commission Act by disclosing, selling, or offering for sale personal customer information, contrary to the terms of its privacy policy that personal information would never be disclosed to third parties.

On July 10, 2000, the FTC entered into a stipulated consent agreement and final order with Toysmart that prohibited the company from selling the customer list as a stand-alone asset. The settlement only allows a sale of such assets as a package that includes the entire web site, and only to a qualified buyer that agrees to abide by the terms of Toysmart's privacy statement. A qualified buyer is defined to mean a business entity that is in a related market and that expressly agrees to be Toysmart's successor-in-interest as to customer information. In the event the buyer wants to change the privacy policy, the buyer must provide notice to consumers and obtain their affirmative consent (opt-in) to the new use of the customer information. If the bankruptcy court does not approve the sale of Toysmart's customer information to a qualified buyer or approve a reorganization plan, Toysmart is ordered to delete or destroy all customer information.

Florida Deceptive and Unfair Trade Practices Act

Part II of ch. 501, F.S., is the Florida Deceptive and Unfair Trade Practices Act. One of the purposes of the Act is to protect the consuming public and legitimate business enterprises from those who engage in unfair methods of competition, or unconscionable, deceptive, or unfair acts or practices in the conduct of any trade or commerce. [10] The act is also intended to make state consumer protection and enforcement consistent with established policies of federal law relating to consumer protection. The state attorneys and the Department of Legal Affairs are the enforcing authorities. Section 501.207, F.S., specifies the actions that the enforcing authority may bring.

Section 501.204, F.S., declares unfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce unlawful. Willful violations occur when the person knew or should have known that his or her conduct was unfair or deceptive.[11] A person willfully violating the provisions of this act is liable for a civil penalty of not more than $10,000 per violation. This penalty is increased to $15,000 for each violation if the willful violation victimizes or attempts to victimize senior citizens or handicapped persons. 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. 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.[12]

III. Effect of Proposed Changes:

Section 1 creates s. 501.2076., F.S., relating to misrepresentation. The section would subject a person who engages in a deceptive and unfair trace practice with the intent to deceive another person into believing that he or she is affiliated with a law enforcement agency, firefighter agency, or public utility is subject to a civil penalty not to exceed $15,000 for each violation.

[10] Section 501.202(2), F.S.
[11] Section 501.2075, F.S.
[12] Section 501.211(1) and (2), F.S.

Section 2 creates s. 501.165, F.S., to provide 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 in violation of part II of ch. 501, F.S., and is subject to the penalties and remedies provided for such violation, in addition to remedies otherwise available for such conduct.

Section 3 provides an exception to s. 501.2075, F.S., regarding the maximum penalty of $10,000 allowable per violation under part II of ch. 501, F.S., to provide that violations of s. 501.2076, F.S., are not subject to this limitation. As noted in section 1 above, these violations are subject to a penalty of up to $15,000 per violation.

Section 4 creates s. 501.166, F.S., which prohibits a person who files for bankruptcy from selling or otherwise transferring to another any database that contains personal customer information if the bankrupt person, through contract or written privacy policy, agreed or stated that such personal customer information would not be disclosed.

Section 5 provides 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 part II of ch. 501, F.S., and is subject to the penalties and remedies provided for such violation, in addition to remedies otherwise available for such conduct.

Section 6 provides that this act shall take effect July 1, 2003.

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 bill provides greater protections for consumers relating to the privacy of personal customer information and deceptive solicitation practices and provides penalties for persons engaging in committing unfair or deceptive acts.

C. Government Sector Impact:

None.

VI. Technical Deficiencies:

None.

VII. Related Issues:

Section 4 of the bill, relating to the prohibition of selling or transferring to another any database that contains personal customer information if the bankrupt person, through contract or written privacy policy, agreed or stated that such personal customer information would not be disclosed does not address other potential parties in a bankruptcy proceeding, including a successor, assignee, or trustee, receiver, or representative of the bankrupt person. The application of this provision to companies that are not based in Florida with Florida-based residents could be problematic.

As written, the bill would not allow a bankruptcy court to sale or transfer such a database in any circumstances. This prohibition could prevent a business from reorganizing under the Bankruptcy Code. If the intent of the provision is to prevent disclosure of such information, the language could be revised to allow a sale or transfer to a business entity that is in a related market and agrees to be the successor in interest as to customer information, as in the Toysmart case.

VIII. Amendments:

None.