STORAGE NAME: h1845a.cpcs.doc
DATE: April 12, 2001

HOUSE OF REPRESENTATIVES
AS REVISED BY THE COMMITTEE ON
CRIME PREVENTION, CORRECTIONS & SAFETY
ANALYSIS

BILL #: HB 1845 (PCB IT 01-01)

RELATING TO: Improper use of personal identification information

SPONSOR(S): Committee on Information Technology

TIED BILL(S):

ORIGINATING COMMITTEE(S)/COUNCIL(S)/COMMITTEE(S) OF REFERENCE:

(1) INFORMATION TECHNOLOGY YEAS 10 NAYS 0
(2) CRIME PREVENTION, CORRECTIONS & SAFETY YEAS 5 NAYS 0
(3) COUNCIL FOR READY INFRASTRUCTURE
(4)
(5)

I. SUMMARY:

Florida recently passed a law creating criminal penalties for identity theft that is codified at s. 817.568, F.S. After conducting hearings across the state concerning the problem of identity theft, the Privacy and Technology Task Force has recommended that changes be made to the existing law to further its goals.

HB 1845 implements many of the recommendations of the Task Force related to identity theft under s. 817.568. The bill revises existing statutory definitions to expand the scope of protection from identity thieves. The bill creates three distinct offenses: obtaining or using personal identification information without authorization; harassment by use of personal identification; and fraudulent use of personal identification information. Additionally, the bill provides for heightened penalties when a defendant unlawfully uses public record information to commit an identity theft crime.

To assist victims in recovering the losses they sustain from criminal use of their personal identification information, the bill enhances the power of the sentencing court to order restitution from identity thieves and to order the correction of records altered by or as a result of such crimes.

Because of the technical nature of the crime, prosecution of identity theft has proven difficult. To make it easier for law enforcement agencies to prosecute identity thefts, the bill would allow prosecutions to be commenced in the county of residence of the victim or in any county where an element of the crime occurred. Additionally, the statute of limitations for violations of s. 817.568 would be extended to five years for all offenses, and up to eight years for fraudulent use of personal identification information.

The Committee on Crime Prevention, Corrections & Safety adopted a strike-everything amendment which is traveling with the bill. See amendment section for details.

II. SUBSTANTIVE ANALYSIS:

A. DOES THE BILL SUPPORT THE FOLLOWING PRINCIPLES:

1.	Less Government	Yes []	No [X]	N/A []
2.	Lower Taxes	Yes []	No []	N/A [x]
3.	Individual Freedom	Yes []	No []	N/A [x]
4.	Personal Responsibility	Yes [X]	No []	N/A []
5.	Family Empowerment	Yes [X]	No []	N/A []

For any principle that received a "no" above, please explain:

The bill may increase the burdens on, and costs of operating, the criminal justice system due to increased prosecutions. Additionally, investigating this type of technology-based crime may require additional training and expertise by law enforcement officers.

B. PRESENT SITUATION:

The rapid expansion of electronic commerce has made obtaining and using personal identification information without authorization for improper purposes a more common occurrence. Such acts are commonly referred to as "identity theft." Identity theft occurs when a person "uses the identifying information of another person – name, social security number, mother's maiden name, or other personal information – to commit fraud or engage in other unlawful activities."[1] When the identity thief fails to pay unlawfully incurred debts, the debt is reported on the victim's credit report.[2] Recent surveys indicate that identity theft is one of the fastest growing crimes in America, affecting nearly half a million victims in 1998 and potentially more than 750,000 victims this year.[3] Florida ranks third, behind California and New York, in complaints of identity theft reported to the Federal Trade Commission.[4]

Identity theft can cause significant economic harm to both the victim and the victim's creditors. Approximately 54% of victims reported credit card fraud, and 26% reported that an identity thief opened up telephone, cellular or other utility services in the victim's name.[5] Bank fraud and fraudulent loans accounted for approximately 27% of identity theft reports. Many instances of identity theft occur without the use of sophisticated technologies. For instance, "dumpster divers" may dig through a person's garbage to obtain credit card receipts, utility bills, or other discarded

---

[1] *Prepared Statement of the Federal Trade Commission on Financial Identity Theft Before the Subcomm. on Telecommunications, Trade and Consumer Protection and the Subcomm. on Finance and Hazardous Materials of the House of Representatives Committee on Commerce*, 105th Cong. 1 (1999) (Statement of Jodie Bernstein, Director of the Bureau of Consumer Protection, Federal Trade Commission), *available at* http://www.ftc.gov/os/1999/9904/identitythefttestimony.htm (last visited February 28, 2001) (hereinafter "FTC Identity Theft Testimony").
[2] *See id.*
[3] *See* Executive Summary of Policy Recommendations, Privacy and Technology Task Force 2 (Feb. 2001) *available at* http://www.myflorida.com/myflorida/government/learn/pttf/index.html (last visited February 28, 2001) (hereinafter "Task Force Executive Summary").
[4] *See id.*
[5] *See id.*

documents that reveal personal identification information. Use of computers and other sophisticated technologies has made identity theft easier and more anonymous.[6]

In response to the surge of instances of identity theft, Congress passed the Identity Theft and Assumption Deterrence Act of 1998.[7] This act served two main purposes: to strengthen criminal penalties governing identity theft and to improve victim assistance. Federal law now criminalizes fraud in connection with the theft and unlawful use of personal information regardless of whether the thief actually uses the information.[8] If a thief then uses the unlawfully obtained information to obtain anything of value totaling more than $1,000 during a one-year period, the thief is subject to a fine or up to 15 years of imprisonment.[9] If the $1,000 threshold is not met, the maximum penalty is three years of imprisonment.[10] The criminal provisions are enforced by the U.S. Department of Justice with cooperation from the Secret Service, the FBI and the U.S. Postal Inspection Service. Attempts or conspiracies to commit these offenses are punishable in the same manner.[11]

In addition to the federal laws, 27 states enacted identity theft legislation in 1999 and 10 states enacted legislation in 2000.[12]

Florida Identity Theft Statutes

In 1999, Florida enacted identity protection legislation that is now codified at s. 817.568, F.S.[13] Section 817.568 creates two crimes: fraudulent use of personal identification information and harassment by use of personal identification information. The term "personal identification information" is defined 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;

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 number or;

4. Telecommunication identifying information or access device.

"Fraudulent use of personal identification information" is committed when a person willfully and without authorization fraudulently uses, or possesses with intent to use, personal identification information concerning an individual without first obtaining that individual's consent. s. 817.568(2), F.S. The offense is a third-degree felony, punishable by a fine of up to $5,000 and five years imprisonment.

---

[6] *See* FTC Identity Theft Testimony at 2. In a practice called "skimming," identity thieves use computers to read and store the magnetic strip of ATM or credit cards. Once that information is stored, it can then be re-encoded on another card.
[7] Pub. L. No 105-318, 112 Stat. 3007 (1998).
[8] *See* 18 U.S.C. § 1028 (a)(7) (2000).
[9] *See id.* at § 1028 (b)(1)(D).
[10] *See id.* at § 1028 (b)(2)(B).
[11] *See id.* at § 1028 (f).
[12] *See, e.g.*, CAL. PENAL CODE § 530.6, § 530.7 (West 2000); 720 ILL. COMP. STAT. 5/16G-15 (West 2000); IOWA CODE § 715A.8 (2000); KY. REV. STAT. ANN. § 411.210, § 514.160, § 514.170, § 532.034 (Banks-Baldwin 2000); N.J. STAT. ANN. § 2C:21-17 (West 2000).
[13] *See* 1999 Fla. Laws ch. 1999-335 (codified at FLA. STAT. § 817.568 (2000)).

"Harassment by use of personal information" is committed when a person "willfully and without authorization possesses, uses, or attempts to use personal identification information concerning an individual without first obtaining that individual's consent, and who does so for the purpose of harassing that individual." s. 817.568 (3) F.S. Thus, in order to commit the prohibited act, a person must specifically intend to harass the individual whose personal information he or she obtained. This offense is a first-degree misdemeanor, punishable by a fine of up to $1,000 and one year of imprisonment.

This section further provides that, when sentencing a defendant, a court may order the defendant to make restitution to "any victim of the offense". s. 817.568(5), F.S. The term "victim" is defined in the restitution statute as "any person who suffers property damage or loss, monetary expense….as a direct or indirect result of the defendant's offense or criminal episode". s. 775.089(1)(c), F.S. Further, the restitution statute requires the court to order a defendant to make restitution for damage or loss caused directly or indirectly by the defendant's offense and damage or loss related to the defendant's criminal episode. s. 775.089(1)(a), F.S. Thus, for purposes of the identity theft statute, "any victim" may include both the individual whose personal identification was unlawfully used and any other person harmed by the defendant fraudulently obtained credit with another person's personal identification information. In other words, a court could order a convicted defendant to pay restitution to the person whose personal identification information was used and to any person from whom credit was obtained. Such restitution could cover the costs, including attorney's fees, incurred by the victims as a result of the defendant's acts.

The Task Force on Privacy and Technology

In the 2000 session, the Legislature created the Task Force on Privacy and Technology.[14] The Task Force was charged with studying and making policy recommendations with respect to four areas:

- privacy issues related to the use of advanced technologies,
- technology fraud and identity theft,
- balancing the need for open public records with protecting citizens' privacy, and
- sale of public records to private individuals and companies.

The Task Force held four public meetings throughout the state and heard testimony from a variety of perspectives including citizens, identity theft victims, agencies, law enforcement officers, credit reporting institutions, and technology industry representatives. The Task Force released its final report to the Governor and the Legislature on February 1, 2001.

The Task Force made several findings with respect to identity theft. Specifically, the Task Force found that, on average, identity theft victims spent more than 175 hours trying to regain the financial status they had prior to being victimized.[15] Additionally, businesses were found to be victimized by identity theft because they are often forced to absorb or pass on to consumers the costs related to identity theft. The Task Force also heard evidence about the need for government to increase efforts with respect to identity theft prosecution and deterrence. Reports and testimony heard by the Task Force indicated that law enforcement officers were often unhelpful in solving identity theft cases. Some law enforcement officers were even unwilling to file formal police reports in response to victim complaints.[16] The Task Force found that there were "significant gaps" in Florida's existing

[14] *See* 2000 Fla. Laws ch. 2000-164 (codified at FLA. STAT. §282.3095 (2000)).
[15] Task Force Executive Summary at 2.
[16] *Id.* at 3.

identity protection laws and law enforcement capacity. The Task Force also heard testimony about how private sector entities could do more to deter identity theft.

Task Force Recommendations

The task force made several recommendations to the Legislature and the Governor to improve Florida's identity theft policies.

1. Expand the Venue for Prosecution – Victims and law enforcement officers testified that existing venue restrictions make it difficult to prosecute identity theft cases where the crime is committed via technology in a jurisdiction other than the one in which the victim lives. The venue statute requires criminal prosecutions to be tried "in the county where the offense was committed". s. 910.03(1), F.S. The task force recommended that the identity theft statute be amended to allow venue for identity theft prosecution in the county of residence of the victim or any county where an element of the crime was committed.

2. Extend the Statute of Limitations – Victims and law enforcement officers felt that the complex nature of many identity theft cases made the existing statute of limitations too restrictive. The statute of limitations statute provides that a prosecution must be commenced within a certain amount of time after an offense is committed as follows: four years for a first degree felony, three years for a second or third degree felony and two years for a first degree misdemeanor. s. 775.15(2), F.S. The Task Force recommended that the identification theft statute be amended to extend the statute of limitations.

3. Enhance Existing Penalties – Victims and law enforcement officers felt that existing penalties for identity theft should be enhanced, especially where public record information has been used to facilitate the crime. This statement is corroborated by the Task Force's findings that identity theft victims are often revictimized when public records are not corrected. The Task Force recommended that section 817.568 be amended to provide that, where public record information is used in perpetrating the crime under section 817.568, the penalty for the respective crime be increased by one level.

4. Increase the Role of the FDLE – Law enforcement officers felt that a lack of resources and trained personnel made investigation high-tech crimes difficult. The Task Force recommended that FDLE be given an increasing role in investigating technology-based and identity theft-related crimes. The Task Force recommended that FDLE be given original jurisdiction to investigate technology-based and identity theft-related crimes where the State is a victim. The Task Force also recommended that the FDLE Computer Crime Center be expanded to include a pilot program for up to ten cyber-crime investigators with jurisdiction over multi-jurisdictional technology-based crimes where losses potentially exceed $50,000.

C. EFFECT OF PROPOSED CHANGES:

HB 1845 implements the recommendations of the Task Force and clarifies existing statutory provisions as follows.

Revising and Deleting Certain Definitions

Currently, subsection s. 817.568(1)(d) defines the term "individual" to mean a "single human being and does not mean a firm, association of individuals, corporation, partnership, joint venture, sole proprietorship, or other entity." HB 1845 deletes this definition because the bill uses the term "person" rather than the term "individual". The use of the term "person" rather than "individual" for

the purposes would expand the scope of protection provided by s. 817.568 to include corporations and other legal entities recognized as "persons" under s. 1.01, F.S.

Establish Venue for Prosecution and Trial

Currently, venue for prosecution and trial is determined by the place or places where the offense was committed without regard to the place where the victim resides. ss. 910.01, F.S., et seq. In response to a recommendation of the Task Force, HB 1845 provides that venue for prosecution and trial of an offense under s. 817.568 is in the county where the victim resides or in the county where any element of the crime was committed.

Extend the Statute of Limitations

Currently, the time limitation for commencing prosecution of a third-degree felony is three years from the date of the offense. s. 775.15(2)(b), F.S. The time limitation for commencing prosecution of a first-degree misdemeanor is two years. s. 775.15(2)(c)-(d). However, if the offense involves fraud, the action may be commenced within one year after the discovery of the offense but no later than three years after the expiration of the original three-year statute of limitations. s. 775.15(3)(a), F.S.

The bill increases the time limitations for commencing a prosecution of any offense under s. 817.568 to five years, unless the offense was fraudulent use of personal identification information and the five years has expired, in which event, pursuant to s. 775.15(3)(a), prosecution of the offense could be commenced within one year of discovery of the offense but no later than eight years (five plus three) after commission of the offense.

Criminal Use of Personal Identification Information

Currently, there are two identification theft offenses within 817.568. One offense states that any person who "willfully and without authorization fraudulently uses, or possesses with intent to fraudulently use, personal identification information concerning an individual without first obtaining that individual's consent" is guilty of the prohibited act. This apparently requires the prosecution to prove three things: willful use, use without authorization and fraudulent use (or possession with intent to fraudulently use). Additionally the current language requires that a person act "without first obtaining that individual's consent." Section 817.568 also requires that the person be successful in obtaining the information.

The second offense is that of use or attempt to use another person's personal identification information without first obtaining that individual's consent for the purpose of harassing that individual.

The bill modifies these offenses as follows:

1. Obtaining or Using Identification Information Without Authorization: The bill provides that any person who knowingly obtains or uses or attempts to obtain or use, another person's personal identification information without being duly authorized to obtain or use such information is guilty of "obtaining or using personal identification information without authorization". The bill makes this offense a second degree misdemeanor. This offense would not contain a specific intent requirement. Thus, any person who knowingly obtains or uses, or attempts to obtain or use another person's personal identification information without authorization, *regardless of the person's motivation*, commits the crime of obtaining personal identification information without authorization. Further, this provision would broaden the scope of conduct prohibited under s. 817.568. A person who steals another

person's social security number would commit the offense of obtaining personal identification information without authorization regardless of whether the thief actually used the number.

2. Harassment by Use of Personal Identification Information: The bill provides that any person who knowingly obtains or uses or attempts to obtain or use another person's personal identification information without being duly authorized to obtain or use such information and who does so with intent to harass any person is guilty of "harassment by use of personal identification information". This offense is a first degree misdemeanor.

   The current definition of "harass" requires that the conduct be "directed at a specific person" and "intended to cause substantial emotional distress." The bill defines the term "harass" to mean:

   > [T]o knowingly engage in an unauthorized course of conduct that serves no legitimate purpose directed at one or more persons with the intent to subject such person or persons to annoyance, embarrassment, humiliation, distress, torment or terror. The term does not include any authorized course of conduct that serves a legitimate commercial or government purpose.

3. Fraudulent Use of Personal Identification Information: The bill provides that any person who knowingly obtains or uses or attempts to obtain or use, another person's personal identification information without being duly authorized to obtain or use such information with intent to use such information fraudulently, is guilty of "fraudulent use of personal identification information." The offense is a third degree felony.

4. Heightened Penalties for Unlawfully Using Public Record Information: In response to a recommendation of the Task Force, HB 1845 provides for heightened penalties for an identity theft offense committed with unlawful use of a public record. Specifically, when a person unlawfully uses public record information to commit the offense of:

   - obtaining or using personal identification information without authorization, the offense would be reclassified from a second-degree misdemeanor to a first-degree misdemeanor;

   - harassment by use of personal identification information, the offense would be reclassified from first-degree misdemeanor to a third-degree felony;

   - fraudulently using personal identification information, the offense be reclassified from a third-degree felony to a second-degree felony.

   The bill amends s.921.0022, F. S., to rank the offense of fraudulent use of personal identification information in Level 3 of the Offense Severity Ranking Chart of the Criminal Punishment Code. The bill also amends s. 921.0024, F. S., to include in the key to the Florida Criminal Punishment Code Worksheet a provision for applying a multiplier of 1.5 times the sentencing points assessed for any offense under s. 817.568, F.S., that involves use of personal identification information unlawfully obtained from a public record.

Revising Restitution Provisions

The bill clarifies that restitution is available to include;

- any person who is a victim of the crime;
- all costs any victim reasonably and necessarily incurs in correcting any error or misrepresentation in the victim's credit history or credit report, or in satisfying or discharging any monetary debt, mortgage, lien or other legal obligation affecting the victim's financial condition that was caused or created by, or resulted from, the defendant committing the crime; and
- correction, completion, restoration or replacement of any public record that is incorrect, incomplete, damaged or missing as a result of the defendant committing the crime.

D. SECTION-BY-SECTION ANALYSIS:

Section 1: Amends s. 817.568, F.S.; relating to theft of personal identification information.

Section 2: Amends s. 775.15, F.S.; relating to time limitations for commencing prosecution.

Section 3: Amends s. 921.0022, F.S.; relating to the Offense Severity Ranking Chart of the Criminal Punishment Code.

Section 4: Amends s. 921.0024; relating to worksheet computation in Criminal Punishment Code.

Section 5: Provides effective date of July 1, 2001.

III. FISCAL ANALYSIS & ECONOMIC IMPACT STATEMENT:

A. FISCAL IMPACT ON STATE GOVERNMENT:

1. Revenues:

The bill would generate no new revenues, except through the collection of any fine imposed as a criminal penalty for conviction of any prohibited act.

2. Expenditures:

The bill would require the State to fund its proportionate share of the additional cost of prosecuting, convicting, incarcerating and supervising persons convicted of any prohibited act.

B. FISCAL IMPACT ON LOCAL GOVERNMENTS:

1. Revenues:

The bill would generate no new revenues, except through collection of any fine imposed as a penalty for conviction of any prohibited act.

2. Expenditures:

The bill would require county governments to fund their proportionate share of the additional costs of prosecuting, convicting, incarcerating and supervising persons convicted of a prohibited act.

C. DIRECT ECONOMIC IMPACT ON PRIVATE SECTOR:

By expanding the scope of protection from identity theft and increasing the penalties for such offenses, the bill help deter the commission of identity theft which would result in economic relief to legitimate consumers and businesses. As the Task Force noted, identity theft victims often spend substantial personal resources and take significant time away from work attempting to repair the damage to the personal identification information. Because most victims are not personally liable for the economic damages done by identity thieves, businesses are often forced to absorb the costs. Any reduction in the occurrence of identity theft would provide a measure of economic relief to legitimate consumers and businesses by reducing losses victims incur and the amount of bad debt businesses absorb. Additionally, the expanded restitution provisions of the bill would provide victims with a greater opportunity to obtain complete relief from the losses they sustain as a result of any crime committed under s. 817.568.

D. FISCAL COMMENTS:

N/A

IV. CONSEQUENCES OF ARTICLE VII, SECTION 18 OF THE FLORIDA CONSTITUTION:

A. APPLICABILITY OF THE MANDATES PROVISION:

This bill is exempt from the requirements of Article VII, Section 18 of the Florida Constitution because it is a criminal law.

B. REDUCTION OF REVENUE RAISING AUTHORITY:

This bill does not reduce the authority that counties or municipalities have to raise revenues in the aggregate.

C. REDUCTION OF STATE TAX SHARED WITH COUNTIES AND MUNICIPALITIES:

This bill does not reduce the percentage of a state tax shared with counties or municipalities.

V. COMMENTS:

A. CONSTITUTIONAL ISSUES:

Article 1, Section 16 of the Florida Constitution requires that a criminal trial be conducted in the county where the crime was committed. State v. Stephens, 608 So.2d 905 (Fla. 5th 1992)(noting that "Florida's Constitution gives a defendant the right to be tried in the county where the crime took place."). "An exception to the strict venue rule is provided by section 910.05 for crimes where the acts constituting one offense are committed in two or more counties. Trial in any county where any of the facts took place is sufficient." State v. Stephens, 586 So.2d 1073 (Fla. 5th DCA 1991). The provision in the bill that allows a prosecution to be commenced in the county of residence of the victim without requiring that any element of the crime be committed in that county may be in conflict with this constitutional requirement.

B. RULE-MAKING AUTHORITY:

None.

C. OTHER COMMENTS:

N/A

VI. AMENDMENTS OR COMMITTEE SUBSTITUTE CHANGES:

The Committee on Crime Prevention, Corrections & Safety adopted a strike-everything amendment which is traveling with the bill. The amendment provides as follows:

- Amends section 817.568 to provide that any person who willfully and without authorization fraudulently uses personal identification information concerning an individual without first obtaining that individual's consent commits a felony of the second degree, if the pecurinary benefit, the value of the services received, the payment sought to be avoided, or the amount of the injury or fraud perpetrated is $75,000 or more.

- Provides that if an offense prohibited under this section was facilitated or furthered by use of a public record, the offense is reclassified to the next higher degree as follows: a first degree misdemeanor is reclassified as a third degree felony; a third degree felony is reclassified as a second degree felony and a second degree felony is reclassified as a felony of the first degree.

- Provides that a felony offense reclassified under this subsection is ranked one level above the ranking of the felony offense committed and a misdemeanor offense that is reclassified is ranked in level 2 of the Offense Severity Ranking Chart of the Criminal Punishment Code.

- Contains a legislative finding that in the absence of evidence to the contrary, the location where the victim gives or fails to give consent to the use of personal identification information is the county where the victim generally resides. The amendment also provides that venue for the prosecution and trial of violations of this section may be commenced and maintained in any county in which an element of the offense occurred, including the county where the victim generally resides.

- Provides that a prosecution of an offense under this section must be commenced within 3 years after the offense occurred. However, a prosecution may be commenced within 1 year after discovery of the offense if such prosecution is commenced within 5 years after the violation occurred.

- Ranks the offense of fraudulent use of personal identification information in level 4 and the offense of fraudulent use of identification information where the fraud is $75,000 or more in level 5 of the Offense Severity Ranking Chart of the Criminal Punishment Code.

VII. SIGNATURES:

COMMITTEE ON CRIME PREVENTION, CORRECTIONS & SAFETY:

Prepared by: Staff Director:

John A. Barley, Chief Legislative Analyst Charles M. Davidson

Richard H. Martin, Legislative Intern

AS REVISED BY THE COMMITTEE ON CRIME PREVENTION, CORRECTIONS & SAFETY:

Prepared by:	Staff Director:
Trina Kramer	David De La Paz