STORAGE NAME: h1845z.it.doc
DATE: June 11, 2001

HOUSE OF REPRESENTATIVES
AS FURTHER REVISED BY THE
COUNCIL FOR READY INFRASTRUCTURE
FINAL ANALYSIS

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

RELATING TO: Criminal use of personal information

SPONSOR(S): Committee on Information Technology

TIED BILL(S):

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

(1) INFORMATION TECHNOLOGY YEAS 10 NAYS 0
(2) CRIME PREVENTION, CORRECTIONS & SAFETY YEAS 5 NAYS 0
(3) COUNCIL FOR READY INFRASTRUCTURE YEAS 17 NAYS 0
(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 (Task Force) recommended that changes be made to the existing law to further its goals.

The bill implements some of the recommendations of the Task Force related to identity theft under s. 817.568, F.S. The bill revises existing statutory definitions to expand the scope of protection from identity thieves. The bill increases the penalty for identity theft from a third degree felony to a second degree felony where the value of the fraud perpetrated by the thief is $75,000 or more. Additionally, the bill provides for heightened penalties when an offender unlawfully uses public record information to commit an identity theft crime.

The bill would take effect July 1, 2001.

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 and imprisonment. 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 3 years of imprisonment.[10] The criminal provisions are enforced by the U.S. Department of Justice with cooperation from the Secret Service, the Federal Bureau of Investigation 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's Identity Theft Statute

In 1999, Florida enacted identity protection legislation that is now codified at s. 817.568, F.S.[13] Section 817.568, F.S., creates two crimes: fraudulent use of personal identification information and harassment by use of personal identification information. To commit either offense, the person must successfully obtain the victim's personal identification information. Attempts to *obtain*, to be distinguished from attempts to *use*, personal identification information (such as hacking) are not prohibited by this statute. The term "personal identification information," as defined in s. 817.568(1)(f), F.S., includes:

> 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;
>
> 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

---

[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)).

4. Telecommunication identifying information or access device.

The crime of "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 5 years imprisonment. The legal standard for the offense apparently requires the prosecution to prove four things: willful use, use without authorization, fraudulent use (or possession with intent to fraudulently use), and that the offender acted "without first obtaining the individual's consent."

"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. The offense is a first-degree misdemeanor, punishable by a fine of up to $1,000 and 1 year of imprisonment. The legal standard for the offense apparently requires the prosecution to prove four things: willful use, use without authorization, that the offender acted "without first obtaining the individual's consent," and that the offender possessed the specific intent to harass the individual whose personal identification information was unlawfully obtained.

Section 817.568 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 who fraudulently obtained credit. 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 (Task Force).[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.

[14] *See* 2000 Fla. Laws ch. 2000-164 (codified at FLA. STAT. §282.3095 (2000)).

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 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 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, 3 years for a second or third degree felony and 2 years for a first degree misdemeanor. s. 775.15(2), F.S. The Task Force recommended that the identity 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 s. 817.568, F.S., be amended to provide that, where public record information is used in perpetrating the crime under s. 817.568, F.S., the penalty for the respective crime be increased by one level.

4. Increase the Role of the Florida Department of Law Enforcement (FDLE) – Law enforcement officers felt that a lack of resources and trained personnel made investigation high-tech crimes difficult. The Task Force recommended that the Legislature increase the role of the FDLE 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.

[15] Task Force Executive Summary at 2.
[16] *Id*. at 3.

C. EFFECT OF PROPOSED CHANGES:

The bill implements some of the recommendations of the Task Force and clarifies existing statutory provisions as follows.

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, the bill would add a new subsection (9) to state that venue for prosecution and trial of an offense under s. 817.568, F.S., is in any county where any element of the crime was committed, including the county where the victim generally resides. The bill also would add a new subsection (8) to state the Legislature's finding that in the absence of evidence to the contrary, the victim is presumed to reside in the location where the victim gives or fails to give consent to the use of personal identification information. The bill's apparent reference to a location where the victim gives consent appears anomalous because, to commit any offense under s. 817.568, the personal identification information must be used without the victim's consent.

Statute of Limitations

The bill modifies the statute of limitations to provide that an offense of fraudulent use of personal identification information must be commenced within three years after the date of the offense occurred. If the three years expires, the bill provides that a prosecution may be commenced within one year after discovery of the offense by an aggrieved party or the party's representative if the prosecution is commenced within five years after the violation occurred.

Criminal Use of Personal Identification Information

The bill increases criminal penalties for fraudulent use of personal identification information causing $75,000 or more in damages and for crimes committed under s. 817.568 that were facilitated by the use of public records.

The bill would add a new subsection (2)(b) to section 817.568 to provide that if a person commits the crime of fraudulent use of personal identification information and the damage caused by the crime is $75,000 or more, the penalty is increased from a third degree felony to a second degree felony. In calculating whether the damage was $75,000 or more, four factors are totaled: the pecuniary benefit derived from the prohibited act, the value of the services received by the defendant, the payment sought to be avoided or the amount of injury or fraud perpetrated.

In response to a recommendation of the Task Force, the bill 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:

- Fraudulent use of personal identification information, the offense is reclassified from a third degree felony to a second degree felony;
- Fraudulent use of personal identification information resulting in damages of $75,000 or more, the offense is reclassified from a second degree felony to a first degree felony;
- Harassment by use of personal identification information, the offense is reclassified from first-degree misdemeanor to a third-degree felony; and

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.

D. SECTION-BY-SECTION ANALYSIS:

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

Section 2: Amends s. 921.0022, F.S.; relating to the Offense Severity Ranking Chart of the Criminal Punishment Code.

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

II. FISCAL ANALYSIS & ECONOMIC IMPACT STATEMENT:

A. FISCAL IMPACT ON STATE GOVERNMENT:

1. Revenues:

The bill generates 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 investigating, prosecuting, incarcerating and supervising persons convicted of any prohibited act.

B. FISCAL IMPACT ON LOCAL GOVERNMENTS:

1. Revenues:

The bill generates 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 investigating, prosecuting, incarcerating and supervising persons convicted of a prohibited act.

C. DIRECT ECONOMIC IMPACT ON PRIVATE SECTOR:

By increasing the penalties for identity theft offenses, the bill will help deter the commission of identity theft, resulting 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 their 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.

D. FISCAL COMMENTS:

N/A

III. 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.

IV. 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 DCA 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, F.S., 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, 1079 (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:

None.

V. AMENDMENTS OR COMMITTEE SUBSTITUTE CHANGES:

On April 12, 2001, the Committee on Crime Prevention, Corrections & Safety adopted a strike-everything amendment, which substantially modified the provisions of the bill. The analysis above reflects the bill as amended.

VI. SIGNATURES:

COMMITTEE ON COMMITTEE ON INFORMATION TECHNOLOGY:

Prepared by:	Staff Director:
John A. Barley/Richard H. Martin	Charles M. Davidson

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

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

AS FURTHER REVISED BY THE COUNCIL FOR READY INFRASTRUCTURE:

Prepared by:	Council Director:
Randy L. Havlicak	Thomas J. Randle

AS FURTHER REVISED BY THE COMMITTEE ON INFORMATION TECHNOLOGY:

Prepared by:	Staff Director:
Richard H. Martin	Charles Davidson