

STORAGE NAME: h1845.it.doc

DATE: March 27, 2001

**HOUSE OF REPRESENTATIVES
COMMITTEE ON
INFORMATION TECHNOLOGY
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)
 - (3)
 - (4)
 - (5)
-

I. SUMMARY:

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 is a costly crime because affected businesses often have no alternative but to absorb debt fraudulently incurred by identity thieves. This cost is ultimately passed along to consumers who are customers of such businesses. Additionally, victims of identity theft are often faced with the laborious task of correcting any damage to their personal identification information caused by identity thieves.

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.

PCB IT 01-01 would implement most of the recommendations of the Task Force related to identity theft under s. 817.568. The PCB would revise existing statutory definitions to expand the scope of protection from identity thieves. The PCB would create 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 PCB would provide 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 PCB would enhance 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 PCB would expand the venue of prosecutions and trials to be in the county of the 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 PCB would also vest jurisdiction to prosecute violations of s. 817.568 in all state attorneys and Florida's statewide prosecutor.

II. SUBSTANTIVE ANALYSIS:

A. DOES THE BILL SUPPORT THE FOLLOWING PRINCIPLES:

- | | | | |
|-----------------------------------|---|--|------------------------------|
| 1. <u>Less Government</u> | Yes <input type="checkbox"/> | No <input checked="" type="checkbox"/> | N/A <input type="checkbox"/> |
| 2. <u>Lower Taxes</u> | Yes <input type="checkbox"/> | No <input checked="" type="checkbox"/> | N/A <input type="checkbox"/> |
| 3. <u>Individual Freedom</u> | Yes <input type="checkbox"/> | No <input checked="" type="checkbox"/> | N/A <input type="checkbox"/> |
| 4. <u>Personal Responsibility</u> | Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/> | N/A <input type="checkbox"/> |
| 5. <u>Family Empowerment</u> | Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/> | N/A <input type="checkbox"/> |

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

PCB IT 01-01 would probably 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. PCB IT 01-01 would limit the exercise of individual freedom by criminalizing obtaining or using personal identification information without authorization.

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 bad 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/identitythefittestimony.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 The Identity Theft and Assumption Deterrence Act of 1998 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 also punishable in the same manner and to the same extent.¹¹

In addition to the federal laws, 27 states enacted identity theft legislation in 1999 and 10 states enacted legislation in 2000.¹² 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. Subsection 2 of section 817.568 defines the crime of fraudulent use of personal identification information. "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. Fraudulent use of personal identification information, as a third-degree felony, is punishable by a fine of up to \$5,000 and/or up to five years of imprisonment.

Subsection 3 of section 817.568 defines the crime of harassment by use of personal identification information. "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. Harassment by use of personal identification information, as a first-degree misdemeanor, is punishable by a fine of up to \$1,000 and/or up to one year of imprisonment.

Subsection 5 of section 817.568 provides that, when sentencing a defendant, a court may order the defendant to make restitution to "any victim of the offense." To be liable for restitution under subsection 5, the criminal defendant must be convicted. Although "victim" is not defined for the purposes of s. 817.568, "any victim" may include both the individual whose personal identification was unlawfully used and any other person harmed by the defendant's conduct. For instance, if a

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)).

defendant fraudulently obtained credit with another person's personal identification information, 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 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.

Identity Theft Policy Recommendations of the Privacy and Technology Task Force

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 Task Force recommended that section 817.568 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 Task Force recommended that section 817.568 be amended to extend the statute of limitations. Specifically, the Task Force recommended that the action be

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.

commenced within three years after commission of the offense, provided the victim could commence the action within one year after discovery of the offense, but in no event later than five years from the time of the offense.

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:

PCB IT 01-01 would implement the recommendations of the Task Force and clarify existing statutory provisions. The bill would amend s. 817.568 to expand the venue for prosecution and to enhance existing penalties for the unlawful use of public record information in committing an offense under s. 817.568. The bill would also amend s. 775.15, F.S., to extend the statute of limitations for prosecuting violations of s. 817.568. Additionally, PCB IT 01-01 would revise and supplement the existing offenses in subsections (2) and (3) of s. 817.568 to provide for three distinct crimes: obtaining or using personal identification information without authorization, harassment by use of personal identification information, and fraudulent use of personal identification information. PCB IT 01-01 would also reclassify the offenses to the next highest level of the offense where committed by making unlawful use of a public record. PCB IT 01-01 would also revise the language in the current version of subsection (5) of s. 817.568 relating to judicial orders for restitution and correction of public records. PCB IT 01-01 would also amend s. 775.15 to increase the time for commencing prosecution of an offense under s. 817.568. PCB IT 01-01 would also amend s. 921.0022 and s. 921.0024 to provide for increased sentencing.

Revising and Deleting Certain Definitions

PCB IT 01-01 would delete the definitions of "person" and "individual" for the purposes of s. 817.568 and would revise the definition of "harass" for the purposes of s. 817.568, and would revise the definition of "personal identification information." The term "person" is presently defined in subsection s. 817.568(1)(e) defined differently than in s. 1.01(3), F.S. Because the definition of "person" provided in s. 1.01(3) is implicit in all Florida statutes, the definition of the term "person" for s. 817.568 is unnecessary. PCB IT 01-01 would eliminate this unnecessary language, and the term "person" would have the same meaning as provided in s. 1.01(3).

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." PCB IT 01-01 would delete this definition because under the language proposed by PCB IT 01-01, the term "person" rather than the term "individual" would be used. Because the term "individual" would no longer be used, a definition for the term is unnecessary. By using the term "person" rather than "individual" for the purposes of s. 817.568,

PCB IT 01-01 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.

PCB IT 01-01 would also revise the definition of the term “harass” for the purposes of s. 817.568. The current definition of “harass” requires that the conduct be “directed at a specific person” and “intended to cause substantial emotional distress.” PCB IT 01-01 would expand the scope of conduct that is defined as “harassment” to include conduct aimed at more than one person. Under PCB IT 01-01, the term “harass” would mean:

to 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.

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. See ss. 910.01, F.S., et seq. In response to a recommendation of the Task Force, PCB IT 01-01 would provide 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

In response to a recommendation of the Task Force, Section 2 of PCB IT 01-01 would amend s. 775.15, F.S. to increase the time limitations for violations of s. 817.568. Currently, the time limitation for commencing prosecution of a third-degree felony is three years from the date of the offense. See s. 775.15(2)(b), F.S. The time limitation for commencing prosecution of a first-degree misdemeanor is two years. See 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. See s. 775.15(3)(a), F.S.

Section 2 of the bill would increase 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.

Clarifying and Adding Language Regarding Offenses

PCB IT 01-01 would clarify the existing language in s. 817.568 that prohibits the fraudulent use of personal identification information and harassment by use of personal identification information. The bill would also create a new offense; namely: obtaining or using personal identification information without authorization.

Currently, subsection (2) of s. 817.568 states that any person who “willfully and without authorization fraudulently uses, or possesses with intent to fraudulently use, personal identification information” is guilty of the prohibited act. Arguably, this language would require 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 and putting the information to fraudulent use. A person who attempts to

obtain personal identification without authorization does not violate s. 817.568, and a person who obtains the information without authorization but has not yet put the information to a fraudulent use does not violate s. 817.568.

If enacted, PCB IT 01-01 would revise the language in subsections (2) and (3) to strengthen the prohibition against obtaining or using personal identification information without authorization. The bill would create a new offense and revise the two existing offenses.

Obtaining or using Personal Identification Information without Authorization

PCB IT 01-01 would create an additional offense under s. 817.568; namely: obtaining or using of personal identification information without authorization. Under PCB IT 01-01, in order to commit the crime of obtaining or using personal identification without authorization, a person must:

- Knowingly,
- Obtain or use, or attempt to obtain or use,
- Another person's personal identification information,
- Without being duly authorized.
- **(Specific Intent)** None.

The crime of obtaining or using personal identification information without authorization would be punishable as a second-degree misdemeanor. Unlike the modifications to the other prohibitions in s. 817.568, the crime of obtaining or using personal identification information would be a general intent crime and 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. This provision would broaden the scope of conduct prohibited under s. 817.568. For instance, under PCB IT 01-01, 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. If the person also took the number with the intention to harass the owner or to use it to perpetuate fraud, the heightened penalties provided by proposed subsections (3) or (4) would apply.

Harassment by use of Personal Identification Information

PCB IT 01-01 would move the existing provisions of subsection (2) of s. 817.568 that define the crime of harassment by use of personal identification information to a new subsection (3). Under PCB IT 01-01, in order to commit the crime of harassment by use of personal identification information, the person must:

- Knowingly,
- Obtain or use, or attempt to obtain or use,
- Another's personal identification information,
- Without being duly authorized,
- **(Specific Intent)** With the intent to harass any person.

To commit the crime of harassment by use of personal identification information, a person must obtain or use, or attempt to obtain or use such information with the intent to harass the person who such information identifies. Harassment by use of personal identification information would be punishable as a first-degree misdemeanor.

Fraudulent Use of Personal Identification Information

PCB IT 01-01 would move the crime of fraudulent use of personal identification information to a new subsection (4). Under PCB IT 01-01, in order to commit the crime of fraudulent use of personal identification information, the person must:

- Knowingly,
- Obtain or use, or attempt to obtain or use,
- Another person's personal identification information,
- Without being duly authorized,
- **(Specific intent)** With the intent to use such information to perpetrate a fraud.

Thus to commit fraudulent use of personal identification information, the person must intend to obtain or use, or attempt to obtain or use such information to perpetrate a fraud. Fraudulent use of personal identification information would be punishable as a third-degree felony.

Heightened Penalties for Unlawfully Using Public Record Information

In response to a recommendation of the Task Force, PCB IT 01-01 would provide for heightened penalties for an offense under s. 817.568 committed with unlawful use of a public record. The bill would increase the penalty for any such offense by one degree when the offense involves the unlawful use of public record information. Specifically, when a person unlawfully uses public record information to commit the offense of:

- obtaining or using personal identification information without authorization would be reclassified from a second-degree misdemeanor to a first-degree misdemeanor;
- harassment by use of personal identification information would be reclassified from first-degree misdemeanor to a third-degree felony; and
- fraudulently using personal identification information would be reclassified from a third-degree felony to a second-degree felony.

Section 3 of PCB IT 01-01 would amend s.921.0022, F. S., to include in the Florida Criminal Punishment Code a provision classifying fraudulent use of personal identification information under s. 817.568 (4) as a Level 3 felony.

Section 4 of PCB IT 01-01 would amend 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 time 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

PCB IT 01-01 would clarify and expand the language in subsection (5) of s. 817.568 that permits the sentencing court to order that a defendant make restitution. The bill would conform the permissive provision for restitution in subsection (5) to the mandatory provision for restitution in s. 775.089, F. S., and would expand the scope of restitution 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.

III. FISCAL ANALYSIS & ECONOMIC IMPACT STATEMENT:

1. Revenues:

PCB IT 01-01 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:

PCB IT 01-01 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:

PCB IT 01-01 would generate no new revenues, except through collection of any fine imposed as a penalty for conviction of any prohibited act.

2. Expenditures:

PCB IT 01-01 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 amendments PCB IT 01-01 would make to ss. 817.568, 775.15, 921.0022 and 921.0024, F. S., may tend to deter the commission of identity theft. Although no reliable estimate can be made as to the extent of the deterrence, any deterrence should 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 PCB IT 01-01 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:

PCB IT 01-01 is expressly excepted from analysis under this part because it would be a criminal law.

B. REDUCTION OF REVENUE RAISING AUTHORITY:

PCB IT 01-01 is expressly excepted from analysis under this part because it would be a criminal law.

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

PCB IT 01-01 is expressly excepted from analysis under this part because it would be a criminal law.

V. COMMENTS:

A. CONSTITUTIONAL ISSUES:

PCB IT 01-01 does not appear to raise any constitutional issues.

B. RULE-MAKING AUTHORITY:

PCB IT 01-01 does not confer rule-making authority on any government agency.

VI. AMENDMENTS OR COMMITTEE SUBSTITUTE CHANGES:

A technical amendment was made to clarify the changes proposed to subsection (5) providing for increasing to the next highest level the severity of offenses under s. 817.568 when committed by using any public record, to clarify that no changes are proposed to subsections (4) and (7) except to renumber subsection (4) to be Subsection (6), to include in subsection (8) reference to the provisions for restitution in s.775.089, and to clarify the provisions of subsection (9) providing for venue of prosecution and trial of any offense under s. 817.568.

VII. SIGNATURES:

COMMITTEE ON INFORMATION TECHNOLOGY:

Prepared by:

John A. Barley, Chief Legislative Analyst

Charles M. Davidson, Staff Director

Richard H. Martin, Legislative Intern