By the Committee on Judiciary; and Senators Campbell and Aronberg

590-2047-05

A bill to be entitled

An act relating to unlawful use of personal identification information; amending s. 817.568, F.S.; including other information within the definition of the term "personal identification information"; defining the term "counterfeit or fictitious personal identification information"; revising criminal penalties relating to the offense of fraudulently using, or possessing with intent to fraudulently use, personal identification information; providing minimum mandatory terms of imprisonment; creating the offenses of willfully and fraudulently using, or possessing with intent to fraudulently use, personal identification information concerning a deceased individual; providing criminal penalties; providing for minimum mandatory terms of imprisonment; creating the offense of willfully and fraudulently creating or using, or possessing with intent to fraudulently use, counterfeit or fictitious personal identification information; providing criminal penalties; providing for reclassification of offenses under certain circumstances; providing for reduction or suspension of sentences under certain circumstances; creating s. 817.5681, F.S.; requiring business persons maintaining computerized data that includes personal information to disclose breaches of system security under certain circumstances; providing requirements; providing for administrative fines; providing exceptions and limitations; authorizing delays of such disclosures under certain circumstances; providing definitions; providing for alternative notice methods; specifying conditions of compliance for persons maintaining certain alternative notification procedures; specifying conditions under which notification is not required; providing requirements for documentation and maintenance of documentation; providing an administrative fine for failing to document certain failures to comply; providing for application of administrative sanctions to certain persons under certain circumstances; authorizing the Department of Legal Affairs to institute proceedings to assess and collect fines; providing an effective date.

Be It Enacted by the Legislature of the State of Florida:

Section 1. Section 817.568, Florida Statutes, is amended to read:

817.568 Criminal use of personal identification information.--

(1) As used in this section, the term:

(a) "Access device" means any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds, other than a transfer originated solely by paper instrument.

(b) "Authorization" means empowerment, permission, or competence to act.

(c) "Harass" means to engage in conduct directed at a specific person that is intended to cause substantial emotional distress to such person and serves no legitimate purpose. "Harass" does not mean to use personal identification information for accepted commercial purposes. The term does not include constitutionally protected conduct such as organized protests or the use of personal identification information for accepted commercial purposes.

(d) "Individual" means a single human being and does not mean a firm, association of individuals, corporation, partnership, joint venture, sole proprietorship, or any other entity.

(e) "Person" means a "person" as defined in s. 1.01(3).

(f) "Personal identification information" means 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, <u>postal or electronic mail address, telephone number,</u> social security number, date of birth, <u>mother's maiden name,</u> official state-issued or United States-issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, Medicaid or food stamp account number, ~~or~~ bank account <u>number,</u> ~~or~~ credit <u>or debit</u> card number<u>, or</u>

CODING: Words ~~stricken~~ are deletions; words <u>underlined</u> are additions.

personal identification number or code assigned to the holder of a debit card by the issuer to permit authorized electronic use of such card;

2. Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;

3. Unique electronic identification number, address, or routing code; ~~or~~

4. Medical records;

5.~~4.~~ Telecommunication identifying information or access device; or~~.~~

6. Other number or information that can be used to access a person's financial resources.

(g) "Counterfeit or fictitious personal identification information" means any counterfeit, fictitious, or fabricated information in the similitude of the data outlined in paragraph (f) that, although not truthful or accurate, would in context lead a reasonably prudent person to credit its truthfulness and accuracy.

(2)(a) 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, commits the offense of fraudulent use of personal identification information, which is a felony of the third degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

(b) 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, punishable as provided in s. 775.082, s. 775.083, or s. 775.084, if the pecuniary benefit, the value of the services received, the payment sought to be avoided, or the amount of the injury or fraud perpetrated is $5,000 or more or if the person fraudulently uses the personal identification information of 10 or more individuals<u>, but fewer than 20 individuals,</u> without their consent. Notwithstanding any other provision of law, the court shall sentence any person convicted of committing the offense described in this paragraph to a mandatory minimum sentence of 3 years' imprisonment.

(c) 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 first degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084, if the pecuniary benefit, the value of the services received, the payment sought to be avoided, or the amount of the injury or fraud perpetrated is $50,000 or more or if the person fraudulently uses the personal identification information of 20 or more individuals<u>, but fewer than 30 individuals,</u> without their consent. Notwithstanding any other provision of law, the court shall sentence any person convicted of committing the offense described in this paragraph~~:~~

~~1.~~ to a mandatory minimum sentence of 5 years' imprisonment. <u>If the pecuniary benefit, the value of the services received, the payment sought to be avoided, or the amount of the injury or fraud perpetrated is $100,000 or more, or if the person fraudulently uses the personal identification information of 30 or more individuals without their consent,</u>

<u>notwithstanding any other provision of law, the court shall sentence any person convicted of committing the offense described in this paragraph</u>

~~2.~~ to a mandatory minimum sentence of 10 years' imprisonment~~, if the pecuniary benefit, the value of the services received, the payment sought to be avoided, or the amount of the injury or fraud perpetrated is $100,000 or more or if the person fraudulently uses the personal identification information of 30 or more individuals without their consent~~.

(3) Neither paragraph (2)(b) nor paragraph (2)(c) prevents a court from imposing a greater sentence of incarceration as authorized by law. If the minimum mandatory terms of imprisonment imposed under paragraph (2)(b) or paragraph (2)(c) exceed the maximum sentences authorized under s. 775.082, s. 775.084, or the Criminal Punishment Code under chapter 921, the mandatory minimum sentence must be imposed. If the mandatory minimum terms of imprisonment under paragraph (2)(b) or paragraph (2)(c) are less than the sentence that could be imposed under s. 775.082, s. 775.084, or the Criminal Punishment Code under chapter 921, the sentence imposed by the court must include the mandatory minimum term of imprisonment as required by paragraph (2)(b) or paragraph (2)(c).

(4) Any person who 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, commits the offense of harassment by use of personal identification information, which is a misdemeanor of the first degree, punishable as provided in s. 775.082 or s. 775.083.

(5) If an offense prohibited under this section was facilitated or furthered by the use of a public record, as defined in s. 119.011, the offense is reclassified to the next higher degree as follows:

(a) A misdemeanor of the first degree is reclassified as a felony of the third degree.

(b) A felony of the third degree is reclassified as a felony of the second degree.

(c) A felony of the second degree is reclassified as a felony of the first degree.

For purposes of sentencing under chapter 921 and incentive gain-time eligibility under chapter 944, a felony offense that is reclassified under this subsection is ranked one level above the ranking under s. 921.0022 of the felony offense committed, and a misdemeanor offense that is reclassified under this subsection is ranked in level 2 of the offense severity ranking chart in s. 921.0022.

(6) Any person who willfully and without authorization fraudulently uses personal identification information concerning an individual who is less than 18 years of age without first obtaining the consent of that individual or of his or her legal guardian commits a felony of the second degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

(7) Any person who is in the relationship of parent or legal guardian, or who otherwise exercises custodial authority over an individual who is less than 18 years of age, who willfully and fraudulently uses personal identification information of that individual commits a felony of the second

degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

(8)(a) Any person who willfully and fraudulently uses, or possesses with intent to fraudulently use, personal identification information concerning a deceased individual commits the offense of fraudulent use or possession with intent to use personal identification information of a deceased individual, a felony of the third degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

(b) Any person who willfully and fraudulently uses personal identification information concerning a deceased individual commits a felony of the second degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084, if the pecuniary benefit, the value of the services received, the payment sought to be avoided, or the amount of injury or fraud perpetrated is $5,000 or more, or if the person fraudulently uses the personal identification information of 10 or more but fewer than 20 deceased individuals. Notwithstanding any other provision of law, the court shall sentence any person convicted of committing the offense described in this paragraph to a mandatory minimum sentence of 3 years' imprisonment.

(c) Any person who willfully and fraudulently uses personal identification information concerning a deceased individual commits the offense of aggravated fraudulent use of the personal identification information of multiple deceased individuals, a felony of the first degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084, if the pecuniary benefit, the value of the services received, the payment sought to be avoided, or the amount of injury or fraud perpetrated is $50,000 or more, or if the person fraudulently uses the personal identification information of 20 or more but fewer than 30 deceased individuals. Notwithstanding any other provision of law, the court shall sentence any person convicted of the offense described in this paragraph to a minimum mandatory sentence of 5 years' imprisonment. If the pecuniary benefit, the value of the services received, the payment sought to be avoided, or the amount of the injury or fraud perpetrated is $100,000 or more, or if the person fraudulently uses the personal identification information of 30 or more deceased individuals, notwithstanding any other provision of law, the court shall sentence any person convicted of an offense described in this paragraph to a mandatory minimum sentence of 10 years' imprisonment.

(9) Any person who willfully and fraudulently creates or uses, or possesses with intent to fraudulently use, counterfeit or fictitious personal identification information concerning a fictitious individual, or concerning a real individual without first obtaining that real individual's consent, with intent to use such counterfeit or fictitious personal identification information for the purpose of committing or facilitating the commission of a fraud on another person, commits the offense of fraudulent creation or use, or possession with intent to fraudulently use, counterfeit or fictitious personal identification information, a felony of the third degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

(10) Any person who commits an offense described in this section and for the purpose of obtaining or using personal identification information misrepresents himself or herself to be a law enforcement officer; an employee or representative of a bank, credit card company, credit

counseling company, or credit reporting agency; or any person who wrongfully represents that he or she is seeking to assist the victim with a problem with the victim's credit history shall have the offense reclassified as follows:

(a) In the case of a misdemeanor, the offense is reclassified as a felony of the third degree.

(b) In the case of a felony of the third degree, the offense is reclassified as a felony of the second degree.

(c) In the case of a felony of the second degree, the offense is reclassified as a felony of the first degree.

(d) In the case of a felony of the first degree or a felony of the first degree punishable by a term of imprisonment not exceeding life, the offense is reclassified as a life felony.

For purposes of sentencing under chapter 921, a felony offense that is reclassified under this subsection is ranked one level above the ranking under s. 921.0022 or s. 921.0023 of the felony offense committed, and a misdemeanor offense that is reclassified under this subsection is ranked in level 2 of the offense severity ranking chart.

(11) The prosecutor may move the sentencing court to reduce or suspend the sentence of any person who is convicted of a violation of this section and who provides substantial assistance in the identification, arrest, or conviction of any of that person's accomplices, accessories, coconspirators, or principals or of any other person engaged in fraudulent possession or use of personal identification information. The arresting agency shall be given an opportunity to be heard in aggravation or mitigation in reference to any such motion. Upon good cause shown, the motion may be filed and heard in

camera. The judge hearing the motion may reduce or suspend the sentence if the judge finds that the defendant rendered such substantial assistance.

(12)~~(8)~~ This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of this state or any of its political subdivisions, of any other state or its political subdivisions, or of the Federal Government or its political subdivisions.

(13)~~(9)~~(a) In sentencing a defendant convicted of an offense under this section, the court may order that the defendant make restitution under ~~pursuant to~~ s. 775.089 to any victim of the offense. In addition to the victim's out-of-pocket costs, ~~such~~ restitution may include payment of any other costs, including attorney's fees incurred by the victim in clearing the victim's credit history or credit rating, or any costs incurred in connection with any civil or administrative proceeding to satisfy any debt, lien, or other obligation of the victim arising as the result of the actions of the defendant.

(b) The sentencing court may issue such orders as are necessary to correct any public record that contains false information given in violation of this section.

(14)~~(10)~~ Prosecutions for violations of this section may be brought on behalf of the state by any state attorney or by the statewide prosecutor.

(15)~~(11)~~ The Legislature finds that, in the absence of evidence to the contrary, the location where a victim gives or fails to give consent to the use of personal identification information is the county where the victim generally resides.

(16)~~(12)~~ Notwithstanding any other provision of law, 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.

(17)~~(13)~~ A prosecution of an offense prohibited under subsection (2), subsection (6), or subsection (7) must be commenced within 3 years after the offense occurred. However, a prosecution may be commenced within 1 year after discovery of the offense by an aggrieved party, or by a person who has a legal duty to represent the aggrieved party and who is not a party to the offense, if such prosecution is commenced within 5 years after the violation occurred.

Section 2. Section 817.5681, Florida Statutes, is created to read:

817.5681 Breach of security concerning confidential personal information in third-party possession; administrative penalties.--

(1)(a) Any person who conducts business in this state and maintains computerized data in a system that includes personal information shall disclose any breach of the security of the system, following discovery or notification of the breach in the security of the data, to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made most expeditiously and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (3) and paragraph (9)(a), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. Disclosure of the breach may only be delayed indefinitely following its discovery under subsection (3). Otherwise, disclosure must be made no later than 30 days following the discovery of the breach.

(b) Any person required to make disclosures under paragraph (a) who fails to do so within the time periods provided in this subsection is liable for an administrative fine in the amount of $1,000 for each day the breach goes undisclosed for up to 30 days.

(c) Except as required for investigations under subsection (3), any person required to make disclosures under paragraph (a) who fails to do so is subject to an administrative fine of up to $50,000 for each 30-day period or portion thereof up to 180 days unless acting under a court order. If such disclosure is not made within 180 days, any person required to make such disclosures under paragraph (a) who fails to do so is subject to an administrative fine of up to $500,000.

(d) The disclosure required under this subsection must be made by each person in the state in possession of computerized data. However, the administrative sanctions for nondisclosure provided in this subsection shall not apply in the case of computerized information in the custody of any governmental agency or political subdivision, unless that governmental agency or political subdivision has entered into a contract with a contractor or third-party administrator to provide governmental services. In such case, the contractor or third-party administrator shall be a person to whom the administrative sanctions provided in this subsection apply, provided such contractor or third-party administrator found in violation of the nondisclosure restrictions in this section may not bring an action for contribution or set-off available against the employing agency or subdivision.

(2)(a) Any person who maintains computerized data that includes personal information on behalf of another business entity shall notify the business entity for which the information is maintained of any breach of the security of the data within 72 hours after the discovery of the breach, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(b) Any person required to make disclosures under paragraph (a) who fails to do so within the time periods provided in this subsection is liable for an administrative fine in the amount of $1,000 for each day the breach goes undisclosed for up to 30 days.

(c) Except as required for investigations under subsection (3), any person required to make disclosures under paragraph (a) who fails to do so is subject to an administrative fine of up to $50,000 for each 30-day period or portion thereof up to 180 days unless acting under court order. If such disclosure is not made within 180 days, any person required to make disclosures under paragraph (a) who fails to do so is subject to an administrative fine of up to $500,000.

(d) The disclosure required under this subsection must be made by each person in the state in possession of computerized data. However, the administrative sanctions for nondisclosure provided in this subsection shall not apply in the case of computerized information in the custody of any governmental agency or political subdivision unless that governmental agency or political subdivision has entered into a contract with a contractor or third-party administrator to provide governmental services. In such case, the contractor or third-party administrator shall be a person to whom the administrative sanctions provided in this subsection would apply, provided such contractor or third-party administrator found in violation of the nondisclosure restrictions in this subsection may not bring an action for contribution or set-off available against the employing agency or subdivision.

(3) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that the notification will not compromise the investigation. The delay in notification allowed under this subsection shall not exceed 90 days unless ordered by a court of competent jurisdiction.

(4) For purposes of this section, the term "breach of the security of the system" means unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by the person. Good faith acquisition of personal information by an employee or agent of a person for the purposes of the person is not a breach of the security of the system, provided the information is not used for a purpose unrelated to the business or subject to further unauthorized disclosure.

(5) For purposes of this section, the term "personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when the data elements are not encrypted:

(a) Social security number.

<u>(b) Driver's license number or Florida identification card number.</u>

<u>(c) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.</u>

<u>(6) For purposes of this section, notice may be provided by one of the following methods:</u>

<u>(a) Written notice;</u>

<u>(b) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. s. 7001; or</u>

<u>(c) Substitute notice, if the person demonstrates that the cost of providing notice would exceed $250,000, the affected class of subject persons to be notified exceeds 500,000, or the person does not have sufficient contact information. Substitute notice shall consist of all of the following:</u>

<u>1. Electronic mail notice when the person has an electronic mail address for the subject person.</u>

<u>2. Conspicuous posting of the notice on the person's website, if the person maintains a website.</u>

<u>3. Notification to major statewide media.</u>

<u>(7) For purposes of this section, the term "unauthorized person" means any person who is not the person to whom the personal information belongs and who does not have permission from or a password issued by the person who stores the computerized data to acquire such data.</u>

<u>(8) Notwithstanding subsection (6), a person who maintains his or her own notification procedures as part of an information security or privacy policy for the treatment of</u>

personal information and which procedures are otherwise consistent with the timing requirements of this part shall be deemed to be in compliance with the notification requirements of this section if the person notifies subject persons in accordance with its procedures in the event of a breach of security of the system.

(9)(a) Notwithstanding subsection (2), notification is not required if, after an appropriate investigation and after consultation with relevant federal, state, and local agencies responsible for law enforcement, the person reasonably determines that the breach has not and will not likely result in harm to the individuals whose personal information has been acquired and accessed. Such a determination must be documented in writing and the documentation must be maintained for 5 years.

(b) Any person required to document a failure to notify affected persons who fails to document the failure as required in this subsection or who, if documentation was created, fails to maintain the documentation for the full 5 years as required in this subsection is liable for an administrative fine in the amount of up to $50,000 for such failure.

(c) The documentation and maintenance of documentation required under this subsection must be made by each person in the state in possession of computerized data. However, the administrative sanctions outlined in this subsection shall not apply in the case of computerized information in the custody of any governmental agency or political subdivision, unless that governmental agency or political subdivision has entered into a contract with a contractor or third-party administrator to provide governmental services. In such case, the contractor or third-party administrator shall be a person to whom the administrative sanctions outlined in this subsection apply, provided such contractor or third-party administrator found in violation of the documentation and maintenance of documentation requirements in this subsection may not bring an action for contribution or set-off available against the employing agency or subdivision.

(10) The Department of Legal Affairs may institute proceedings to assess and collect the fines provided in this section.

Section 3. This act shall take effect July 1, 2005.

STATEMENT OF SUBSTANTIAL CHANGES CONTAINED IN
COMMITTEE SUBSTITUTE FOR
Senate Bill 978

The committee substitute makes the following changes to the underlying bill:

-- Removes new s. 501.165, F.S., on fraudulent use of personal identification information;

-- Removes proposed language that would have made it a crime to disclose, sell, or transfer, or attempt to disclose, sell, or transfer, personal identification information without that person's consent;

-- Removes proposed subsection that would have made a violation of the identity theft statute also a violation under the Florida Deceptive and Unfair Trade Practices Act; and

-- Deletes revisions to cross-referenced criminal punishment statute that would have been necessary to provide for proposed changes to statute that were removed.