AN ACT

relating to the prevention and punishment of identity theft and the
rights of certain victims of identity theft; providing penalties.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF TEXAS:

SECTION 1. (a) Chapter 2, Code of Criminal Procedure, is
amended by adding Article 2.29 to read as follows:

Art. 2.29. REPORT REQUIRED IN CONNECTION WITH FRAUDULENT
USE OR POSSESSION OF IDENTIFYING INFORMATION. (a) A peace officer
who is alleged to have been a victim of violation of Section 32.51, Penal Code, shall make a written report to the law enforcement agency
that employs the peace officer that includes the following
information:

(1) the name of the victim;

(2) the name of the suspect, if known;

(3) the type of identifying information obtained,

possessed, transferred, or used in violation of Section 32.51,
Penal Code; and

(4) the results of any investigation.

(b) On the victim's request, the law enforcement agency
shall provide the report created under Subsection (a) to the
victim. In providing the report, the law enforcement agency shall
redact any otherwise confidential information that is included in
the report, other than the information described by Subsection (a).

(b) The change in law made by this section applies only to
the investigation of an offense committed on or after September 1, 2005. The investigation of an offense committed before September 1, 2005, is covered by the law in effect when the offense was committed, and the former law is continued in effect for that purpose. For purposes of this subsection, an offense is committed before September 1, 2005, if any element of the offense occurs before that date.

SECTION 2. Title 4, Business & Commerce Code, is amended by adding Chapter 48 to read as follows:

CHAPTER 48. UNAUTHORIZED USE OF IDENTIFYING INFORMATION

SUBCHAPTER A. GENERAL PROVISIONS

Sec. 48.001. SHORT TITLE. This chapter may be cited as the Identity Theft Enforcement and Protection Act.

Sec. 48.002. DEFINITIONS. In this chapter:

(1) "Personal identifying information" means information that alone or in conjunction with other information identifies an individual, including an individual's:

(A) name, social security number, date of birth, or government-issued identification number;

(B) mother's maiden name;

(C) unique biometric data, including the individual's fingerprint, voice print, and retina or iris image;

(D) unique electronic identification number, address, or routing code; and

(E) telecommunication access device.

(2) "Sensitive personal information":

(A) means an individual's first name or first
initial and last name in combination with any one or more of the
following items, if the name and the items are not encrypted:

(i) social security number;

(ii) driver's license number or government-issued identification number; or

(iii) 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; and

(B) does not include publicly available information that is lawfully made available to the general public from the federal government or a state or local government.

(3) "Telecommunication access device" has the meaning assigned by Section 32.51, Penal Code.

(4) "Victim" means a person whose identifying information is used by an unauthorized person.

[Sections 48.003-48.100 reserved for expansion]
U.S.C. Section 1681 et seq.); and

(2) is in compliance with that Act and regulations adopted under that Act.

(c) This section does not apply to:

(1) a financial institution as defined by 15 U.S.C. Section 6809; or

(2) a covered entity as defined by Section 601.001 or 602.001, Insurance Code.

Sec. 48.102. BUSINESS DUTY TO PROTECT AND SAFEGUARD SENSITIVE PERSONAL INFORMATION. (a) A business shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect and safeguard from unlawful use or disclosure any sensitive personal information collected or maintained by the business in the regular course of business.

(b) A business shall destroy or arrange for the destruction of customer records containing sensitive personal information within the business’s custody or control that are not to be retained by the business by:

(1) shredding;

(2) erasing; or

(3) otherwise modifying the sensitive personal information in the records to make the information unreadable or undecipherable through any means.

(c) This section does not apply to a financial institution as defined by 15 U.S.C. Section 6809.

Sec. 48.103. NOTIFICATION REQUIRED FOLLOWING BREACH OF
SECURITY OF COMPUTERIZED DATA. (a) In this section, "breach of system security" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person. Good faith acquisition of sensitive personal information by an employee or agent of the person or business for the purposes of the person is not a breach of system security unless the sensitive personal information is used or disclosed by the person in an unauthorized manner.

(b) A person that conducts business in this state and owns or licenses computerized data that includes sensitive personal information shall disclose any breach of system security, after discovering or receiving notification of the breach, to any resident of this state whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made as quickly as possible, except as provided by Subsection (d) or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(c) Any person that maintains computerized data that includes sensitive personal information that the person does not own shall notify the owner or license holder of the information of any breach of system security immediately after discovering the breach, if the sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(d) A person may delay providing notice as required by Subsections (b) and (c) at the request of a law enforcement agency.
that determines that the notification will impede a criminal investigation. The notification shall be made as soon as the law enforcement agency determines that it will not compromise the investigation.

(e) A person may give notice as required by Subsections (b) and (c) by providing:

(1) written notice;

(2) electronic notice, if the notice is provided in accordance with 15 U.S.C. Section 7001; or

(3) notice as provided by Subsection (f).

(f) If the person or business demonstrates that the cost of providing notice would exceed $250,000, the number of affected persons exceeds 500,000, or the person does not have sufficient contact information, the notice may be given by:

(1) electronic mail, if the person has an electronic mail address for the affected persons;

(2) conspicuous posting of the notice on the person's website; or

(3) notice published in or broadcast on major statewide media.

(g) Notwithstanding Subsection (e), a person that maintains its own notification procedures as part of an information security policy for the treatment of sensitive personal information that complies with the timing requirements for notice under this section complies with this section if the person notifies affected persons in accordance with that policy.

(h) If a person is required by this section to notify at one
time more than 10,000 persons of a breach of system security, the
person shall also notify, without unreasonable delay, all consumer
reporting agencies, as defined by 15 U.S.C. Section 1681a, that
maintain files on consumers on a nationwide basis, of the timing,
distribution, and content of the notices.

[Sections 48.104-48.200 reserved for expansion]

SUBCHAPTER C. REMEDIES AND OFFENSES

Sec. 48.201. CIVIL PENALTY; INJUNCTION. (a) A person who
violates this chapter is liable to the state for a civil penalty of
at least $2,000 but not more than $50,000 for each violation. The
attorney general may bring suit to recover the civil penalty
imposed by this subsection.

(b) If it appears to the attorney general that a person is
engaging in, has engaged in, or is about to engage in conduct that
violates this chapter, the attorney general may bring an action in
the name of this state against the person to restrain the violation
by a temporary restraining order or a permanent or temporary
injunction.

(c) An action brought under Subsection (b) shall be filed in
a district court in Travis County or:

(1) in any county in which the violation occurred; or
(2) in the county in which the victim resides,
regardless of whether the alleged violator has resided, worked, or
done business in the county in which the victim resides.

(d) The plaintiff in an action under this section is not
required to give a bond. The court may also grant any other
equitable relief that the court considers appropriate to prevent
any additional harm to a victim of identity theft or a further
violation of this chapter or to satisfy any judgment entered
against the defendant, including the issuance of an order to
appoint a receiver, sequester assets, correct a public or private
record, or prevent the dissipation of a victim's assets.

(e) The attorney general is entitled to recover reasonable
expenses incurred in obtaining injunctive relief, civil penalties,
or both, under this section, including reasonable attorney's fees,
court costs, and investigatory costs. Amounts collected by the
attorney general under this section shall be deposited in the
general revenue fund and may be appropriated only for the
investigation and prosecution of other cases under this chapter.

(f) The fees associated with an action under this section
are the same as in a civil case, but the fees may be assessed only
against the defendant.

Sec. 48.202. COURT ORDER TO DECLARE INDIVIDUAL A VICTIM OF
IDENTITY THEFT. (a) A person who is injured by a violation of
Section 48.101 or who has filed a criminal complaint alleging
commission of an offense under Section 32.51, Penal Code, may file
an application with a district court for the issuance of a court
order declaring that the person is a victim of identity theft. A
person may file an application under this section regardless of
whether the person is able to identify each person who allegedly
transferred or used the person's identifying information in an
unlawful manner.

(b) A person is presumed to be a victim of identity theft
under this section if the person charged with an offense under
Section 32.51, Penal Code, is convicted of the offense.

(c) After notice and hearing, if the court is satisfied by a preponderance of the evidence that the applicant has been injured by a violation of Section 48.101 or is the victim of an offense under Section 32.51, Penal Code, the court shall enter an order containing:

(1) a declaration that the person filing the application is a victim of identity theft resulting from a violation of Section 48.101 or an offense under Section 32.51, Penal Code, as appropriate;

(2) any known information identifying the violator or person charged with the offense;

(3) the specific personal identifying information and any related document used to commit the alleged violation or offense; and

(4) information identifying any financial account or transaction affected by the alleged violation or offense, including:

(A) the name of the financial institution in which the account is established or of the merchant involved in the transaction, as appropriate;

(B) any relevant account numbers;

(C) the dollar amount of the account or transaction affected by the alleged violation or offense; and

(D) the date of the alleged violation or offense.

(d) An order rendered under this section must be sealed because of the confidential nature of the information required to
be included in the order. The order may be opened and the order or a
copy of the order may be released only:

(1) to the proper officials in a civil proceeding
brought by or against the victim arising or resulting from a
violation of this chapter, including a proceeding to set aside a
judgment obtained against the victim;
(2) to the victim for the purpose of submitting the
copy of the order to a governmental entity or private business to:
   (A) prove that a financial transaction or account
of the victim was directly affected by a violation of this chapter
or the commission of an offense under Section 32.51, Penal Code; or
   (B) correct any record of the entity or business
that contains inaccurate or false information as a result of the
violation or offense;
(3) on order of the judge; or
(4) as otherwise required or provided by law.

(e) A court at any time may vacate an order issued under this
section if the court finds that the application or any information
submitted to the court by the applicant contains a fraudulent
misrepresentation or a material misrepresentation of fact.

(f) A copy of an order provided to a person under Subsection
(d)(1) must remain sealed throughout and after the civil
proceeding. Information contained in a copy of an order provided to
a governmental entity or business under Subsection (d)(2) is
confidential and may not be released to another person except as
otherwise required or provided by law.
Section 48.101 is a deceptive trade practice actionable under Subchapter E, Chapter 17.

SECTION 3. This Act takes effect September 1, 2005.
S.B. No. 122

President of the Senate

I hereby certify that S.B. No. 122 passed the Senate on April 21, 2005, by the following vote: Yeas 31, Nays 0; May 17, 2005, Senate refused to concur in House amendments and requested appointment of Conference Committee; May 20, 2005, House granted request of the Senate; May 26, 2005, Senate adopted Conference Committee Report by the following vote: Yeas 31, Nays 0.

Speaker of the House

Secretary of the Senate

I hereby certify that S.B. No. 122 passed the House, with amendments, on May 13, 2005, by a non-record vote; May 20, 2005, House granted request of the Senate for appointment of Conference Committee; May 27, 2005, House adopted Conference Committee Report by the following vote: Yeas 142, Nays 0, two present not voting.

Chief Clerk of the House

Approved:

__________________________
Date

__________________________
Governor