

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 to whom an alleged violation of Section 32.51, Penal Code, is reported 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

1 the investigation of an offense committed on or after September 1,
2 2005. The investigation of an offense committed before September
3 1, 2005, is covered by the law in effect when the offense was
4 committed, and the former law is continued in effect for that
5 purpose. For purposes of this subsection, an offense is committed
6 before September 1, 2005, if any element of the offense occurs
7 before that date.

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

10 CHAPTER 48. UNAUTHORIZED USE OF IDENTIFYING INFORMATION

11 SUBCHAPTER A. GENERAL PROVISIONS

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

14 Sec. 48.002. DEFINITIONS. In this chapter:

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

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

20 (B) mother's maiden name;

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

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

25 (E) telecommunication access device.

26 (2) "Sensitive personal information":

27 (A) means an individual's first name or first

1 initial and last name in combination with any one or more of the
2 following items, if the name and the items are not encrypted:

3 (i) social security number;

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

6 (iii) account number or credit or debit
7 card number in combination with any required security code, access
8 code, or password that would permit access to an individual's
9 financial account; and

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

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

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

17 [Sections 48.003-48.100 reserved for expansion]

18 SUBCHAPTER B. IDENTITY THEFT

19 Sec. 48.101. UNAUTHORIZED USE OR POSSESSION OF PERSONAL
20 IDENTIFYING INFORMATION. (a) A person may not obtain, possess,
21 transfer, or use personal identifying information of another person
22 without the other person's consent and with intent to obtain a good,
23 a service, insurance, an extension of credit, or any other thing of
24 value in the other person's name.

25 (b) It is a defense to an action brought under this section
26 that an act by a person:

27 (1) is covered by the Fair Credit Reporting Act (15

1 U.S.C. Section 1681 et seq.); and

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

4 (c) This section does not apply to:

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

7 (2) a covered entity as defined by Section 601.001 or
8 602.001, Insurance Code.

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

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

20 (1) shredding;

21 (2) erasing; or

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

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

27 Sec. 48.103. NOTIFICATION REQUIRED FOLLOWING BREACH OF

1 SECURITY OF COMPUTERIZED DATA. (a) In this section, "breach of
2 system security" means unauthorized acquisition of computerized
3 data that compromises the security, confidentiality, or integrity
4 of sensitive personal information maintained by a person. Good
5 faith acquisition of sensitive personal information by an employee
6 or agent of the person or business for the purposes of the person is
7 not a breach of system security unless the sensitive personal
8 information is used or disclosed by the person in an unauthorized
9 manner.

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

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

26 (d) A person may delay providing notice as required by
27 Subsections (b) and (c) at the request of a law enforcement agency

1 that determines that the notification will impede a criminal
2 investigation. The notification shall be made as soon as the law
3 enforcement agency determines that it will not compromise the
4 investigation.

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

7 (1) written notice;

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

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

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

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

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

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

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

27 (h) If a person is required by this section to notify at one

1 time more than 10,000 persons of a breach of system security, the
2 person shall also notify, without unreasonable delay, all consumer
3 reporting agencies, as defined by 15 U.S.C. Section 1681a, that
4 maintain files on consumers on a nationwide basis, of the timing,
5 distribution, and content of the notices.

6 [Sections 48.104-48.200 reserved for expansion]

7 SUBCHAPTER C. REMEDIES AND OFFENSES

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

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

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

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

25 (d) The plaintiff in an action under this section is not
26 required to give a bond. The court may also grant any other
27 equitable relief that the court considers appropriate to prevent

1 any additional harm to a victim of identity theft or a further
2 violation of this chapter or to satisfy any judgment entered
3 against the defendant, including the issuance of an order to
4 appoint a receiver, sequester assets, correct a public or private
5 record, or prevent the dissipation of a victim's assets.

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

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

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

26 (b) A person is presumed to be a victim of identity theft
27 under this section if the person charged with an offense under

1 Section 32.51, Penal Code, is convicted of the offense.

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

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

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

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

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

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

22 (B) any relevant account numbers;

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

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

26 (d) An order rendered under this section must be sealed
27 because of the confidential nature of the information required to

1 be included in the order. The order may be opened and the order or a
2 copy of the order may be released only:

3 (1) to the proper officials in a civil proceeding
4 brought by or against the victim arising or resulting from a
5 violation of this chapter, including a proceeding to set aside a
6 judgment obtained against the victim;

7 (2) to the victim for the purpose of submitting the
8 copy of the order to a governmental entity or private business to:

9 (A) prove that a financial transaction or account
10 of the victim was directly affected by a violation of this chapter
11 or the commission of an offense under Section 32.51, Penal Code; or

12 (B) correct any record of the entity or business
13 that contains inaccurate or false information as a result of the
14 violation or offense;

15 (3) on order of the judge; or

16 (4) as otherwise required or provided by law.

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

21 (f) A copy of an order provided to a person under Subsection
22 (d)(1) must remain sealed throughout and after the civil
23 proceeding. Information contained in a copy of an order provided to
24 a governmental entity or business under Subsection (d)(2) is
25 confidential and may not be released to another person except as
26 otherwise required or provided by law.

27 Sec. 48.203. DECEPTIVE TRADE PRACTICE. A violation of

1 Section 48.101 is a deceptive trade practice actionable under
2 Subchapter E, Chapter 17.

3 SECTION 3. This Act takes effect September 1, 2005.

President of the Senate

Speaker of the House

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.

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