BUSINESS AND COMMERCE CODE

TITLE 11. PERSONAL IDENTITY INFORMATION

SUBTITLE B. IDENTITY THEFT

CHAPTER 521. UNAUTHORIZED USE OF IDENTIFYING INFORMATION

SUBCHAPTER A. GENERAL PROVISIONS

Sec. 521.001. SHORT TITLE. This chapter may be cited as the Identity Theft Enforcement and Protection Act.

Added by Acts 2007, 80th Leg., R.S., Ch. 885 (H.B. 2278), Sec. 2.01, eff. April 1, 2009.

Sec. 521.002. DEFINITIONS. (a) 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 as defined by Section 32.51, Penal Code.

(2) "Sensitive personal information" means, subject to Subsection (b):

(A) 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; or

(B) information that identifies an individual and relates to:

(i) the physical or mental health or condition of the individual;

(ii) the provision of health care to the individual; or

(iii) payment for the provision of health care to the individual.

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

(b) For purposes of this chapter, the term "sensitive personal information" does not include publicly available information that is lawfully made available to the public from the federal government or a state or local government.

Added by Acts 2007, 80th Leg., R.S., Ch. 885 (H.B. 2278), Sec. 2.01, eff. April 1, 2009.

Amended by:

Acts 2009, 81st Leg., R.S., Ch. 419 (H.B. 2004), Sec. 1, eff. September 1, 2009.

SUBCHAPTER B. IDENTITY THEFT

Sec. 521.051. UNAUTHORIZED USE OR POSSESSION OF PERSONAL IDENTIFYING INFORMATION. (a) A person may not obtain, possess, transfer, or use personal identifying information of another person without the other person's consent or effective consent and with intent to obtain a good, a service, insurance, an extension of credit, or any other thing of value in the other person's name.

(a-1) For purposes of this section, "effective consent" includes consent given by a person legally authorized to act on behalf of the person from whom consent is required. Consent is not effective if:

(1) induced by force, threat, fraud, or coercion; or

(2) given by a person who by reason of youth, mental illness, or intellectual disability is known by the actor to be unable to make reasonable decisions.

(b) It is a defense to an action brought under this section

that an act by a person:

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

Added by Acts 2007, 80th Leg., R.S., Ch. 885 (H.B. 2278), Sec. 2.01, eff. April 1, 2009.

Amended by:

Acts 2021, 87th Leg., R.S., Ch. 143 (H.B. 3529), Sec. 1, eff. September 1, 2021.

Sec. 521.052. BUSINESS DUTY TO PROTECT SENSITIVE PERSONAL INFORMATION. (a) A business shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect 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 indecipherable through any means.

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

(d) As used in this section, "business" includes a nonprofit athletic or sports association.

Added by Acts 2007, 80th Leg., R.S., Ch. 885 (H.B. 2278), Sec. 2.01, eff. April 1, 2009.

Amended by:

Acts 2009, 81st Leg., R.S., Ch. 419 (H.B. 2004), Sec. 2, eff. September 1, 2009.

Sec. 521.053. 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, including data that is encrypted if the person accessing the data has the key required to decrypt the data. Good faith acquisition of sensitive personal information by an employee or agent of the person for the purposes of the person is not a breach of system security unless the person uses or discloses the sensitive personal information in an unauthorized manner.

(b) A person who 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 individual whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made without unreasonable delay and in each case not later than the 60th day after the date on which the person determines that the breach occurred, 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.

(b-1) If the individual whose sensitive personal information was or is reasonably believed to have been acquired by an unauthorized person is a resident of a state that requires a person described by Subsection (b) to provide notice of a breach of system security, the notice of the breach of system security required under Subsection (b) may be provided under that state's law or under Subsection (b).

(c) Any person who maintains computerized data that includes sensitive personal information not owned by the person 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 Subsection (b) or (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 the notification will not compromise the investigation.

(e) A person may give notice as required by Subsection (b) or (c) by providing:

(1) written notice at the last known address of the individual;

(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 required to give notice under Subsection (b) or (c) 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 electronic mail addresses 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 who maintains the person's 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 each consumer reporting agency, as defined by 15 U.S.C. Section 1681a, that maintains files on consumers on a nationwide basis, of the timing, distribution, and content of the

notices. The person shall provide the notice required by this subsection without unreasonable delay.

(i) A person who is required to disclose or provide notification of a breach of system security under this section shall notify the attorney general of that breach as soon as practicable and not later than the 30th day after the date on which the person determines that the breach occurred if the breach involves at least 250 residents of this state. The notification under this subsection must be submitted electronically using a form accessed through the attorney general's Internet website and must include:

(1) a detailed description of the nature and circumstances of the breach or the use of sensitive personal information acquired as a result of the breach;

(2) the number of residents of this state affected by the breach at the time of notification;

(3) the number of affected residents that have been sent a disclosure of the breach by mail or other direct method of communication at the time of notification;

(4) the measures taken by the person regarding the breach;

(5) any measures the person intends to take regarding the breach after the notification under this subsection; and

(6) information regarding whether law enforcement is engaged in investigating the breach.

(j) The attorney general shall post on the attorney general's publicly accessible Internet website:

(1) an electronic form for submitting a notification under Subsection (i); and

(2) a listing of the notifications received by the attorney general under Subsection (i), excluding any sensitive personal information that may have been reported to the attorney general under that subsection, any information that may compromise a data system's security, and any other information reported to the attorney general that is made confidential by law. The attorney general shall:

(A) update the listing not later than the 30th

day after the date the attorney general receives notification of a new breach of system security;

(B) remove a notification from the listing not later than the first anniversary of the date the attorney general added the notification to the listing if the person who provided the notification has not notified the attorney general of any additional breaches under Subsection (i) during that period; and

(C) maintain only the most recently updated listing on the attorney general's website.

Added by Acts 2007, 80th Leg., R.S., Ch. 885 (H.B. 2278), Sec. 2.01, eff. April 1, 2009.

Amended by:

Acts 2009, 81st Leg., R.S., Ch. 419 (H.B. 2004), Sec. 3, eff. September 1, 2009.

Acts 2011, 82nd Leg., R.S., Ch. 1126 (H.B. 300), Sec. 14, eff. September 1, 2012.

Acts 2013, 83rd Leg., R.S., Ch. 1368 (S.B. 1610), Sec. 1, eff. June 14, 2013.

Acts 2019, 86th Leg., R.S., Ch. 1326 (H.B. 4390), Sec. 1, eff. January 1, 2020.

Acts 2021, 87th Leg., R.S., Ch. 496 (H.B. 3746), Sec. 1, eff. September 1, 2021.

Acts 2023, 88th Leg., R.S., Ch. 246 (S.B. 768), Sec. 1, eff. September 1, 2023.

SUBCHAPTER C. COURT ORDER DECLARING INDIVIDUAL A VICTIM OF IDENTITY THEFT

Sec. 521.101. APPLICATION FOR COURT ORDER TO DECLARE INDIVIDUAL A VICTIM OF IDENTITY THEFT. (a) A person who is injured by a violation of Section 521.051 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 an order declaring that the person is a victim of identity theft.

(b) 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.

Added by Acts 2007, 80th Leg., R.S., Ch. 885 (H.B. 2278), Sec. 2.01, eff. April 1, 2009.

Sec. 521.102. PRESUMPTION OF APPLICANT'S STATUS AS VICTIM. An applicant under Section 521.101 is presumed to be a victim of identity theft under this subchapter if the person charged with an offense under Section 32.51, Penal Code, is convicted of the offense.

Added by Acts 2007, 80th Leg., R.S., Ch. 885 (H.B. 2278), Sec. 2.01, eff. April 1, 2009.

Sec. 521.103. ISSUANCE OF ORDER; CONTENTS. (a) After notice and hearing, if the court is satisfied by a preponderance of the evidence that an applicant under Section 521.101 has been injured by a violation of Section 521.051 or is the victim of an offense under Section 32.51, Penal Code, the court shall enter an order declaring that the applicant is a victim of identity theft resulting from a violation of Section 521.051 or an offense under Section 32.51, Penal Code, as appropriate.

(b) An order under this section must contain:

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

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

(3) 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.

Added by Acts 2007, 80th Leg., R.S., Ch. 885 (H.B. 2278), Sec. 2.01, eff. April 1, 2009.

Sec. 521.104. CONFIDENTIALITY OF ORDER. (a) An order issued under Section 521.103 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.

(b) A copy of an order provided to a person under Subsection (a)(1) must remain sealed throughout and after the civil proceeding.

(c) Information contained in a copy of an order provided to a governmental entity or business under Subsection (a)(2) is confidential and may not be released to another person except as otherwise required or provided by law.

Added by Acts 2007, 80th Leg., R.S., Ch. 885 (H.B. 2278), Sec. 2.01, eff. April 1, 2009.

Sec. 521.105. GROUNDS FOR VACATING ORDER. A court at any time may vacate an order issued under Section 521.103 if the court finds that the application filed under Section 521.101 or any information submitted to the court by the applicant contains a fraudulent misrepresentation or a material misrepresentation of

fact.

Added by Acts 2007, 80th Leg., R.S., Ch. 885 (H.B. 2278), Sec. 2.01, eff. April 1, 2009.

SUBCHAPTER D. REMEDIES

Sec. 521.151. CIVIL PENALTY; INJUNCTION. (a) A person who violates this chapter is liable to this state for a civil penalty of at least $2,000 but not more than $50,000 for each violation. The attorney general may bring an action to recover the civil penalty imposed under this subsection.

(a-1) In addition to penalties assessed under Subsection (a), a person who fails to take reasonable action to comply with Section 521.053(b) is liable to this state for a civil penalty of not more than $100 for each individual to whom notification is due under that subsection for each consecutive day that the person fails to take reasonable action to comply with that subsection. Civil penalties under this section may not exceed $250,000 for all individuals to whom notification is due after a single breach. The attorney general may bring an action to recover the civil penalties imposed under 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 the state against the person to restrain the violation by a temporary restraining order or by a permanent or temporary injunction.

(c) An action brought under Subsection (b) must 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 transacted business in the county in which the victim resides.

(d) The attorney general is not required to give a bond in an action under this section.

(e) In an action under this section, the court may grant any other equitable relief that the court considers appropriate to:

(1) prevent any additional harm to a victim of identity theft or a further violation of this chapter; or

(2) satisfy any judgment entered against the defendant, including issuing an order to appoint a receiver, sequester assets, correct a public or private record, or prevent the dissipation of a victim's assets.

(f) The attorney general is entitled to recover reasonable expenses, including reasonable attorney's fees, court costs, and investigatory costs, incurred in obtaining injunctive relief or civil penalties, or both, under this section. 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.

(g) 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.

Added by Acts 2007, 80th Leg., R.S., Ch. 885 (H.B. 2278), Sec. 2.01, eff. April 1, 2009.

Amended by:

Acts 2011, 82nd Leg., R.S., Ch. 1126 (H.B. 300), Sec. 15, eff. September 1, 2012.

Sec. 521.152. DECEPTIVE TRADE PRACTICE. A violation of Section 521.051 is a deceptive trade practice actionable under Subchapter E, Chapter 17.

Added by Acts 2007, 80th Leg., R.S., Ch. 885 (H.B. 2278), Sec. 2.01, eff. April 1, 2009.