

## **Texas Business and Commerce Code**

### **Title 11 – Personal Identity Information**

#### **Chapter 521 – Protection of Driver’s License and Social Security Numbers**

##### **§ 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.

##### **§ 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 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 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;
- (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.

### **§ 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.

(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.