Tex. Bus. & Com. Code § 521.053

This document is current through the 2023 Regular Session; the 1st C.S.; the 2nd C.S.; the 3rd C.S. and the 4th C.S. of the 88th Legislature; and the November 7, 2023 general election results.

Texas Statutes & Codes Annotated by LexisNexis® > Business and Commerce Code > Title 11 Personal Identity Information (Subts. A — C) > Subtitle B Identity Theft (Chs. 521 — 523) > Chapter 521 Unauthorized Use of Identifying Information (Subchs. A — D) > Subchapter B Identity Theft (§§ 521.051 — 521.053)

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.

History

Enacted by Acts 2007, 80th Leg., ch. 885 (H.B. 2278), § 2.01, effective April 1, 2009; am. Acts 2009, 81st Leg., ch. 419 (H.B. 2004), § 3, effective September 1, 2009; am. Acts 2011, 82nd Leg., ch. 1126 (H.B. 300), § 14, effective September 1, 2012; am. Acts 2013, 83rd Leg., ch. 1368 (S.B. 1610), § 1, effective June 14, 2013; Acts 2019, 86th Leg., ch. 1326 (H.B. 4390), § 1, effective January 1, 2020; Acts 2021, 87th Leg., ch. 496 (H.B. 3746), § 1, effective September 1, 2021; Acts 2023, 88th Leg., ch. 246 (S.B. 768), § 1, effective September 1, 2023.