BILL ANALYSIS

Senate Research Center

H.B. 3746
By: Capriglione (Nelson)
Business & Commerce
5/15/2021
Engrossed

AUTHOR'S / SPONSOR'S STATEMENT OF INTENT

Last session, the Texas Legislature enacted legislation requiring entities that experience a security breach affecting at least 250 Texans to notify the attorney general of the breach. Since implementation of the bill, more than 30 million Texans have had their data compromised by a security breach. This number is higher than the United States Census Bureau's most recent population estimates for the state, meaning some individuals have had their personal information compromised more than once.

H.B. 3746 seeks to make information regarding these breaches more publicly accessible by requiring the attorney general to post a comprehensive list of the security breach notices on the attorney general's website. The bill also revises the required contents of the notice to provide the attorney general a more accurate picture of how many security breach victims are sufficiently notified that their data has been compromised.

H.B. 3746 amends current law relating to certain notifications required following a breach of security of computerized data.

RULEMAKING AUTHORITY

This bill does not expressly grant any additional rulemaking authority to a state officer, institution, or agency.

SECTION BY SECTION ANALYSIS

SECTION 1. Amends Section 521.053, Business & Commerce Code, by amending Subsection (i) and adding Subsection (j), as follows:

> (i) Requires that the notification of a breach of system security under this subsection include 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. Makes nonsubstantive changes.
>
> (j) Requires the attorney general to post on the attorney general's publicly accessible Internet website 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. Requires the attorney general to:
>
> > (1) update the listing not later than the 30th day after the date the attorney general receives notification of a new breach of system security;
> >
> > (2) 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

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

SECTION 2. Effective date: September 1, 2021.