

SUBJECT: Requiring certain notification of breaches of secure computerized data

COMMITTEE: Business and Industry — favorable, without amendment

VOTE: 7 ayes — C. Turner, Hefner, Cain, Crockett, Lambert, Ordaz Perez,  
Patterson

0 nays

2 absent — Shine, S. Thompson

WITNESSES: For — (*Registered, but did not testify*: Dana Harris, Austin Chamber of  
Commerce; Micah Rodriguez, Credit Union Coalition of Texas; Stephen  
Scurlock, Independent Bankers Association of Texas; Megan Herring,  
Texas Association of Business; Larry Gonzales, Texas Credit Union  
Association; Thomas Parkinson; Calvin Tillman; Al Zito)

Against — None

On — (*Registered, but did not testify*: Servando Esparza, TechNet; Troy  
Alexander, Texas Medical Association)

BACKGROUND: Business and Commerce Code sec. 521.053 requires persons who own,  
license, or maintain computerized data that includes certain sensitive  
personal information to notify the attorney general of a breach of system  
security within a specified time frame if the breach involves at least 250  
residents of the state. The notification must include certain information,  
including a description of the breach and the number of residents of the  
state affected by the breach.

Interested parties have expressed concern that the Office of the Attorney  
General is not receiving sufficient information about Texas residents who  
receive direct notification of a data breach. Concerns also have been  
expressed that the information compiled by the Office of the Attorney  
General is accessible only through a public information request.

**DIGEST:** HB 3746 would require a notification sent to the attorney general regarding a breach of system security under Business and Commerce Code sec. 521.053 to include the number of affected residents that had been sent a disclosure of the breach by mail or other direct method of communication at the time of notification.

The attorney general would have to post on the attorney general's website a comprehensive listing of all received notifications of security system breaches, and the listing would have to be updated within 30 days after notification of a new breach of system security was received. Sensitive personal information and other confidential information that had been reported to the attorney general under sec. 521.053 would be excluded from the listing.

The bill would take effect September 1, 2021.