By: Blanco, et al. S.B. No. 2610
(Capriglione)

A BILL TO BE ENTITLED

AN ACT

relating to a limitation on civil liability of business entities in connection with a breach of system security.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF TEXAS:

SECTION 1. Subtitle C, Title 11, Business & Commerce Code, is amended by adding Chapter 542 to read as follows:

CHAPTER 542. CYBERSECURITY PROGRAM

Sec. 542.001. DEFINITIONS. In this chapter:

(1) "Breach of system security" has the meaning assigned by Section 521.053.

(2) "Exemplary damages" has the meaning assigned by Section 41.001, Civil Practice and Remedies Code.

(3) "Personal identifying information" and "sensitive personal information" have the meanings assigned by Section 521.002.

Sec. 542.002. APPLICABILITY OF CHAPTER. This chapter applies only to a business entity in this state that:

(1) has fewer than 250 employees; and

(2) owns or licenses computerized data that includes sensitive personal information.

Sec. 542.003. CYBERSECURITY PROGRAM SAFE HARBOR: EXEMPLARY DAMAGES PROHIBITED. Notwithstanding any other law, in an action arising from a breach of system security, a person harmed as a result of the breach may not recover exemplary damages from a

business entity to which this chapter applies if the entity demonstrates that at the time of the breach the entity implemented and maintained a cybersecurity program in compliance with Section 542.004.

Sec. 542.004. CYBERSECURITY PROGRAM. (a) For purposes of Section 542.003, a cybersecurity program must:

(1) contain administrative, technical, and physical safeguards for the protection of personal identifying information and sensitive personal information;

(2) conform to an industry-recognized cybersecurity framework as described by Subsection (b);

(3) be designed to:

(A) protect the security of personal identifying information and sensitive personal information;

(B) protect against any threat or hazard to the integrity of personal identifying information and sensitive personal information; and

(C) protect against unauthorized access to or acquisition of personal identifying information and sensitive personal information that would result in a material risk of identity theft or other fraud to the individual to whom the information relates; and

(4) with regard to the scale and scope, meet the following requirements:

(A) for a business entity with fewer than 20 employees, simplified requirements, including password policies and appropriate employee cybersecurity training;

(B) for a business entity with at least 20 employees but fewer than 100 employees, moderate requirements, including the requirements of the Center for Internet Security Controls Implementation Group 1; and

(C) for a business entity with at least 100 employees but fewer than 250 employees, compliance with the requirements of Subsection (b).

(b) A cybersecurity program under this section conforms to an industry-recognized cybersecurity framework for purposes of this section if the program conforms to:

(1) a current version of or any combination of current versions of the following:

(A) the Framework for Improving Critical Infrastructure Cybersecurity published by the National Institute of Standards and Technology (NIST);

(B) the NIST's special publication 800-171;

(C) the NIST's special publications 800-53 and 800-53a;

(D) the Federal Risk and Authorization Management Program's FedRAMP Security Assessment Framework;

(E) the Center for Internet Security Critical Security Controls for Effective Cyber Defense;

(F) the ISO/IEC 27000-series information security standards published by the International Organization for Standardization and the International Electrotechnical Commission;

(G) the Health Information Trust Alliance's Common Security Framework;

(H) the Secure Controls Framework;

(I) the Service Organization Control Type 2 Framework; or

(J) other similar frameworks or standards of the cybersecurity industry;

(2) if the business entity is subject to its requirements, the current version of the following:

(A) the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. Section 1320d et seq.);

(B) Title V, Gramm-Leach-Bliley Act (15 U.S.C. Section 6801 et seq.);

(C) the Federal Information Security Modernization Act of 2014 (Pub. L. No. 113-283); or

(D) the Health Information Technology for Economic and Clinical Health Act (Division A, Title XIII, and Division B, Title IV, Pub. L. No. 111-5); and

(3) if applicable to the business entity, a current version of the Payment Card Industry Data Security Standard.

(c) If any standard described by Subsection (b)(1) is published and updated, a business entity's cybersecurity program continues to meet the requirements of a program under this section if the entity updates the program to meet the updated standard not later than the later of:

(1) the implementation date published in the updated standard; or

(2) the first anniversary of the date on which the updated standard is published.

Sec. 542.005. CONSTRUCTION OF CHAPTER; NO PRIVATE CAUSE OF ACTION. This chapter may not be construed to create a private cause of action or change a common law or statutory duty.

SECTION 2. Section 542.003, Business & Commerce Code, as added by this Act, applies only to a cause of action that accrues on or after the effective date of this Act.

SECTION 3. This Act takes effect September 1, 2025.