By: Blanco S.B. No. 2610

A BILL TO BE ENTITLED

AN ACT

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

Sec. 542.002. APPLICABILITY OF CHAPTER. This chapter applies to a business entity in this state that owns or licenses computerized data that includes sensitive personal information.

Sec. 542.003. LIABILITY FOR DATA BREACH. If a business entity fails to implement reasonable cybersecurity controls and that failure results in a breach of system security, the business entity is liable to a person whose sensitive personal information was stolen in the breach and who suffered economic harm as a result of the theft of the information.

Sec. 542.004. INDUSTRY STANDARD CYBERSECURITY PROGRAM. (a) For purposes of Section 542.003, a business entity has implemented

reasonable cybersecurity controls if the entity has created and maintained a cybersecurity program:

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

(2) that conforms to an industry recognized cybersecurity framework as described by Subsection (b);

(3) that is 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) the scale and scope of which meets the requirements of Subsection (d).

(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, as determined by the Department of Public Safety:

(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, as determined by the Department of Public Safety:

(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, as determined by the Department of Public Safety.

(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 180th day after the date on which the standard is published.

(d) The scale and scope of a cybersecurity program under this section must be based on:

(1) the size and complexity of the business entity;

(2) the nature and scope of the activities of the business entity;

(3) the sensitivity of the personal identifying information or sensitive personal information; and

(4) the cost and availability of tools to improve information security and reduce vulnerabilities.

Sec. 542.005. AUTHORITY OF ATTORNEY GENERAL NOT AFFECTED. This chapter may not be construed to limit the authority of the attorney general to seek any legal or equitable remedy under the laws of this state.

Sec. 542.006. CLASS ACTION CERTIFICATION NOT AFFECTED.

This chapter does not affect the certification of an action as a class action.

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.