General Assembly

Raised Bill No. 6607

January Session, 2021

LCO No. **4480**

Referred to Committee on COMMERCE

Introduced by:
(CE)

AN ACT INCENTIVIZING THE ADOPTION OF CYBERSECURITY STANDARDS FOR BUSINESSES.

Be it enacted by the Senate and House of Representatives in General Assembly convened:

Section 1. (NEW) (*Effective October 1, 2021*) (a) As used in this section:

(1) "Business" means any individual or sole proprietorship, partnership, firm, corporation, trust, limited liability company, limited liability partnership, joint stock company, joint venture, association or other legal entity through which business for profit or not-for-profit is conducted;

(2) "Covered entity" means a business that accesses, maintains, communicates or processes personal information or restricted information in or through one or more systems, networks or services located in or outside this state;

(3) "Data breach" means unauthorized access to and acquisition of computerized data that compromises the security or confidentiality of personal information or restricted information owned by or licensed to a covered entity and that causes, reasonably is believed to have caused

or reasonably is believed will cause a material risk of identity theft or other fraud to a person or property. "Data breach" does not include (A) good faith acquisition of personal information or restricted information by the covered entity's employee or agent for the purposes of the covered entity, provided the personal information or restricted information is not used for an unlawful purpose or subject to further unauthorized disclosure, or (B) acquisition of personal information or restricted information pursuant to a search warrant, subpoena or other court order, or pursuant to a subpoena, order or duty of a regulatory state agency;

(4) "Personal information" means an individual's name, consisting of the individual's first name or first initial and last name, in combination with and linked to any one or more of the following data elements, when the data elements are not encrypted, redacted or altered by any method or technology in such a manner that the data elements are unreadable: (A) Social security number; (B) driver's license number or state identification number; or (C) account number or credit or debit card number, in combination with and linked to any required security code, access code or password that would permit access to an individual's financial account; and

(5) "Restricted information" means any information about an individual, other than personal information, that, alone or in combination with other information, including personal information, can be used to distinguish or trace the individual's identity or that is linked or linkable to an individual, if the information is not encrypted, redacted or altered by any method or technology in such a manner that the information is unreadable, and the breach of which is likely to result in a material risk of identity theft or other fraud to a person or property.

(b) In any cause of action founded in tort that is brought under the laws of this state or in the courts of this state and that alleges that the failure to implement reasonable cybersecurity controls resulted in a data breach concerning personal information or restricted information, it shall be an affirmative defense that a covered entity created, maintained

and complied with a written cybersecurity program that contains administrative, technical and physical safeguards for the protection of personal or restricted information and that reasonably conforms to an industry recognized cybersecurity framework, as described in subsection (c) of this section and that such covered entity designed its cybersecurity program in accordance with the provisions of subsection (d) of this section.

(c) A covered entity's cybersecurity program, as described in subsection (b) of this section, reasonably conforms to an industry recognized cybersecurity framework if:

(1) (A) The cybersecurity program reasonably conforms to the current version of or any combination of the current versions of:

(i) The "Framework for Improving Critical Infrastructure Cybersecurity" published by the National Institute of Standards and Technology;

(ii) The National Institute of Standards and Technology's special publication 800-171;

(iii) The National Institute of Standards and Technology's special publications 800-53 and 800-53a;

(iv) The Federal Risk and Management Program's "FedRAMP Security Assessment Framework";

(v) The Center for Internet Security's "Center for Internet Security Critical Security Controls for Effective Cyber Defense"; or

(vi) The "ISO/IEC 27000-series" information security standards published by the International Organization for Standardization and the International Electrotechnical Commission.

(B) When a revision to a document listed in subparagraph (A) of this section is published, a covered entity whose cybersecurity program reasonably conforms to a prior version of said document, such covered

entity shall reasonably conform to such revision not later than one year after the publication date of such revision.

(2) (A) The covered entity is regulated by the state or the federal government or is otherwise subject to the requirements of any of the laws or regulations identified in subparagraph (A)(i) to (A)(iv), inclusive, of this subdivision, and such covered entity's cybersecurity program reasonably conforms to the current version of:

(i) The security requirements of the Health Insurance Portability and Accountability Act of 1996, P.L. 104-191, as amended from time to time, as set forth in 45 CFR 164, Subpart C, as amended from time to time;

(ii) Title V of the Gramm-Leach-Bliley Act of 1999, P.L. 106-102, as amended from time to time;

(iii) The Federal Information Security Modernization Act of 2014, P.L. 113-283, as amended from time to time;

(iv) The security requirements of the Health Information Technology for Economic and Clinical Health Act, as amended from time to time, as set forth in 45 CFR 162, as amended from time to time.

(B) If any of the laws or regulations identified in subparagraph (A)(i) to (A)(iv), inclusive, of this subdivision are amended, a covered entity whose cybersecurity program reasonably conforms to a prior version of said laws or regulations, such covered entity shall reasonably conform to such amended law or regulation not later than one year after the date of such amendment.

(3) (A) The cybersecurity program reasonably complies with the current version of the "Payment Card Industry Data Security Standard" and the current version of another applicable industry recognized cybersecurity framework described in subparagraph (A) of subdivision (1) of this subsection.

(B) When a revision to the "Payment Card Industry Data Security Standard" is published, a covered entity whose cybersecurity program

reasonably conforms to a prior version of said document, such covered entity shall reasonably conform to such revision not later than one year after the publication date of such revision.

(d) (1) A covered entity's cybersecurity program shall be designed to do the following with respect to personal and restricted information: (A) Protect the security and confidentiality of such information; (B) protect against any anticipated threats or hazards to the security or integrity of such information; and (C) protect against unauthorized access to and acquisition of the information that is likely to result in a material risk of identity theft or other fraud to the individual to whom the information relates.

(2) The scale and scope of a covered entity's cybersecurity program shall be based on the following factors: (A) The size and complexity of the covered entity; (B) the nature and scope of the activities of the covered entity; (C) the sensitivity of the information to be protected; (D) the cost and availability of tools to improve information security and reduce vulnerabilities; and (E) the resources available to the covered entity.

This act shall take effect as follows and shall amend the following sections:		
Section 1	*October 1, 2021*	New section

Statement of Purpose:

To incentivize the adoption of cybersecurity standards for businesses by allowing businesses that adopt certain cybersecurity framework to plead an affirmative defense to any cause of action that alleges that a failure to implement reasonable cybersecurity controls resulted in a data breach concerning personal or restricted information.

[Proposed deletions are enclosed in brackets. Proposed additions are indicated by underline, except that when the entire text of a bill or resolution or a section of a bill or resolution is new, it is not underlined.]