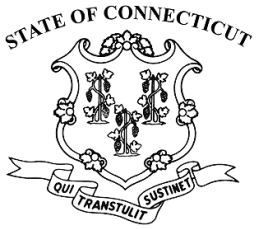

Substitute House Bill No. 6607

Public Act No. 21-119

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 (A) first name or first initial and last name in combination with any one, or more, of the following data: (i) Social Security number; (ii) taxpayer identification number; (iii) identity protection personal identification number issued by the Internal Revenue Service; (iv) driver's license number, state identification card number, passport number, military identification number or other identification number issued by the government that is commonly used to verify identity; (v) credit or debit card number; (vi) financial account number in combination with any required security code, access code or password that would permit access to such financial account; (vii) medical information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; (viii) health insurance policy number or subscriber identification number, or any unique identifier used by a health insurer to identify the individual; or (ix) biometric information consisting of data generated by electronic measurements of an individual's unique physical characteristics used to authenticate or ascertain the individual's identity, such as a fingerprint, voice print, retina or iris image; or (B) user name or electronic mail address, in combination with a password or security question and answer that would permit access to an online account. "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media; and

(5) "Restricted information" means any information about an individual, other than personal information or publicly available 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 reasonably 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, the Superior Court shall not assess punitive damages against a covered entity if such 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 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. The provisions of this subsection shall not apply if such failure to implement reasonable cybersecurity controls was the result of gross negligence or wilful or wanton conduct.

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

(1) (A) The cybersecurity program 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 conforms to a prior version of said document, such covered entity shall conform to such revision not later than six months 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 subparagraphs (A)(i) to (A)(iv), inclusive, of this subdivision, and such covered entity's cybersecurity program 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; or

(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 subparagraphs (A)(i) to (A)(iv), inclusive, of this subdivision are amended, a covered entity whose cybersecurity program conforms to a prior version of said laws or regulations, such covered entity shall conform to such amended law or regulation not later than six months after the date of such amendment; or

(3) (A) The cybersecurity program 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 conforms to a prior version of said document, such covered entity shall conform to such revision not later than six months after the publication date of such revision.

(d) (1) A covered entity's cybersecurity program, as described in subsection (b) of this section, 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 threats or hazards to the security or integrity of such information; and (C) protect against unauthorized access to and acquisition of the information that would 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; and (D) the cost and availability of tools to improve information security and reduce vulnerabilities.

(e) Nothing in this section shall be construed to affect or limit the process by which certification is granted in class actions founded in tort.

(f) Nothing in this section shall be construed to limit the authority of the Attorney General or the Commissioner of Consumer Protection to seek administrative, legal or equitable relief as otherwise allowed by the general statutes or common law.

(g) Nothing in this section shall be construed to affect or limit any requirement of section 4e-70 or 36a-701b of the general statutes.