House of Representatives

File No. 714

General Assembly

January Session, 2021

(Reprint of File No. 598)

Substitute House Bill No. 6607
As Amended by House Amendment
Schedule "A"

Approved by the Legislative Commissioner
May 24, 2021

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.

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

The following Fiscal Impact Statement and Bill Analysis are prepared for the benefit of the members of the General Assembly, solely for purposes of information, summarization and explanation and do not represent the intent of the General Assembly or either chamber thereof for any purpose. In general, fiscal impacts are based upon a variety of informational sources, including the analyst's professional knowledge. Whenever applicable, agency data is consulted as part of the analysis, however final products do not necessarily reflect an assessment from any specific department.

OFA Fiscal Note

State Impact: None

Municipal Impact: None

Explanation

The bill establishes an affirmative defense for covered entities in civil actions and does not result in a fiscal impact to the state or municipalities.

House "A" makes technical and clarifying changes that do not result in a fiscal impact.

The Out Years

State Impact: None

Municipal Impact: None

OLR Bill Analysis

sHB 6607 (as amended by House "A")*

AN ACT INCENTIVIZING THE ADOPTION OF CYBERSECURITY STANDARDS FOR BUSINESSES.

SUMMARY

This bill prohibits the Superior Court from assessing punitive damages against a covered entity (see below) for a data breach of personal or restricted information if the covered entity meets specified cybersecurity requirements.

Specifically, when a civil action alleges that a data breach resulted from a covered entity's failure to implement reasonable cybersecurity controls, the court may not assess punitive damages if the covered entity created, maintained, and complied with a written cybersecurity program containing administrative, technical, and physical safeguards for protecting personal or restricted information. To qualify for this protection, these cybersecurity programs must (1) meet specified design requirements and (2) conform to an industry-recognized cybersecurity framework. However, the protection does not apply if the covered entity's failure to implement reasonable cybersecurity controls resulted from gross negligence or willful or wanton conduct.

Under the bill, "covered entities" are businesses accessing, maintaining, communicating, or processing personal or restricted information in or through systems, networks, or services located inside or outside the state.

The bill's provisions do not:

1. affect or limit the process of granting certification in class actions;

2. affect or limit existing statutory requirements for (a) state contractors who receive confidential information and (b) Connecticut businesses that maintain computerized personal information and suffer security breaches; or

3. limit the authority of the attorney general or the Department of Consumer Protection commissioner to seek administrative, legal, or equitable relief allowed by law.

*House Amendment "A" (1) changes the bill's protection for qualifying covered entities from an affirmative defense to a prohibition on punitive damages and disqualifies covered entities from this protection for certain conduct; (2) changes, to six months, the time period by which a covered entity's cybersecurity program must conform with revisions or amendments to certain cybersecurity frameworks, laws, and regulations; (3) explicitly exempts certain statutes, executive powers, and legal processes from the bill's provisions; (4) makes changes to the definitions of personal and restricted information; and (5) makes minor and technical changes.

EFFECTIVE DATE: October 1, 2021

CYBERSECURITY PROGRAM DESIGN REQUIREMENTS

To qualify for the bill's protection against punitive damages, a covered entity's cybersecurity program must be designed to protect the security and confidentiality of personal and restricted information. The program must specifically protect this information against (1) threats or hazards to its security or integrity and (2) unauthorized access and acquisition that would cause material risk of identity theft or other fraud.

The bill requires the scale and scope of a covered entity's cybersecurity program to be based on the:

1. entity's size and complexity, and the nature and scope of its activities;

2. sensitivity of the information to be protected; and

3. cost and availability of tools to improve information security and reduce vulnerabilities.

INDUSTRY-RECOGNIZED CYBERSECURITY FRAMEWORKS

Under the bill, an industry-recognized cybersecurity framework includes the most current version of:

1. one or any combination of six specifically recognized frameworks (see Table 1),

2. one of four specified federal laws and regulations (for entities regulated by any of these laws or the state or federal government; see Table 2), or

3. the "Payment Card Industry Data Security Standard" in combination with one of the acceptable frameworks mentioned in Table 1 below.

Table 1: Industry-Recognized Cybersecurity Frameworks

Publisher	*Framework*
National Institute of Standards and Technology	"Framework for Improving Critical Infrastructure Cybersecurity" Special Publication (SP) 800-171 SP 800-53 and 800-53a
Federal Risk and Management Program	"FedRAMP Security Assessment Framework"
Center for Internet Security	"Center for Internet Security Critical Security Controls for Effective Cyber Defense"
International Organization for Standardization and the International Electrotechnical Commission	"ISO/IEC 27000-series"

Table 2: Federal Cybersecurity Laws and Regulations

Citation	*Law or Regulation*
P.L. 104-191; 45 C.F.R. 164 (Subpart C)	Security requirements of the Health Insurance Portability and Accountability Act of 1996
P.L. 106-102	Title V of the Gramm-Leach-Bliley Act of 1999
P.L. 113-283	Federal Information Security Modernization Act of 2014
45 C.F.R. 162	Security requirements of the Health Information Technology for Economic and Clinical Health Act

The bill requires a covered entity to conform with revisions or amendments to these frameworks, laws, and regulations within six months after the revised document is published or the laws or regulations are amended, as applicable.

DEFINITIONS

Businesses

Under the bill, a covered entity's business type may include an individual or a sole proprietorship, partnership, firm, corporation, trust, limited liability company or partnership, joint stock company, joint ventures, associations, or other legal entities through which for-profit or non-profit business is conducted.

Data Breach

The bill defines a "data breach" as unauthorized access to and acquisition of computerized data that (1) compromises the security or confidentiality of personal or restricted information owned by or licensed to a covered entity and (2) causes a material risk of identity theft or other fraud to a person or property (or reasonably is believed to have caused or will cause such risk). The definition specifically excludes:

1. employees or agents of a covered entity acquiring personal or restricted information in good faith for the purposes of the entity, so long as the entity does not unlawfully use this information or subject it to further unauthorized disclosure, or

2. the acquisition of this information pursuant to a (a) search warrant, (b) subpoena or other court order, or (c) regulatory state agency's order or duty.

Personal and Restricted Information

Under the bill, "personal information" means an individual's first name or initial and last name in combination with one or more of the following:

1. social security, taxpayer identification, Internal Revenue Service-issued identity protection personal identification, driver's license, state identification card, passport, or military identification numbers, or other commonly used government-issued identification numbers;

2. credit or debit card numbers; financial account numbers in combination with required security codes, access codes, or passwords that would permit access to these accounts;

3. medical information on an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional;

4. health insurance policy or subscriber identification numbers, or unique identifiers health insurers use to identify individuals; or

5. biometric information that can identify an individual using their unique physical characteristics, including a fingerprint, voice print, or retina or iris image.

Personal information also includes user names or e-mail addresses in combination with passwords or security questions and answers that would permit access to online accounts. However, the definition excludes publicly available information lawfully available to the general public from federal, state, or local government records or widely distributed media.

"Restricted information" means any unencrypted, unredacted, or unaltered information about an individual that, alone or in combination with other information (including personal information as described above), (1) can be used to distinguish or trace the individual's identity or is reasonably linked or linkable to an individual and (2) is likely to result in a material risk of identity theft or other fraud to a person or property if breached. The definition excludes personal or publicly available information.

COMMITTEE ACTION

Commerce Committee

Joint Favorable Change of Reference - JUD
Yea 22 Nay 1 (03/22/2021)

Judiciary Committee

Joint Favorable Substitute
Yea 32 Nay 3 (04/09/2021)