PA 21-119—sHB 6607
Commerce Committee
Judiciary Committee

AN ACT INCENTIVIZING THE ADOPTION OF CYBERSECURITY STANDARDS FOR BUSINESSES

SUMMARY: This act prohibits the Superior Court from assessing punitive damages against a covered entity for a data breach of personal or restricted information if the covered entity meets certain cybersecurity requirements. 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 act, "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 act'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 that 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.

EFFECTIVE DATE: October 1, 2021

PROTECTION AGAINST PUNITIVE DAMAGES

Under the act, 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.

CYBERSECURITY PROGRAM DESIGN REQUIREMENTS

To qualify for the act'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 act requires that the scale and scope of a covered entity's cybersecurity program 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 act, an industry-recognized cybersecurity framework includes the most current version of:

1. one or any combination of six specifically recognized frameworks (see table below);
2. one of the following federal laws and regulations (for entities subject to them or regulated by the state or federal government): (a) the security requirements of the Health Insurance Portability and Accountability Act of 1996, (b) Title V of the Gramm-Leach-Bliley Act of 1999, (c) the Federal Information Security Modernization Act of 2014, or (d) the security requirements of the Health Information Technology for Economic and Clinical Health Act; or
3. the "Payment Card Industry Data Security Standard" in combination with one of the acceptable frameworks listed in the table below.

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"

The act 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 act, 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 act 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 act, "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 about 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 his or her 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.