HINSHAW

Connecticut Cybersecurity Bill Prohibiting Punitive Damages for Businesses Advances in State Legislature

Privacy, Cyber & AI Decoded Alert | 2 min read
Jun 16, 2021

On May 24, 2021, the Connecticut House of Representatives passed House Bill 6607, "An Act Incentivizing The Adoption Of Cybersecurity Standards For Businesses," which carves out a data security safe harbor provision for Connecticut businesses. The Bill prohibits the Connecticut Superior Court from assessing punitive damages to covered business entities for data breaches of personal or restricted information under certain circumstances.

The Bill requires covered entities to create, maintain, and comply with a written cybersecurity plan that conforms to industry standards and is risk-based. "Covered Entities" are defined as businesses that access, maintain, communicate, or process personal or restricted information via systems, networks, or services located inside or outside the state.

First, the scale and scope of a covered entity's cybersecurity plan must be based on the entity's size, complexity, and the nature and scope of its activities. The plan must also be based upon the sensitivity of the information to be protected in addition to the cost and availability of tools to improve information security and reduce vulnerabilities.

Second, a qualifying cybersecurity plan must be based on a current version of any of the six listed frameworks in combination with the Payment Card Industry Data Security Standard. For entities regulated by the Health Insurance Portability and Accountability Act of 1996, Title V of the Gramm-Leach-Bliley Act of 1999, the Federal Information Security Modernization Act of 2014, security requirements of the Health Information Technology for Economic and Clinical Health Act, or state or federal government, the cybersecurity framework must incorporate one of the four federal laws and regulations specified in the Bill.

An earlier version of the Bill provided an affirmative defense to a civil action rather than a bar on punitive damages. The Assembly further amended the Bill to disqualify covered entities for certain conduct and implemented a six-month time period by which a covered entity's cybersecurity program must conform with revisions or amendments to certain cybersecurity frameworks, laws, and regulations. In addition to creating

specific exemptions to certain statutes, executive powers, and legal processes, the amendment altered the definitions of personal and restricted information.

The Bill would not:

- Limit the authority of the attorney general or the Department of Consumer Protection commissioner to seek administrative, legal, or equitable relief allowed by law;
- Affect or limit the process of granting class certifications in class actions; or
- Affect or limit existing statutory structures for (1) state contractors who receive confidential information and (2) Connecticut businesses that maintain computerized personal information and suffer security breaches.

Passed by the Connecticut Senate on June 7, the Bill is now on a consent calendar as a formality before heading to the Governor. The Bill would be effective on October 1, 2021.

Related Capabilities

Data Privacy, AI & Cybersecurity