Published on *The National Law Review* https://natlawreview.com

Connecticut Enacts Safe Harbor from Punitive Damages in Data Breach Cases

Article By:

Joseph J. Lazzarotti

Jason C. Gavejian

Effective October 1, 2021, Connecticut becomes the third state with a data breach litigation "safe harbor" law (Public Act No. 21-119), joining Utah and Ohio. In short, the Connecticut law prohibits courts in the state from assessing punitive damages in data breach litigation against a covered defendant that created, maintained, and complied with a cybersecurity program that meets certain requirements. Cyberattacks are on the rise – think Colonial Pipeline, Kaseya, JBS, and others – with ransomware attacks up 158 percent from 2019-2020 in North America.

The hope is this law will provide covered entities of all sizes an incentive to implement stronger controls over their information systems. According to Homeland Security Secretary Alejandro Mayorkas:

> ***As a matter of fact, small businesses comprise approximately one-half to three-quarters of the victims of ransomware***

So, what can "covered entities" in Connecticut do to at least try to protect themselves from punitive damages if sued following a data breach?

First, it is important to note that the law applies to "covered entities" – defined to include 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."

The definition of "personal information" tracks the definition of the same term in Connecticut's recently updated data breach notification law. But, the law adds the term "restricted information" to the mix, defined to include:

> *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.*

PA 21-119 prohibits superior courts from assessing punitive damages against a covered entity defendant in any tort action brought under Connecticut law or in Connecticut courts alleging a failure to implement reasonable cybersecurity controls that resulted in a data breach involving personal information *or restricted information*, **provided that**:

> [the 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 conforms to an industry recognized cybersecurity framework.

Examples of the frameworks listed in the statute include: NIST SP 800-171, NIST SP 800-53, and the Center for Internet Security's "Center for Internet Security Critical Security Controls for Effective Cyber Defense." Covered entities regulated under federal or state laws, such as the Security Rule under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), can rely on compliance with the current version of those regulatory frameworks. Should these frameworks change, covered entities have six months to confirm to the changes.

Additionally, the cybersecurity program must be designed to:

- protect the security and confidentiality of personal and restricted information;
- protect against any threats or hazards to the security or integrity of such information; and
- protect against unauthorized access to and acquisition of such information that would result in a material risk of identity theft or other fraud to the individual to whom the information relates.

Importantly, covered entities should consider how the framework they use covers the personal and restricted information they maintain. For example, a HIPAA covered entity or business associate relying solely on the HIPAA security rule could mean that its cybersecurity program reaches only "protected health information" as defined by HIPAA, but not personal and restricted information as defined in PA 21-119.

The Connecticut law, however, permits the program to be shaped by several factors including (i) the size and complexity of the covered entity; (ii) the nature and scope of the activities of the covered entity; (iii) the sensitivity of the information to be protected; and (iv) the cost and availability of tools to improve information security and reduce vulnerabilities.

This law, similar to the measures in Utah and Ohio, incentivize heightened protection of personal data, while providing a safe harbor from certain claims for organizations facing data breach litigation. Creating, maintaining, and complying with a robust data protection program is a critical risk management and legal compliance step, and one that might provide protection from litigation following a data breach.

National Law Review, Volume XI, Number 204