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

Connecticut Enacts Legislation to Incentivize Adoption of Cybersecurity Safeguards and Expand Breach Reporting Obligations

Article By:

Conor O. Duffy

Michael G. Lisitano

On June 16, and then on July 6, 2021, Connecticut Governor Ned Lamont signed into law a pair of bills that together address privacy and cybersecurity in the state. As cybersecurity risks continue to pose a significant threat to businesses and the integrity of private information, Connecticut joins other states in revisiting its data breach reporting laws to strengthen reporting requirements, and offer protection to businesses that have been the subject of a breach despite implementing cybersecurity safeguards from certain damages in resulting litigation.

Public Act 21-59 "An Act Concerning Data Privacy Breaches" (PA 21-59) modifies Connecticut law addressing data privacy breaches to expand the types of information that are protected in the event of a breach, to shorten the timeframe for reporting a breach, to clarify applicability of the law to anyone who owns, licenses, or maintains computerized data that includes "personal information," and to create an exception for entities that report breaches in accordance with HIPAA. Public Act 21-119 "An Act Incentivizing the Adoption of Cybersecurity Standards for Businesses" (PA 21-119) correspondingly establishes statutory protection from punitive damages in a tort action alleging that inadequate cybersecurity controls resulted in a data breach against an entity covered by the law if the entity maintained a written cybersecurity program conforming to industry standards (as set forth in PA 21-119).

Both laws take effect October 1, 2021.

Public Act 21-59

Personal Information

Under Connecticut law, a "breach of security" is reportable as a data breach if there is unauthorized access to, or acquisition of, electronic data containing unsecured "personal information." Previously, the term "personal information" referred to a person's first name or first initial and last name in combination with one or more of the following: a Social Security number; driver's license number; state identification card number; credit or debit card number; or financial account number in

combination with any required security code, access code, or password that would permit access to such financial account.

PA 21-59 expands the definition of personal information to also include the following types of data in combination with a person's first name or first initial and last name: (i) passport number; (ii) military identification number; (iii) other government identification numbers commonly used to verify identity; (iv) taxpayer identification number; (v) identity protection personal identification number issued by the Internal Revenue Service; (vi) medical information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; (vii) health insurance policy number or subscriber identification number, or any unique identifier used by a health insurer to identify the individual; or (viii) 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. PA 21-59 also newly defines "personal information" to include a user name or electronic mail address, in combination with a password or security question and answer that would permit access to an online account.

Breach Notification

PA 21-59 clarifies that the state's data breach notification requirements apply to anyone who owns, licenses, or maintains computerized data that includes "personal information," rather than just those who do so in the ordinary course of doing business in Connecticut, as under current law, which potentially broadens applicability of the notification requirements. Additionally, PA 21-59 shortens the deadline for providing notice of a breach to affected Connecticut residents to 60 days from breach discovery – from the prior 90 day requirement – and eliminates a provision that made such reporting subject to completion of an investigation to determine the nature and scope of the incident and individuals affected. Instead, if the reporting entity identifies additional residents affected by an incident after the reporting deadline passes, the entity is obligated to act in good faith to notify those individuals "as expediently as possible."

PA 21-59 also extends the circumstances in which an entity is obligated to offer identity theft protection to Connecticut residents affected by a breach. Currently, an entity is required to offer 24 months of identity theft prevention (and if applicable, identity theft mitigation) services at no cost to residents affected by a breach involving social security numbers. PA 21-59 expands that requirement to also apply to residents affected by a breach involving taxpayer identification numbers.

HIPAA Compliance

PA 21-59 also adds a new provision under which any entity that is covered by and acts in compliance with HIPAA (Health Insurance Portability and Accountability Act) and HITECH (Health Information Technology for Economic and Clinical Health Act) privacy and security regulations will be deemed in compliance with the state data breach reporting requirements, as long as the entity provides notice to the Connecticut Attorney General not later than the time when notice is provided to residents (if notice to the Attorney General is required).

Notice Requirements

Along with expanding the definition of personal information that may be subject to breach reporting to include a user name or electronic mail address, in combination with a password or security question and answer that would permit access to an online account, PA 21-59 provides that if there is a

breach of login credentials, notice can be provided in electronic or other form to direct the recipient to promptly change login credentials or take other steps to protect all affected online accounts. Moreover, an entity that furnishes an email account cannot provide notice to the same email account that was breached unless the entity can reasonably verify that the affected resident received such notification; otherwise an alternative form of notice must be used or the resident must receive a clear and conspicuous notice while online from a location known to be associated with the resident.

Protection of Breach Reporting from Freedom of Information Requests

PA 21-59 newly establishes that "documents, materials and information" provided in response to an investigative demand for an investigation into a potential violation of Connecticut's unfair trade practices act arising from a data breach are exempt from public disclosure under Connecticut's freedom of information law, but the Attorney General is permitted to make such documents, material, and information available to third parties for investigative purposes.

PA 21-119

This law establishes a liability shield against punitive damages for businesses in certain tort actions arising from data breaches that appears intended to incentivize implementation of cybersecurity safeguards to protect data containing personal information.

Under PA 21-119 any "business" (as defined below) that accesses, maintains, communicates, or processes personal information (as defined under the state's data breach law referenced above, as amended by PA 21-59) may not be subject to punitive damages in a tort action alleging failure to implement reasonable cybersecurity controls resulting in a data breach involving personal information or "restricted information" (as defined below) if the business created, maintained, and complied with a written cybersecurity program containing safeguards conforming with an industry-recognized framework, unless the failure to implement cybersecurity controls was due to gross negligence or willful misconduct.

The law provides that a covered business's cybersecurity framework may conform with industry standards if: (i) it complies with certain recognized information security standards, such as the ""Framework for Improving Critical Infrastructure Cybersecurity" published by the National Institute of Standards and Technology (NIST), or NIST's special publication 800-171, among other standards; (ii) the business is regulated by HIPAA, Gramm-Leach-Bliley, or certain other federal or state laws imposing security frameworks, and the business complies with the requirements set forth in such laws or regulations; or (iii) the business complies with the Payment Card Industry Data Security Standard (PCI-DSS) and one of the NIST or similar information security standards identified in the law. The business's cybersecurity program must be designed to protect the security and confidentiality of personal and restricted information, and protect against threats and unauthorized access to such information, and should be scaled based on the size of the business, and scope and sensitivity of data held.

For purposes of this law, a "business" is defined as "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" and a new term – "restricted information" – is defined to refer to "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." Finally, the phrase "data breach" is a defined term that refers to "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 business subject to the law 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." Notably, the state's data breach reporting law modified by PA 21-59 actually uses a different defined term – "breach of security" – to refer to a data breach that may implicate the reporting requirement in that law.

This post was co-authored by Erin Howard, legal intern at Robinson+Cole. Erin is not yet admitted to practice law.

National Law Review, Volume XI, Number 194