Articles + Publications | July 19, 2021

Connecticut Passes Stronger Data Breach Notification and Cybersecurity Liability Statutes

WRITTEN BY

Angelo A. Stio, III | Ronald Raether, Jr. | Jason J. Moreira

Introduction

The Connecticut legislature recently enacted a pair of new data breach and cybersecurity statutes — Public Act 21-59 and Public Act 21-119 — on June 16 and July 6, respectively. Both laws will take effect on October 1, and will expand the notice obligations for businesses subject to a data security incident and provide business incentives for enhanced cybersecurity standards to protect personal information.

Public Act 21-59: An Act Concerning Data Privacy Breaches

Public Act 21-59 modifies Connecticut's existing data breach and cybersecurity law in three key areas. First, it expands the substantive definition of what constitutes "personal information" subject to legal protection. Second, it shortens the deadline for providing notice of data breaches (subject to certain qualifications and exceptions as further discussed below) and creates unique notification requirements for incidents involving a breach of login credentials. Third, it protects from public disclosure certain information provided in response to a Connecticut unfair trade practices investigation arising from a data breach.

Expanded Definition of "Personal Information"

Connecticut law previously defined "personal information" as a person's first name or first initial and last name in combination with one or more of the following: (1) Social Security number; (2) driver's license number; (3) state identification card number; (4) credit or debit card number; or (5) financial account number in combination with any password or security code that would permit access to such account.

Public Act 21-59 expands this definition significantly to include the following data elements:

- Taxpayer identification number;
- IRS identity protection personal identification number;
- Passport number, military identification number, or other government-issued identification number used to verify identity (*e.g.*, Social Security number);
- Information regarding medical history, mental or physical condition, or medical treatment or diagnosis by a

health care professional;

- Health insurance policy number, subscriber identification number, or other number used by a medical insurer to identify the individual;

- Biometric information consisting of data generated by measurements of unique physical characteristics, such as a fingerprint, voice print, retina, or iris image, used to authenticate identity;

- User name or electronic mail address in combination with a password or security code that would permit access to an online account.

Strengthened Data Breach Notice Requirements

Under Public Act 21-59, the deadline for providing notice of a data breach to affected individuals and the Connecticut attorney general is shortened from 90 days to "without unreasonable delay, but not later than 60 days." In the event that the notifying entity discovers additional individuals after the reporting deadline, it is still obligated to act in good faith to notify those individuals "as expediently as possible." Moreover, if the entity determines it cannot confirm the identities of and provide notice to all affected individuals within the new 60-day deadline, it must provide preliminary substitute notice to all potentially affected individuals and follow up with direct notice as soon as possible. Substitute notice consists of (1) email notice (where the individual's email address is known), (2) "conspicuous posting" of the notice on the entity's website (if any), and (3) "notification to major state-wide media, including newspapers, radio and television."

Further, Public Act 21-59 contains special rules applicable to incidents involving a breach of login credentials. Notice of a breach of login credentials can be provided via email (or other electronic means) to direct the recipient to change their login credentials or take other steps to secure their account. However, if the affected individual's receipt of the email notification cannot be verified, then an alternative form of notice must be used, or the individual must receive "clear and conspicuous notice" while the individual is "connected to the online account" that the individual "customarily accesses … ." Although not expressly required by the statute, businesses also can consider forcing affected customers to change their passwords or other login information.

Notably, Public Act 21-59 provides that data breach notification requirements apply to *anyone* who owns, licenses, or maintains computerized data that includes "personal information," not just those who do so in the ordinary course of business. This broadens the applicability of the statute's prior notification requirements.

Exemption for HIPAA/HITECH Compliant Companies

With two important exceptions, any entity subject to (and in compliance with) HIPAA and/or HITECH privacy and security standards is deemed to be in compliance with the notice obligations set forth in Public Act 21-59. The exceptions are that (1) an entity required to notify Connecticut residents of a breach under HIPAA/HITECH must also notify the attorney general when those residents are notified; and (2) if the entity would have been required to provide identity protection or mitigation services under Connecticut law (*e.g.,* due to breach of a Social Security number), that requirement remains in effect. This provision attempts to address any confusion from conflicting

state law requirements and requirements under HIPAA/HITECH.

Protection of Data Breach Reporting from Freedom of Information Requests

Public Act 21-59 also provides confidentiality protections to businesses responding to an investigation into alleged violations of Connecticut's Unfair Trade Practices Act arising from a data breach. Public Act 21-59 recognizes that "documents, materials and information" provided in response to an investigation of a potential violation of Connecticut's Unfair Trade Practices Act arising from a data breach are exempt disclosure requirements under Connecticut's freedom of information law. However, the attorney general is permitted to make such documents, material, and information available to third parties for investigative purposes.

Public Act 21-119: An Act Incentivizing the Adoption of Cybersecurity Standards for Businesses

Public Act 21-119 seeks to incentivize greater adoption of cybersecurity standards by businesses. Among other things, Public Act 21-119 allows businesses that comply with certain industry-recognized cybersecurity practices to avoid punitive damages in any tort claim that alleges a failure to implement "reasonable cybersecurity controls resulted in a data breach concerning personal or restricted information." The immunity from punitive damages afforded by Public Act 21-119, however, is subject to a few qualifications.

First, protection from punitive damages is provided only for tort claims "brought under the laws of [the state of Connecticut] or in the courts [of the state of Connecticut]." Second, the entity must have complied with a formal, *written* cybersecurity program that contains "administrative, technical and physical safeguards for the protection of personal or restricted information … ." Finally, the program must conform to one or more of the industry-recognized cybersecurity frameworks referenced in the statute. These frameworks include standards adopted by the National Institute of Standards and Technology (NIST), Center for Internet Security (CIS), and the Payment Card Industry (PCI) Security Standards Council — and, for applicable businesses, the security regulations established by HIPAA, HITECH, FISMA, or GLBA. Entities will be deemed in compliance with subsequently amended or revised versions of the industry-recognized frameworks listed in the statute as long as they conform to such amended or revised version within six months of its publication.

Conclusion

Connecticut's updated data breach notification and cybersecurity statutes are consistent with a growing trend of states seeking to protect personal information by expanding the definition of personal identifying information and by providing businesses with new tools to stay in compliance with the law and manage risk associated with information security and privacy.

The tightened notice requirements and expanded definition of "personal information" set forth in Public Act 21-59 will require affected businesses to enhance their efforts to quickly and effectively respond to data breach and other cybersecurity threats. To do so, businesses should strongly consider reviewing and updating their incident response plans, enhancing their training and roundtable exercises, and having in place a list of forensic consultants, outside counsel, and media advisors to meet the tightened deadlines and manage their response.

The immunity from punitive damages afforded by Public Act 21-119 should serve to galvanize potentially affected

businesses, as well as their general counsels, CTOs, risk managers, and other privacy professionals to reevaluate and strengthen their information security policies and procedures and adopt industry-recognized standards.

Finally, the exemption from compliance with Public Act 21-59 for entities already compliant with HIPAA and/or HITECH's privacy and security obligations should enhance efficiency and avoid confusion between state and federal standards, at least with respect to covered entities in the health care industry.

Connecticut is not the last state that will enhance its privacy and security laws. Alabama, Arizona, Illinois, Kentucky, Maryland, Massachusetts, Minnesota, New York, Pennsylvania, and Oklahoma all have legislation pending. Troutman Pepper's Cybersecurity, Information Governance, and Privacy Practice Group continues to track pending data breach and cybersecurity legislation and will publish updates and client alerts when new laws are adopted.

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber