Akin®

Connecticut Expands Breach Reporting and Creates Cybersecurity Safe Harbor

Oct 5, 2021

Reading Time : **7 min**

By: Natasha G. Kohne

Expanding Breach Notification Requirements

The first Act (PA 21-59), signed on June 16, 2021, modifies Connecticut's existing breach notification by (1) expanding the types of information protected, (2) shortening the notification timeline from 90 days to "without unreasonable delay, but not later than 60 days," from the day of breach discovery and (3) expanding coverage beyond those businesses that use personal information in "the ordinary course of business in Connecticut."[1]

What Counts as Protected Personal Information?

Connecticut 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: social security number, driver's license number, state ID card, credit or debit card number, or financial account number in combination with any required security code or password. PA 21-59 expands this definition to include:

i. Taxpayer ID number

ii. Identity protection personal ID number issued by the IRS

iii. Passport number, military number, or other government issued ID number

iv. Biometric data

v. Certain types of medical information

vi. Health insurance ID numbers

vii. A username or email address in combination with a password or security questions and answers.[2]

These alterations are in line with amendments made by other state data breach notification laws to include tax identification numbers, biometrics, health-related information and a username and password.

When Does a Business Need to Report?

Businesses now have 60 days from the date of breach discovery to inform affected Connecticut residents of a breach.[3] Under the original law, countdown to the deadline began after the breach had been discovered and upon completion of an investigation into the nature and scope of the incident. PA 21-59 omits the investigation requirement, suggesting that the 60-day timeline begins only after the business discovers the breach and not after completing the investigation. This contrasts with states like Texas and Washington, which allow for deadline extensions to determine scope. The timing of the notice to the Attorney General is unchanged, to be provided no later than notice to the affected individuals.

PA 21-59 recognizes that some investigations may take longer than 60 days and provides for a "good faith" notice requirement on individuals noticed after that date. Specifically, if additional Connecticut residents "whose information was breached or reasonably believed to have been breached" after the 60-day deadline, the business must "proceed in good faith" and notify the additional Connecticut residents "as expediently as possible."[4] However, this good faith notification is not required if investigation reveals that no harm is likely to result for individuals whose personal information was acquired or accessed.

When the bill was introduced on January 22, 2021, it included a novel provision that would have required businesses to provide "preliminary substitute notice" to Connecticut residents that were not notified within the 60-day window after the breach. Even after providing preliminary notice (which could take the form of an email, a web posting or notice in state media), the business that suffered a breach would also have to provide direct notice to affected residents. The final version of the bill omits this provision, removing what would have been a significant obligation.

Special notice requirements apply in the event that login credentials are breached. A business can provide notice to customers by email to direct its customers to change their login credentials or otherwise secure their accounts. But businesses that host email accounts cannot provide electronic notice to email accounts that were breached, unless the business can verify that the affected customer received the notice. If businesses cannot verify that a customer received the notice, then the business must either use alternative notice or "clear

and conspicuous notice" in an online location from which the customer is known to access the account.

What Businesses Are Covered?

Previously, Connecticut's data breach notification law only covered entities using personal information in the "ordinary course of business in Connecticut." PA 21-59 strikes this qualification, now covering anyone who owns, licenses or maintains computerized data that contains personal information.[5] This potentially increases the number of entities subject to notification requirements—businesses no longer have to use personal information "in the ordinary course of business in Connecticut" to be held liable.

Other Changes

PA 21-59 also includes a number of new additions, such as an exemption for entities subject to the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH). Another new measure extends the 24 free months of identity theft protection companies must provide to affected residents to include victims of a breach of taxpayer ID numbers. Finally, PA 21-59 grants an exemption for data related to an investigation under Connecticut's Unfair Trade Practices Act arising from a data breach (with the Attorney General still able to make such data available to third parties for an investigation).

Safe Harbor for Security Measures

The second Act (PA 21-119), signed on July 6, 2021, offers protection for companies during a data breach provided that they follow certain cybersecurity protocols.[6]

New Term: Restricted Information

PA 21-119 creates a new category of information—"restricted information"—that companies must account for along with personal information. Restricted information is information that is not publicly available or personal 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.[7]

Companies will now have to treat restricted information just as they would personal information during a breach and adopt the same procedures and safeguards.

Incentivizing a Cybersecurity Framework

Critically, the new law incentivizes written cybersecurity programs containing safeguards that conform to an industry-wide framework by barring punitive damages (except for in those cases where there is gross negligence or willful misconduct) in tort actions that allege failure to implement reasonable cybersecurity controls resulting in a data breach.[8]

Seven standards qualify as an industry-recognized framework for the safe harbor:

- National Institute of Standards and Technology (NIST) standards, such as special publication 800-171
- Federal Risk and Authorization Management Program (FedRAMP)
- The Center for Internet Security's (CIS) "Center for Internet Security Critical Security Controls for Effective Cyber Defense"
- ISO 27001 or 27002 certification
- HIPAA
- Gramm-Leach-Bliley
- Payment Card Industry Data Security Standard (PCI-DSS) (though PCI-DSS compliance must also include compliance with another framework such as NIST, FedRAMP or ISO 27001 or 27002 standards).

This law specifies that cybersecurity programs must be tailored to the size of the company and the nature of its operations. The sensitivity of the information and the cost of the security should also be taken into account.

Finally, PA 21-119 does not shield companies from all damages, and companies could still face damages from other claims. While there is no private right of action, the law allows victims of a breach to bring general tort claims without punitive damages.

Key Takeaways

States have taken up the reins of data privacy and cybersecurity law in the United States, and Connecticut's contribution should come as no surprise. Revision of data breach reporting requirements is increasing as cyber attacks expand in scope and impact, with Texas and Nevada both passing amendments to their reporting requirements in June of this year.[9]

Companies should be prepared for the continuing trend of expanding data breach definitions and shortened breach notification timelines.

The cybersecurity safe harbor provision of PA 21-119 is the most important takeaway for businesses. It encourages more companies to take proactive cybersecurity measures, providing a roadmap to limit liability in the lawsuits that follow with increasing frequency following data breaches.

Connecticut now joins Ohio and Utah as the third state to adopt a safe harbor that seeks to incentivize companies to enhance cybersecurity measures.[10] All of these state laws encourage the adoption of frameworks such as the NIST standards and the CIS "Center for Internet Security Critical Security Controls for Effective Cyber Defense."

The Connecticut Acts are a step forward for the safe harbor incentive system as more states recognize the importance of maintaining more robust data privacy and information security programs. Companies should reevaluate their written information security benchmarked against industry-recognized security frameworks as more states will likely adopt a similar strategy.

Please contact a member of Akin Gump's cybersecurity, privacy and data protection team if you have any questions about how the new Connecticut Acts may impact your company or your company's data privacy and cybersecurity programs.

---

[1] Public Act No. 21-59, H.B. 5310, An Act Concerning Data Privacy Breaches (June 16, 2021) available at https://www.cga.ct.gov/2021/ACT/PA/PDF/2021PA-00059-R00HB-05310-PA.PDF.

[2] *Id*. at 2.

[3] *Id*. at 2.

[4] *Id*.

[5] *Id*. at 3.

[6] Public Act No. 21-19, H.B. 6607, An Act Incentivizing the Adoption of Cybersecurity Standards for Business (July 6, 2021) available at

https://www.cga.ct.gov/2021/ACT/PA/PDF/2021PA-00119-R00HB-06607-PA.PDF.

[7] *Id*. at 3

[8] *Id*.

[9] Texas H.B. No. 3746, 87th Legislature (June 14, 2021) (Bill stating that companies must inform Texas Attorney General of number of affected residents that have received breach notification, taking effect September 1, 2021) available at https://capitol.texas.gov/BillLookup/History.aspx?LegSess=87R&Bill=HB3746; Nevada A.B. 61, 81st Legislature (June 2, 2021) (Bill stating Nevada Attorney General will be able to impost criminal and civil penalties for breach requirement violations under state deceptive trade practices law, taking effect October 1, 2021) available at https://www.leg.state.nv.us/App/NELIS/REL/81st2021/Bill/7314/Overview.

[10] Ohio SB 220, 132nd General Assembly (September 20, 2018) available at https://www.legislature.ohio.gov/legislation/legislation-documents?id=GA132-SB-220; Utah H.B. No. 80, 2021 General Session (March 11, 2021) available at https://le.utah.gov/~2021/bills/static/HB0080.html.

Categories

State Privacy Policy | Data Breach | Cybersecurity & Information Security

other associated entities under which the Akin Gump network operates worldwide, please see our Legal Notices page.