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

New Connecticut Breach Notification Requirements and Cybersecurity Safe Harbor Effective October 2021

Article By:

Hunton Andrews Kurth's Privacy and Cybersecurity

Connecticut recently passed two cybersecurity laws that will become effective on October 1, 2021. The newly passed laws modify Connecticut's existing breach notification requirements and establish a safe harbor for businesses that create and maintain a written cybersecurity program that complies with applicable state or federal law or industry-recognized security frameworks.

New Breach Notification Requirements (HB 5310)

On June 16, 2021, Connecticut Governor Ned Lamont signed HB 5310, An Act Concerning Data Privacy Breaches. HB 5310 amends Connecticut's existing breach notification requirements by:

- expanding the types of personal information that may trigger notification requirements if breached, to include: (i) taxpayer ID number; (ii) identity protection personal ID number issued by the IRS; (iii) passport number, military ID number or other government-issued ID number; (iv) biometric data; (v) certain types of medical information; (vi) health insurance ID numbers; and (vii) a user name or email address in combination with a password or security question and answer;

- shortening the notification timeline of a breach to affected Connecticut residents and the Attorney General from 90 days to no later than 60 days post-discovery of the breach; and

- requiring "preliminary substitute notice" to individuals if a business cannot provide direct notification within the 60-day notification timeframe. Businesses must also follow up with direct notice as soon as possible following such preliminary substitute notice.

In passing the law, Connecticut joins a number of other states in expanding the definition of "personal information" in its data breach notification statute.

Cybersecurity Safe Harbor (HB 6607)

On July 6, 2021, Governor Ned Lamont signed HB 6607, An Act Incentivizing the Adoption of Cybersecurity Standards for Businesses.

HB 6607 prevents the Connecticut Superior Court from assessing punitive damages against an organization that 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 (e.g., the Payment Card Industry Data Security Standard, the National Institute of Standards and Technology's Cybersecurity Framework, the ISO/IEC 27000-series information security standards).

The safe harbor also applies in cases where the cybersecurity program conforms to applicable state or federal security laws and regulations (e.g., the security requirements of the Health Insurance Portability and Accountability Act and the Gramm-Leach Bliley Act).

In passing the law, Connecticut joins Ohio and Utah as the third state to enact a cybersecurity safe harbor statute.

Copyright © 2025, Hunton Andrews Kurth LLP. All Rights Reserved.

National Law Review, Volume XI, Number 214

Source URL:https://natlawreview.com/article/new-connecticut-breach-notification-requirements-and-cybersecurity-safe-harbor