NOW + NEXT

CYBERSECURITY & PRIVACY ALERT | NIXON PEABODY LLP

JULY 8, 2021

Connecticut to limit liability for data security breaches—if businesses implement cybersecurity controls

By Leslie Hartford and Erin Huntington

The recently passed Connecticut Cybersecurity Standards Act creates a "safe harbor" from punitive damages for companies that implement a written cybersecurity policy in compliance with recognized standards. The law, which goes into effect October 1, applies to any business that "accesses, maintains, communicates or processes personal information" and also expands the definition of personal information to include biometric data. If applicable, the new legislation would shield businesses from punitive damages in actions brought under Connecticut law concerning a breach that compromises the personally identifiable information of Connecticut residents.

The Connecticut Cybersecurity Standards Act joins comparable legislation from Ohio and Utah in encouraging comprehensive and standardized cybersecurity policies in exchange for safe harbor. The law lists six frameworks employed in the public and private sectors: "(i) The "Framework for Improving Critical Infrastructure Substitute House Bill Cybersecurity" published by the National Institute of Standards and Technology; (ii) The National Institute of Standards and Technology's special publication 800-171; (iii) The National Institute of Standards and Technology's special publications 800-53 and 800-53a; (iv) The Federal Risk and Management Program's "FedRAMP Security Assessment Framework"; (v) The Center for Internet Security's "Center for Internet Security Critical Security Controls for Effective Cyber Defense"; or (vi) The "ISO/IEC 27000-series" information security standards published by the International Organization for Standardization and the International Electrotechnical Commission."

A company may also qualify by conforming to the data security requirements of the Health Insurance Portability and Accountability Act (HIPPA), the Gramm-Leach-Biley Act, the Federal Information Security Modernization Act, or the Health Information Technology for Economic and Clinical Health Act (HITECH). As is the norm in the data privacy realm, conformity obligations are continually evolving, and a company has six months to update its policies to remain in compliance following any amendments to these laws or risk losing its safe harbor status.

The Cybersecurity Standards Act also notes cybersecurity policies are proportional to the nature of each business. It states that the "scale and scope" of a company's cybersecurity program may

consider the size and complexity of the business, the nature of the business's activities, the sensitivity of the protected information, and the cost and availability of the tools necessary to improve cybersecurity. However, the bar on punitive damages does not apply if the company fails to implement reasonable cybersecurity protocols as a "result of gross negligence or willful or wanton conduct." Businesses should consult with their Nixon Peabody attorney, or other knowledgeable advisor, to ensure that their policies and protocols are sufficient to qualify under the Act.

For more information on the content of this alert, please contact your Nixon Peabody attorney or:

- Leslie Hartford, 617-345-1369, lhartford@nixonpeabody.com
- Erin Huntington, 518-427-2748, ehuntington@nixonpeabody.com