PA 21-59—sHB 5310
General Law Committee
Government Administration and Elections Committee

AN ACT CONCERNING DATA PRIVACY BREACHES

SUMMARY: This act expands the data breach notification law to apply to additional types of information and cover additional individuals who keep this information. It extends the data breach notification requirements to include anyone who owns, licenses, or maintains computerized data that includes personal information ("data managers"), rather than just those who do so in the ordinary course of doing business in the state, as under prior law.

The data breach notification law generally requires data managers to disclose a security breach without unreasonable delay to state residents whose personal information has been, or is reasonably believed to have been, accessed by an unauthorized person. The act generally shortens, from 90 to 60 days after the security breach was discovered, the amount of time data managers have to inform consumers and the attorney general.

The act narrows the circumstances under which those who own or license computerized data with breached information must offer residents appropriate identity theft prevention or mitigation services.

As under existing law, the act deems violations of the data breach notification law a Connecticut Unfair Trade Practices Act (CUTPA) violation (see BACKGROUND). Additionally, under the act, all documents, materials, and information provided in response to a CUTPA investigative demand connected to the security breach investigation are exempt from public disclosure under the Freedom of Information Act. But the attorney general may make it available to third parties for investigative purposes.
EFFECTIVE DATE: October 1, 2021

BROADENING PERSONAL INFORMATION

The act expands the types of information that, when combined with a person's first name or first initial and last name, are considered "personal information" and therefore subject to data breach notification requirements. By law, these types of information are (1) Social Security number, (2) driver's license or state identification card number, (3) credit or debit card number, or (4) financial account number, in combination with other information that would permit access to the account. The act additionally includes the following types of information:

1. taxpayer identification number;
2. identity protection personal identification number issued by the Internal Revenue Service;
3. other identification numbers the government issues that are commonly

used to verify identity, such as passport and military identification numbers;
4. information about the person's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional;
5. health insurance policy number or subscriber identification number, or any unique identifier a health insurer uses to identify the person; or
6. biometric data generated by electronic measurements of the person's unique physical characteristics used to authenticate or ascertain identity (e.g., fingerprint, voice print, or retina or iris image).

Under the act, "personal information" also includes a person's username or e-mail address, combined with a password or security question and answer that would allow access to an online account (i.e., breach of login credentials).

SHORTENED NOTIFICATION TIMEFRAME

Under prior law, with some exceptions, data managers must have notified consumers and the attorney general of any data breach within 90 days of discovering it and completed an investigation to determine the incident's nature and scope, identify affected individuals, or restore the data system's integrity. The act eliminates the investigation requirement and shortens the timeframe from 90 to 60 days after the security breach is discovered. The act requires data managers to proceed in good faith to notify additional residents affected by the data breach as quickly as possible if they are identified after the 60-day deadline.

Under prior law, the notification was not required if, after an appropriate investigation and consultation with relevant federal, state, and local law enforcement, the data manager reasonably determined the breach would not likely result in harm to the individuals whose personal information had been acquired and accessed. The act eliminates the consultation requirement and requires data managers to send notice if the breach will harm individuals whose information has been acquired or just accessed.

IDENTITY THEFT SERVICES

Under prior law, those who owned or licensed computerized data that included personal information were required to offer residents appropriate identity theft prevention or mitigation services when their personal information or nonpublic information was breached or believed to have been breached. By law, these services must be provided for free and last for at least 24 months. The act eliminates this requirement for breaches of nonpublic information and narrows the types of personal information breaches subject to the requirement to only breaches of Social Security numbers and taxpayer identification numbers.

By law, "nonpublic information" is data and information that is not publicly available, not related to a consumer's age or gender, and that (1) would materially affect a licensee's business, operation, or security if disclosed or used without authorization; (2) is created by or derived from a consumer or health care provider and concerns behavioral, mental, or physical health, or health care services or

payments; or (3) concerns a consumer's name, number, or other identifiable information that can identify a consumer when used in combination with an access or security code to a consumer's financial account; account, credit, or debit card number; biometric records; driver's license or nondriver identification number; or Social Security number (CGS § 38a-38(b)(9)).

NOTICE REQUIREMENTS

E-mail Account Breach

By law, notice to a resident may be provided through written, telephonic, or electronic notice. Substitute notice may be given if (1) the first three methods would cost more than $250,000, (2) the affected class is over 500,000 people, or (3) there is insufficient contact information. One type of substitute notice is by e-mail.

The act prohibits data managers that furnish e-mail accounts from complying with the data breach notification law by e-mailing the breached e-mail account if they cannot reasonably verify the affected resident's receipt of the notification. In such an event, data managers must provide notice by another method (e.g., written or telephone) or by clear and conspicuous notice delivered to the resident online when the resident is connected to the account from an Internet Protocol address or an online location the data manager knows the resident customarily uses to access the account.

Login Credentials

Under the act, for instances of data breaches involving login credentials (i.e., username and e-mail), data managers may provide notice in electronic or other form. The provided notice directs the resident whose personal information was breached, or is reasonably believed to have been breached, to promptly change any password or security question and answer or take other appropriate steps to protect the affected online account and other online accounts with the same information or questions.

FEDERAL HEALTH DATA PRIVACY COMPLIANCE

Under the act, data managers that are subject to and in compliance with the privacy and security standards of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH, see BACKGROUND) are deemed to be in compliance with the state data breach notification law under certain conditions. To be in compliance, data managers must:

1. notify the attorney general within the same timeframe under the state data breach notification law if they are required to notify Connecticut residents under HITECH and
2. provide appropriate identity theft prevention and mitigation services for up

to 24 months, as applicable.

BACKGROUND

Connecticut Unfair Trade Practices Act (CUTPA)

The law prohibits businesses from engaging in unfair and deceptive acts or practices. CUTPA allows the Department of Consumer Protection commissioner to issue regulations defining what constitutes an unfair trade practice, investigate complaints, issue cease and desist orders, order restitution in cases involving less than $10,000, enter into consent agreements, ask the attorney general to seek injunctive relief, and accept voluntary statements of compliance. It also allows individuals to sue. Courts may issue restraining orders; award actual and punitive damages, costs, and reasonable attorney's fees; and impose civil penalties of up to $5,000 for willful violations and $25,000 for a violation of a restraining order (CGS § 42-110a et seq.).

Health Information Technology for Economic and Clinical Health (HITECH) Act

The federal HITECH Act (P. L. 111-5, § 13402(h)(2)) addresses privacy and security concerns associated with electronically transmitting health information through several provisions that strengthen the civil and criminal enforcement of federal HIPAA rules.