House of Representatives

General Assembly

File No. 9

January Session, 2021

Substitute House Bill No. 5310

House of Representatives, March 4, 2021

The Committee on General Law reported through REP. D'AGOSTINO of the 91st Dist., Chairperson of the Committee on the part of the House, that the substitute bill ought to pass.

AN ACT CONCERNING DATA PRIVACY BREACHES.

Be it enacted by the Senate and House of Representatives in General Assembly convened:

Section 1. Section 36a-701b of the general statutes, as amended by section 231 of public act 19-117 and section 9 of public act 19-196, is repealed and the following is substituted in lieu thereof (*Effective October 1, 2021*):

(a) For purposes of this section, (1) "breach of security" means unauthorized access to or unauthorized acquisition of electronic files, media, databases or computerized data, containing personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable; and (2) "personal information" means an individual's (A) first name or first initial and last name in combination with any one, or more, of the following data: **[**(A)**]** (i) Social Security number; **[**(B)**]** (ii) taxpayer identification number; (iii) identity protection personal identification number issued by the Internal Revenue Service; (iv) driver's license

number, [or] state identification card number, [; (C)] passport number, military identification number or other identification number issued by the government that is commonly used to verify identity; (v) credit or debit card number; [or (D)] (vi) financial account number in combination with any required security code, access code or password that would permit access to such financial account; (vii) medical information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; (viii) health insurance policy number or subscriber identification number, or any unique identifier used by a health insurer to identify the individual; or (ix) biometric information consisting of data generated by electronic measurements of an individual's unique physical characteristics used to authenticate or ascertain the individual's identity, such as a fingerprint, voice print, retina or iris image; or (B) user name or electronic mail address, in combination with a password or security question and answer that would permit access to an online account. "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media.

(b) (1) Any person who [conducts business in this state, and who, in the ordinary course of such person's business,] owns, licenses or maintains computerized data that includes personal information, shall provide notice of any breach of security following the discovery of the breach to any resident of this state whose personal information was breached or is reasonably believed to have been breached. Such notice shall be made without unreasonable delay but not later than [ninety] sixty days after the discovery of such breach, unless a shorter time is required under federal law, subject to the provisions of subsection (d) of this section. [and the completion of an investigation by such person to determine the nature and scope of the incident, to identify the individuals affected, or to restore the reasonable integrity of the data system.] If the person identifies additional residents of this state whose personal information was breached or reasonably believed to have been breached following sixty days after the discovery of such breach, the person shall proceed in good faith to notify such additional residents as

expediently as possible. Such notification shall not be required if, after an appropriate investigation [and consultation with relevant federal, state and local agencies responsible for law enforcement,] the person reasonably determines that the breach will not likely result in harm to the individuals whose personal information has been acquired [and] or accessed.

(2) If notice of a breach of security is required by subdivision (1) of this subsection:

(A) The person who [conducts business in this state, and who, in the ordinary course of such person's business,] owns, licenses or maintains computerized data that includes personal information, shall, not later than the time when notice is provided to the resident, also provide notice of the breach of security to the Attorney General; and

(B) The person who [conducts business in this state, and who, in the ordinary course of such person's business,] owns or licenses computerized data that includes personal information, shall offer to each resident whose [nonpublic] personal information under [subparagraph (B)(i) of subdivision (9) of subsection (b) of section 38a-38 or personal information as defined in] clause (i) or (ii) of subparagraph (A) of subdivision (2) of subsection (a) of this section was breached or is reasonably believed to have been breached, appropriate identity theft prevention services and, if applicable, identity theft mitigation services. Such service or services shall be provided at no cost to such resident for a period of not less than twenty-four months. Such person shall provide all information necessary for such resident to enroll in such service or services and shall include information on how such resident can place a credit freeze on such resident's credit file.

(c) Any person that maintains computerized data that includes personal information that the person does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following its discovery, if the personal information of a resident of this state was breached or is reasonably believed to have been breached.

(d) Any notification required by this section shall be delayed for a reasonable period of time if a law enforcement agency determines that the notification will impede a criminal investigation and such law enforcement agency has made a request that the notification be delayed. Any such delayed notification shall be made after such law enforcement agency determines that notification will not compromise the criminal investigation and so notifies the person of such determination.

(e) Any notice to a resident, owner or licensee required by the provisions of this section may be provided by one of the following methods, subject to the provisions of subsection (f) of this section: (1) Written notice; (2) telephone notice; (3) electronic notice, provided such notice is consistent with the provisions regarding electronic records and signatures set forth in 15 USC 7001; (4) substitute notice, provided such person demonstrates that the cost of providing notice in accordance with subdivision (1), (2) or (3) of this subsection would exceed two hundred fifty thousand dollars, that the affected class of subject persons to be notified exceeds five hundred thousand persons or that the person does not have sufficient contact information. Substitute notice shall consist of the following: (A) Electronic mail notice when the person has an electronic mail address for the affected persons; (B) conspicuous posting of the notice on the web site of the person if the person maintains one; and (C) notification to major state-wide media, including newspapers, radio and television.

(f) (1) In the event of a breach of login credentials under subparagraph (B) of subdivision (2) of subsection (a) of this section, notice to a resident may be provided in electronic or other form that 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, as applicable, or to take other appropriate steps to protect the affected online account and all other online accounts for which the resident uses the same user name or electronic mail address and password or security question and answer.

(2) Any person that furnishes an electronic mail account shall not

comply with this section by providing notification to the electronic mail account that was breached or reasonably believed to have been breached if the person cannot reasonably verify the affected resident's receipt of such notification. In such an event, the person shall provide notice by another method described in this section or by clear and conspicuous notice delivered to the resident online when the resident is connected to the online account from an Internet protocol address or online location from which the person knows the resident customarily accesses the account.

[(f)**]** (g) Any person that maintains such person's own security breach procedures as part of an information security policy for the treatment of personal information and otherwise complies with the timing requirements of this section, shall be deemed to be in compliance with the security breach notification requirements of this section, provided such person notifies, as applicable, residents of this state, owners and licensees in accordance with such person's policies in the event of a breach of security and in the case of notice to a resident, such person also notifies the Attorney General not later than the time when notice is provided to the resident. Any person that maintains such a security breach procedure pursuant to the rules, regulations, procedures or guidelines established by the primary or functional regulator, as defined in 15 USC 6809(2), shall be deemed to be in compliance with the security breach notification requirements of this section, provided (1) such person notifies, as applicable, such residents of this state, owners, and licensees required to be notified under and in accordance with the policies or the rules, regulations, procedures or guidelines established by the primary or functional regulator in the event of a breach of security, and (2) if notice is given to a resident of this state in accordance with subdivision (1) of this subsection regarding a breach of security, such person also notifies the Attorney General not later than the time when notice is provided to the resident.

(h) Any person that is subject to and in compliance with the privacy and security standards under the Health Insurance Portability and Accountability Act of 1996 and the Health Information Technology for

Economic and Clinical Health Act ("HITECH") shall be deemed to be in compliance with this section, provided that (1) any person required to provide notification to Connecticut residents pursuant to HITECH shall also provide notice to the Attorney General not later than the time when notice is provided to such residents if notification to the Attorney General would otherwise be required under subparagraph (A) of subdivision (2) of subsection (b) of this section, and (2) the person otherwise complies with the requirements of subparagraph (B) of subdivision (2) of subsection (b) of this section.

(i) All documents, materials and information provided in response to an investigative demand issued pursuant to subsection (c) of section 42-110d in connection with the investigation of a breach of security as defined by this section shall be exempt from public disclosure under subsection (a) of section 1-210, provided the Attorney General may make such documents, materials or information available to third parties in furtherance of such investigation.

[(g)**]** (j) Failure to comply with the requirements of this section shall constitute an unfair trade practice for purposes of section 42-110b and shall be enforced by the Attorney General.

This act shall take effect as follows and shall amend the following sections:		
Section 1	*October 1, 2021*	36a-701b

GL *Joint Favorable Subst.*

The following Fiscal Impact Statement and Bill Analysis are prepared for the benefit of the members of the General Assembly, solely for purposes of information, summarization and explanation and do not represent the intent of the General Assembly or either chamber thereof for any purpose. In general, fiscal impacts are based upon a variety of informational sources, including the analyst's professional knowledge. Whenever applicable, agency data is consulted as part of the analysis, however final products do not necessarily reflect an assessment from any specific department.

OFA Fiscal Note

State Impact: None

Municipal Impact: None

Explanation

The bill expands data breach notification requirements to include additional types of consumer information and, extends current data breach notification requirements to include managers of electronic data. Also, the bill shortens the notification period, from 90 to 60 days after detection of a security breach, for data managers to inform consumers and the attorney general.

No fiscal impact is anticipated as any additional violations filed due to these expanded notification requirements are expected to be minimal.

The Out Years

State Impact: None

Municipal Impact: None

OLR Bill Analysis
sHB 5310

AN ACT CONCERNING DATA PRIVACY BREACHES.

SUMMARY

This bill 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 current 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 bill generally shortens the maximum notification period, from 90 to 60 days after the security breach was discovered, for data managers to inform consumers and the attorney general.

The bill 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 bill deems violations of the data breach notification law a Connecticut Unfair Trade Practices Act (CUTPA) violation (see BACKGROUND). Additionally, under the bill, 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 bill 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. Under existing 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. The bill additionally includes the following:

1. taxpayer identification number;
2. identity protection personal identification number issued by the Internal Revenue Service;
3. passport number;
4. military identification number;
5. other identification number the government issues that is commonly used to verify identity;
6. information about the person's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional;
7. health insurance policy number or subscriber identification number, or any unique identifier a health insurer uses to identify the person; or
8. biometric data generated by electronic measurements of the person's unique physical characteristics used to authenticate or ascertain identity (e.g., fingerprint, voice print, retina or iris image).

Under the bill, "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 current law, with some exceptions, data managers must notify consumers and the attorney general of any data breach within 90 days of discovering it and completing an investigation to determine the incident's nature and scope, identify affected individuals, or restore the data system's integrity. The bill eliminates the investigation requirement and shortens the timeframe from 90 to 60 days after the security breach is discovered. The bill 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 current law, the notification is not required if after an appropriate investigation and consultation with relevant federal, state, and local law enforcement, the data manager reasonably determines the breach will not likely result in harm to the individuals whose personal information has been acquired and accessed. The bill 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 current law, those who own or license computerized data that includes personal information must 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 at least 24 months. The bill 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

Under existing law, notice to a resident may be provided through written notice, telephone, 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, or (3) there is not sufficient contact information. One type of substitute notice is by e-mail.

Under the bill, data managers that furnish e-mail accounts must not comply 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 online location the data manager knows the resident customarily uses to access the account.

Login Credentials

Under the bill, 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 bill, any 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. In order to be in compliance, data managers must:

1. notify the attorney general in the same timeframe as 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.

COMMITTEE ACTION

General Law Committee

Joint Favorable Substitute
Yea 19 Nay 0 (02/16/2021)