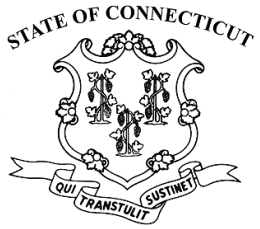

Substitute House Bill No. 5310

Public Act No. 21-59

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of the general statutes, as amended by section 231 of public act 19-117 and section 9 of public act 19-196, is repealed and the following is substituted in lieu thereof (*Effective October 1, 2021*):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

Approved June 16, 2021