General Assembly

Raised Bill No. 117

February Session, 2026

LCO No. **1087**

Referred to Committee on GENERAL LAW

Introduced by:
(GL)

AN ACT CONCERNING BREACHES OF SECURITY INVOLVING ELECTRONIC PERSONAL INFORMATION.

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

Section 1. Section 36a-701b of the general statutes is repealed and the following is substituted in lieu thereof (*Effective October 1, 2026*):

(a) For purposes of this section: **[**,**]**

(1) **[**"breach of security"**]** "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"**]**

(2) "Massive breach of security" means a breach of security where (A) the personal information of at least one hundred thousand residents of this state has been breached or is reasonably believed to have been breached, and (B) the breach of security occurred due to the

unauthorized use of a computer or computer network; and

(3) "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: (i) Social Security number; (ii) taxpayer identification number; (iii) identity protection personal identification number issued by the Internal Revenue Service; (iv) driver's license number, state identification card number, 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; (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; (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 **[**,**]** or retina or iris image; or (x) precise geolocation data, as defined in section 42-515; 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 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 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. 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, the person reasonably determines that the breach will not likely result in harm to the individuals whose personal information has been acquired or accessed.

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

(A) The person who owns, licenses or maintains the computerized data that includes the 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 in a form and manner prescribed by the Attorney General; and

(B) The person who owns or licenses the computerized data that includes the personal information **[**,**]** shall offer to each resident whose personal information under clause (i) or (ii) of subparagraph (A) of subdivision **[**(2)**]** (3) 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 two years. 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**]** who maintains computerized data that includes personal information that the person does not own shall notify the owner or licensee of the personal 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**]** such 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, **[**;**]** as amended from time to time; or (4) substitute notice, provided such person demonstrates in the notice provided to the Attorney General 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, but not limited to, newspapers, radio and television.

(f) (1) In the event of a breach of login credentials under subparagraph (B) of subdivision **[**(2)**]** (3) of subsection (a) of this section, notice to a resident may be provided in an 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**]** who furnishes an electronic mail account shall not **[**comply**]** be deemed to have complied with this section **[**by providing**]** if such person provides notification to the electronic mail account that was breached, or is reasonably believed to have been breached, **[**if the person**]** and 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.

(g) Any person **[**that**]** who 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, in a form and manner prescribed by the Attorney General, not later than the time when notice is provided to the resident. Any person **[**that**]** who 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), as amended from time to time, 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, in a form and manner prescribed by the Attorney General, not later than the time when notice is provided to the resident.

(h) Any person **[**that**]** who 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"), as either of said acts may be amended from time to time, 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, in a form and manner prescribed by 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) (1) Notwithstanding the provisions of subsections (g) and (h) of this section, any person who owns, licenses or maintains computerized data that includes personal information shall (A) immediately following the discovery of a massive breach of security, retain a third party who has experience performing forensic examinations and analyses of computers or computer networks to (i) perform a forensic examination and analysis of the computer or computer network that was the subject of the unauthorized use that gave rise to the massive breach of security, and (ii) prepare a detailed forensic report disclosing, at a minimum, (I) the results of the forensic examination and analysis, and (II) how the unauthorized use that gave rise to the massive breach of security occurred, as well as the root causes of such unauthorized use, to the extent the forensic examination and analysis revealed such information,

and (B) not later than ninety days following the discovery of the massive breach of security, submit to the Attorney General, in a form and manner prescribed by the Attorney General, the forensic report prepared pursuant to subparagraph (A)(ii) of this subdivision.

(2) If any person fails to submit a forensic report to the Attorney General in accordance with the provisions of subdivision (1) of this subsection, the Attorney General may retain a third party who has experience performing forensic examinations and analyses of computers or computer networks to (A) perform a forensic examination and analysis pursuant to subparagraph (A)(i) of subdivision (1) of this subsection, and (B) prepare and submit the forensic report to the Attorney General in accordance with the provisions of subdivision (1) of this subsection.

(3) Any person who retains a third party to perform a forensic examination and analysis and submit a forensic report to the Attorney General pursuant to subdivision (1) of this subsection, or who fails to submit a forensic report to the Attorney General as set forth in subdivision (2) of this subsection, shall bear the cost of the forensic examination and analysis performed, and of the forensic report submitted, pursuant to subdivision (1) or (2) of this subsection, as applicable.

[(i)**]** (j) 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**]** and all forensic reports provided to the Attorney General pursuant to subsection (i) of 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 or forensic reports available to third parties in furtherance of such investigation.

[(j)**]** (k) (1) 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.

(2) In addition to any penalty imposed under chapter 735a, any person who fails to submit a forensic report to the Attorney General in accordance with the provisions of subdivision (1) of subsection (i) of this section shall be subject to a civil penalty (A) in the amount of one hundred thousand dollars if such person is a small business, as defined by the United States Small Business Administration, or (B) in the amount of five hundred thousand dollars if such person is not a small business, as defined by the United States Small Business Administration.

[(k)**]** (l) Any civil penalties collected for failure to comply with the requirements of this section may be deposited into the privacy protection guaranty and enforcement account established pursuant to section 42-472a.

This act shall take effect as follows and shall amend the following sections:		
Section 1	*October 1, 2026*	36a-701b

Statement of Purpose:

To (1) provide that certain materials provided to the Attorney General following a breach of security involving electronic personal information shall be provided to the Attorney General in a form and manner prescribed by the Attorney General, (2) define "massive breach of security", (3) require a third-party forensic examination, analysis and report following a massive breach of security, and (4) impose an additional penalty for any person who fails to submit a third-party forensic report to the Attorney General following a massive breach of security.

[Proposed deletions are enclosed in brackets. Proposed additions are indicated by underline, except that when the entire text of a bill or resolution or a section of a bill or resolution is new, it is not underlined.]