Senate

General Assembly

File No. 340

February Session, 2026

Substitute Senate Bill No. 117

Senate, April 2, 2026

The Committee on General Law reported through SEN. MARONEY of the 14th Dist., Chairperson of the Committee on the part of the Senate, that the substitute bill ought to pass.

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 Section 36a-701b of the general statutes is repealed and the following is substituted in lieu thereof (*Effective October 1, 2026*):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 likely to have been breached, and (B) the breach of security occurred due to any unauthorized access to, or any 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. In the case of a massive breach of security, the performance of a forensic examination and analysis by a third party as required under subsection (i) of this section shall also be delayed if a law enforcement agency determines that the performance of such examination and analysis will impede a criminal investigation and such law enforcement agency has made a request that performance of such examination and analysis be delayed. Any such delayed examination and analysis shall be performed after such law enforcement agency determines that performance of such examination and analysis 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 affected resident online when the affected resident is connected to the online account from an Internet protocol address or online location from which the person knows the affected 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, subject to the provisions of subsection (d) of this section, (A) immediately following the discovery of any unauthorized access to, or any unauthorized use of, a computer or computer network that will likely result in 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 such unauthorized access or use, and (ii) prepare a detailed forensic report disclosing, at a minimum, (I) the results of the forensic examination and analysis, and (II) how such unauthorized access or use occurred, as well as the root causes of such unauthorized access or use, to the extent the forensic examination and analysis revealed such information, and (B) not later than sixty days following the discovery of any unauthorized access to, or any unauthorized use of, a computer or computer network that will likely result in a massive breach of security, submit to the Attorney General, in a form and manner prescribed by the Attorney General, a reasonable timeline to (i) prepare the detailed forensic report, and (ii) submit such report to the Attorney General upon request by the Attorney General.

(2) If any person fails to submit a detailed forensic report to the Attorney General, upon request by the Attorney General and in a form and manner prescribed by the Attorney General, 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 detailed 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 prepare a detailed forensic report for submission to the Attorney General pursuant to subdivision (1) of this subsection, or who fails to submit a detailed 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 detailed 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 prepared 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. To the extent any forensic report prepared pursuant to subsection (i) of this section includes information subject to attorney-client privilege or work product protection, submission of such report to the Attorney General shall not constitute a waiver of such privilege or protection.

[(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 detailed forensic report to the Attorney General, upon request by the Attorney General and in a form and manner prescribed by the Attorney General, in accordance with the provisions of subsection (i) of this section shall be subject to a civil penalty in an amount not to exceed two hundred fifty thousand dollars. In determining the amount of the civil penalty to be imposed on such person, the court shall consider whether such person is (A) a small business or micro business, as such terms are defined in section 32-344, or (B) a nonprofit employer that employs (i) not more than five hundred employees, or (ii) fewer than fifty full-time employees.

[(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 Legislative Commissioners:
In Subsec. (f)(2), "resident" was changed to "affected resident" for internal consistency.

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:

Agency Affected	Fund-Effect	FY 27 $	FY 28 $
Resources of the General Fund	GF - Potential Revenue Gain	See Below	See Below

Note: GF=General Fund

Municipal Impact: None

Explanation

The bill requires a forensic examination for a massive breach of security[1] and allows the Office of the Attorney General (OAG) to issue a civil penalty of up to $250,000 for noncompliance, resulting in a potential revenue gain to the General Fund to the extent violations occur.

The bill also makes violations an unfair trade practice enforced by the OAG resulting in no fiscal impact because the OAG has the resources and expertise to meet the requirements of the bill.

The Out Years

The annualized ongoing fiscal impact identified above would continue into the future subject to the number of violations.

[1]The bill requires the person or entity who experiences a massive breach of security to pay for a third-party to conduct a forensic examination.

OLR Bill Analysis

sSB 117

AN ACT CONCERNING BREACHES OF SECURITY INVOLVING ELECTRONIC PERSONAL INFORMATION.

SUMMARY

This bill requires a person or entity with computerized data that includes personal information to immediately retain a third party for a forensic examination after discovering a massive breach of security. A "massive breach of security" is a breach or a likely breach of at least 100,000 residents' personal information through unauthorized access to or use of a computer or computer network. The law generally already requires these people and entities to notify affected individuals and the attorney general about any security breach and offer identity theft protection to certain affected individuals. It also makes it a Connecticut Unfair Trade Practices Act (CUTPA) violation to violate these provisions.

Within 60 days of discovering a breach that likely results in a massive breach of security, the bill requires the person or entity to give the attorney general, in a way set by the attorney general, a reasonable timeline for (1) preparing the forensic report and (2) submitting it, if requested, to the attorney general. If the person or entity does not submit a requested report in a way set by the attorney general, the attorney general can have a third party conduct the examination and produce a report.

The bill delays a required forensic examination if a law enforcement agency requests a delay because the examination will impede a criminal investigation. The delay ends when the law enforcement agency issues notice that the examination will not compromise the investigation.

The bill exempts these forensic reports and other information related

to investigations under the bill from disclosure under the Freedom of Information Act (FOIA). It also (1) makes violations of the bill a CUTPA violation that is enforced by the attorney general and (2) allows the attorney general to impose a civil penalty of up to $250,000 for failing to submit a requested forensic report to the attorney general.

The bill also makes minor, technical, and conforming changes, including that when the law requires certain security breach notices to the attorney general, they be in a form and manner set by the attorney general.

EFFECTIVE DATE: October 1, 2016

FORENSIC EXAMINATION AND REPORT

The bill requires the third party retained for a forensic examination under the bill to have experience in forensic examinations and analyzing computers or computer networks. The third party must produce a detailed forensic report that includes (1) the examination and analysis results and (2) how the unauthorized access or use occurred and its root causes, if known.

The person or entity discovering the massive breach of security must pay for the cost of the examination, analysis, and report, whether the third party is retained by the person or entity or the attorney general.

FOIA

Under existing law, information provided as part of a response to an investigation of a CUTPA violation related to a security breach is exempt from disclosure under FOIA, but the attorney general may give this information to third parties as part of the investigation. The bill extends this exemption to cover CUTPA investigations related to the bill's provisions, exempts the bill's required forensic reports from disclosure under FOIA, and allows the attorney general to make the reports available to third parties as part of a CUTPA investigation.

The bill specifies that submitting the forensic reports to the attorney general does not waive the attorney-client privilege or work product

protection, if it applies to specific information in the reports.

PENALTIES

By law, it is a CUTPA violation, enforceable by the attorney general, for failing to comply with existing law's security breach notice requirements. The bill expands this to also include violations of the bill's requirements.

In addition to CUTPA penalties, the bill allows the attorney general to impose a civil penalty of up to $250,000 for failure to submit a requested forensic report. The bill requires a court, presumably if reviewing the amount of the civil penalty on appeal, to consider whether the business is a (1) for profit small business with up to 500 employees, (2) independently owned and operated business with less than 50 full-time employees or less than $5 million in gross annual sales (a micro business), or (3) nonprofit entity employing up to 500 employees or less than 50 full-time employees.

As with civil penalties related to violating the law's security breach notice requirements, the bill permits depositing civil penalties collected for violating the bill's provisions in the privacy protection guaranty and enforcement account. By law, this account is used to enforce certain laws about safeguarding personal information and reimburses individuals hurt by violations of these provisions.

BACKGROUND

Breach of Security

By law, a "breach of security" is unauthorized access to, or acquisition of, electronic files, media, databases or computerized data containing personal information when access to that information has not been secured by encryption or alternate means rendering it unreadable or unusable.

Personal Information

By law, "personal information" includes a person's first name or first initial and last name combined with certain information such as a social

security, taxpayer identification, driver's license, credit or debit card number; medical or biometric information; geolocation data; or user name or email address combined with a password or security question and answer. It does not include information that is lawfully available to the public from government or widely distributed media.

CUTPA

By law, CUTPA prohibits businesses from engaging in unfair and deceptive acts or practices. It allows the Department of Consumer Protection commissioner, under specified procedures, to issue regulations defining an unfair trade practice, investigate complaints, issue cease and desist orders, order restitution in cases involving less than $10,000, impose civil penalties of up to $5,000**,** 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 up to $25,000 for a restraining order violation.

COMMITTEE ACTION

General Law Committee

Joint Favorable Substitute
Yea 21 Nay 0 (03/16/2026)