



General Assembly

Substitute Bill No. 117

February Session, 2026



**AN ACT CONCERNING BREACHES OF SECURITY INVOLVING
ELECTRONIC PERSONAL INFORMATION.**

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

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 Section 36a-701b of the general statutes is repealed and the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

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

4 (1) ["breach of security"] "Breach of security" means unauthorized
5 access to, or unauthorized acquisition of, electronic files, media,
6 databases or computerized data [,] containing personal information
7 when access to the personal information has not been secured by
8 encryption or by any other method or technology that renders the
9 personal information unreadable or unusable; [and (2) "personal
10 information"]

11 (2) "Massive breach of security" means a breach of security where (A)
12 the personal information of at least one hundred thousand residents of
13 this state has been breached or is likely to have been breached, and (B)
14 the breach of security occurred due to any unauthorized access to, or
15 any unauthorized use of, a computer or computer network; and

16 (3) "Personal information" means an individual's (A) first name or
17 first initial and last name in combination with any one, or more, of the

18 following data: (i) Social Security number; (ii) taxpayer identification
19 number; (iii) identity protection personal identification number issued
20 by the Internal Revenue Service; (iv) driver's license number, state
21 identification card number, passport number, military identification
22 number or other identification number issued by the government that is
23 commonly used to verify identity; (v) credit or debit card number; (vi)
24 financial account number in combination with any required security
25 code, access code or password that would permit access to such
26 financial account; (vii) medical information regarding an individual's
27 medical history, mental or physical condition [] or medical treatment or
28 diagnosis by a health care professional; (viii) health insurance policy
29 number or subscriber identification number, or any unique identifier
30 used by a health insurer to identify the individual; (ix) biometric
31 information consisting of data generated by electronic measurements of
32 an individual's unique physical characteristics used to authenticate or
33 ascertain the individual's identity, such as a fingerprint, voice print []
34 or retina or iris image; or (x) precise geolocation data, as defined in
35 section 42-515; or (B) user name or electronic mail address, in
36 combination with a password or security question and answer that
37 would permit access to an online account. "Personal information" does
38 not include publicly available information that is lawfully made
39 available to the general public from federal, state or local government
40 records or widely distributed media.

41 (b) (1) Any person who owns, licenses or maintains computerized
42 data that includes personal information [] shall provide notice of any
43 breach of security, following the discovery of the breach, to any resident
44 of this state whose personal information was breached or is reasonably
45 believed to have been breached. Such notice shall be made without
46 unreasonable delay but not later than sixty days after the discovery of
47 such breach, unless a shorter time is required under federal law, subject
48 to the provisions of subsection (d) of this section. If the person identifies
49 additional residents of this state whose personal information was
50 breached or reasonably believed to have been breached following sixty
51 days after the discovery of such breach, the person shall proceed in good

52 faith to notify such additional residents as expediently as possible. Such
53 notification shall not be required if, after an appropriate investigation,
54 the person reasonably determines that the breach will not likely result
55 in harm to the individuals whose personal information has been
56 acquired or accessed.

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

59 (A) The person who owns, licenses or maintains the computerized
60 data that includes the personal information [,] shall, not later than the
61 time when notice is provided to the resident, also provide notice of the
62 breach of security to the Attorney General in a form and manner
63 prescribed by the Attorney General; and

64 (B) The person who owns or licenses the computerized data that
65 includes the personal information [,] shall offer to each resident whose
66 personal information under clause (i) or (ii) of subparagraph (A) of
67 subdivision [(2)] (3) of subsection (a) of this section was breached, or is
68 reasonably believed to have been breached, appropriate identity theft
69 prevention services and, if applicable, identity theft mitigation services.
70 Such [service or] services shall be provided at no cost to such resident
71 for a period of not less than two years. Such person shall provide all
72 information necessary for such resident to enroll in such [service or]
73 services and shall include information on how such resident can place a
74 credit freeze on such resident's credit file.

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

81 (d) Any notification required by this section shall be delayed for a
82 reasonable period of time if a law enforcement agency determines that
83 the notification will impede a criminal investigation and such law

84 enforcement agency has made a request that [the] such notification be
85 delayed. Any such delayed notification shall be made after such law
86 enforcement agency determines that notification will not compromise
87 the criminal investigation and so notifies the person of such
88 determination. In the case of a massive breach of security, the
89 performance of a forensic examination and analysis by a third party as
90 required under subsection (i) of this section shall also be delayed if a law
91 enforcement agency determines that the performance of such
92 examination and analysis will impede a criminal investigation and such
93 law enforcement agency has made a request that performance of such
94 examination and analysis be delayed. Any such delayed examination
95 and analysis shall be performed after such law enforcement agency
96 determines that performance of such examination and analysis will not
97 compromise the criminal investigation and so notifies the person of such
98 determination.

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

116 (f) (1) In the event of a breach of login credentials under
117 subparagraph (B) of subdivision [(2)] (3) of subsection (a) of this section,

118 notice to a resident may be provided in an electronic or other form that
119 directs the resident whose personal information was breached, or is
120 reasonably believed to have been breached, to promptly change any
121 password or security question and answer, as applicable, or to take
122 other appropriate steps to protect the affected online account and all
123 other online accounts for which the resident uses the same user name or
124 electronic mail address and password or security question and answer.

125 (2) Any person [that] who furnishes an electronic mail account shall
126 not [comply] be deemed to have complied with this section [by
127 providing] if such person provides notification to the electronic mail
128 account that was breached, or is reasonably believed to have been
129 breached, [if the person] and cannot reasonably verify the affected
130 resident's receipt of such notification. In such an event, the person shall
131 provide notice by another method described in this section or by clear
132 and conspicuous notice delivered to the affected resident online when
133 the affected resident is connected to the online account from an Internet
134 protocol address or online location from which the person knows the
135 affected resident customarily accesses the account.

136 (g) Any person [that] who maintains such person's own security
137 breach procedures as part of an information security policy for the
138 treatment of personal information, and otherwise complies with the
139 timing requirements of this section, shall be deemed to be in compliance
140 with the security breach notification requirements of this section,
141 provided such person notifies, as applicable, residents of this state,
142 owners and licensees in accordance with such person's policies in the
143 event of a breach of security and, in the case of notice to a resident, such
144 person also notifies the Attorney General, in a form and manner
145 prescribed by the Attorney General, not later than the time when notice
146 is provided to the resident. Any person [that] who maintains such a
147 security breach procedure pursuant to the rules, regulations, procedures
148 or guidelines established by the primary or functional regulator, as
149 defined in 15 USC 6809(2), as amended from time to time, shall be
150 deemed to be in compliance with the security breach notification
151 requirements of this section, provided (1) such person notifies, as

152 applicable, such residents of this state, owners [,] and licensees required
153 to be notified under, and in accordance with, the policies or the rules,
154 regulations, procedures or guidelines established by the primary or
155 functional regulator in the event of a breach of security, and (2) if notice
156 is given to a resident of this state in accordance with subdivision (1) of
157 this subsection regarding a breach of security, such person also notifies
158 the Attorney General, in a form and manner prescribed by the Attorney
159 General, not later than the time when notice is provided to the resident.

160 (h) Any person [that] who is subject to, and in compliance with, the
161 privacy and security standards under the Health Insurance Portability
162 and Accountability Act of 1996 and the Health Information Technology
163 for Economic and Clinical Health Act ("HITECH"), as either of said acts
164 may be amended from time to time, shall be deemed to be in compliance
165 with this section, provided [that] (1) any person required to provide
166 notification to Connecticut residents pursuant to HITECH shall also
167 provide notice to the Attorney General, in a form and manner
168 prescribed by the Attorney General, not later than the time when notice
169 is provided to such residents if notification to the Attorney General
170 would otherwise be required under subparagraph (A) of subdivision (2)
171 of subsection (b) of this section, and (2) the person otherwise complies
172 with the requirements of subparagraph (B) of subdivision (2) of
173 subsection (b) of this section.

174 (i) (1) Notwithstanding the provisions of subsections (g) and (h) of
175 this section, any person who owns, licenses or maintains computerized
176 data that includes personal information shall, subject to the provisions
177 of subsection (d) of this section, (A) immediately following the
178 discovery of any unauthorized access to, or any unauthorized use of, a
179 computer or computer network that will likely result in a massive
180 breach of security, retain a third party who has experience performing
181 forensic examinations and analyses of computers or computer networks
182 to (i) perform a forensic examination and analysis of the computer or
183 computer network that was the subject of such unauthorized access or
184 use, and (ii) prepare a detailed forensic report disclosing, at a minimum,
185 (I) the results of the forensic examination and analysis, and (II) how such

186 unauthorized access or use occurred, as well as the root causes of such
187 unauthorized access or use, to the extent the forensic examination and
188 analysis revealed such information, and (B) not later than sixty days
189 following the discovery of any unauthorized access to, or any
190 unauthorized use of, a computer or computer network that will likely
191 result in a massive breach of security, submit to the Attorney General,
192 in a form and manner prescribed by the Attorney General, a reasonable
193 timeline to (i) prepare the detailed forensic report, and (ii) submit such
194 report to the Attorney General upon request by the Attorney General.

195 (2) If any person fails to submit a detailed forensic report to the
196 Attorney General, upon request by the Attorney General and in a form
197 and manner prescribed by the Attorney General, the Attorney General
198 may retain a third party who has experience performing forensic
199 examinations and analyses of computers or computer networks to (A)
200 perform a forensic examination and analysis pursuant to subparagraph
201 (A)(i) of subdivision (1) of this subsection, and (B) prepare and submit
202 the detailed forensic report to the Attorney General in accordance with
203 the provisions of subdivision (1) of this subsection.

204 (3) Any person who retains a third party to perform a forensic
205 examination and analysis and prepare a detailed forensic report for
206 submission to the Attorney General pursuant to subdivision (1) of this
207 subsection, or who fails to submit a detailed forensic report to the
208 Attorney General as set forth in subdivision (2) of this subsection, shall
209 bear the cost of the forensic examination and analysis performed, and of
210 the detailed forensic report submitted, pursuant to subdivision (1) or (2)
211 of this subsection, as applicable.

212 [(i)] (j) All documents, materials and information provided in
213 response to an investigative demand issued pursuant to subsection (c)
214 of section 42-110d in connection with the investigation of a breach of
215 security, [as defined by this section] and all forensic reports prepared
216 pursuant to subsection (i) of this section, shall be exempt from public
217 disclosure under subsection (a) of section 1-210, provided the Attorney
218 General may make such documents, materials, [or] information or

219 forensic reports available to third parties in furtherance of such
220 investigation. To the extent any forensic report prepared pursuant to
221 subsection (i) of this section includes information subject to attorney-
222 client privilege or work product protection, submission of such report
223 to the Attorney General shall not constitute a waiver of such privilege
224 or protection.

225 [(j)] (k) (1) Failure to comply with the requirements of this section
226 shall constitute an unfair trade practice for purposes of section 42-110b
227 and shall be enforced by the Attorney General.

228 (2) In addition to any penalty imposed under chapter 735a, any
229 person who fails to submit a detailed forensic report to the Attorney
230 General, upon request by the Attorney General and in a form and
231 manner prescribed by the Attorney General, in accordance with the
232 provisions of subsection (i) of this section shall be subject to a civil
233 penalty in an amount not to exceed two hundred fifty thousand dollars.
234 In determining the amount of the civil penalty to be imposed on such
235 person, the court shall consider whether such person is (A) a small
236 business or micro business, as such terms are defined in section 32-344,
237 or (B) a nonprofit employer that employs (i) not more than five hundred
238 employees, or (ii) fewer than fifty full-time employees.

239 [(k)] (l) Any civil penalties collected for failure to comply with the
240 requirements of this section may be deposited into the privacy
241 protection guaranty and enforcement account established pursuant to
242 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.*