



General Assembly

Amendment

February Session, 2026

LCO No. 5001



Offered by:

SEN. MARONEY, 14th Dist.

REP. LEMAR, 96th Dist.

REP. TURCO, 27th Dist.

To: Subst. Senate Bill No. 117

File No. 340

Cal. No. 226

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

1 Strike everything after the enacting clause and substitute the
2 following in lieu thereof:

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 Section 36a-701b of the general statutes is repealed and the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

5 (a) For purposes of this section: []

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

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

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

44 (b) (1) Any person who owns, licenses or maintains computerized
45 data that includes personal information [] shall provide notice of any

46 breach of security, following the discovery of the breach, to any resident
47 of this state whose personal information was breached or is reasonably
48 believed to have been breached. Such notice shall be made without
49 unreasonable delay but not later than sixty days after the discovery of
50 such breach, unless a shorter time is required under federal law, subject
51 to the provisions of subsection (d) of this section. If the person identifies
52 additional residents of this state whose personal information was
53 breached or reasonably believed to have been breached following sixty
54 days after the discovery of such breach, the person shall proceed in good
55 faith to notify such additional residents as expediently as possible. Such
56 notification shall not be required if, after an appropriate investigation,
57 the person reasonably determines that the breach will not likely result
58 in harm to the individuals whose personal information has been
59 acquired or accessed.

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

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

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

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

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

102 (e) Any notice to a resident, owner or licensee required by the
103 provisions of this section may be provided by one of the following
104 methods, subject to the provisions of subsection (f) of this section: (1)
105 Written notice; (2) telephone notice; (3) electronic notice, provided such
106 notice is consistent with the provisions regarding electronic records and
107 signatures set forth in 15 USC 7001, [;] as amended from time to time; or
108 (4) substitute notice, provided such person demonstrates in the notice
109 provided to the Attorney General that the cost of providing notice in
110 accordance with subdivision (1), (2) or (3) of this subsection would

111 exceed two hundred fifty thousand dollars, that the affected class of
112 subject persons to be notified exceeds five hundred thousand persons or
113 that the person does not have sufficient contact information. Substitute
114 notice shall consist of the following: (A) Electronic mail notice when the
115 person has an electronic mail address for the affected persons; (B)
116 conspicuous posting of the notice on the web site of the person if the
117 person maintains one; and (C) notification to major state-wide media,
118 including, but not limited to, newspapers, radio and television.

119 (f) (1) In the event of a breach of login credentials under
120 subparagraph (B) of subdivision [(2)] (3) of subsection (a) of this section,
121 notice to a resident may be provided in an electronic or other form that
122 directs the resident whose personal information was breached, or is
123 reasonably believed to have been breached, to promptly change any
124 password or security question and answer, as applicable, or to take
125 other appropriate steps to protect the affected online account and all
126 other online accounts for which the resident uses the same user name or
127 electronic mail address and password or security question and answer.

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

139 (g) Any person [that] who maintains such person's own security
140 breach procedures as part of an information security policy for the
141 treatment of personal information, and otherwise complies with the
142 timing requirements of this section, shall be deemed to be in compliance
143 with the security breach notification requirements of this section,

144 provided such person notifies, as applicable, residents of this state,
145 owners and licensees in accordance with such person's policies in the
146 event of a breach of security and, in the case of notice to a resident, such
147 person also notifies the Attorney General, in a form and manner
148 prescribed by the Attorney General, not later than the time when notice
149 is provided to the resident. Any person [that] who maintains such a
150 security breach procedure pursuant to the rules, regulations, procedures
151 or guidelines established by the primary or functional regulator, as
152 defined in 15 USC 6809(2), as amended from time to time, shall be
153 deemed to be in compliance with the security breach notification
154 requirements of this section, provided (1) such person notifies, as
155 applicable, such residents of this state, owners [] and licensees required
156 to be notified under, and in accordance with, the policies or the rules,
157 regulations, procedures or guidelines established by the primary or
158 functional regulator in the event of a breach of security, and (2) if notice
159 is given to a resident of this state in accordance with subdivision (1) of
160 this subsection regarding a breach of security, such person also notifies
161 the Attorney General, in a form and manner prescribed by the Attorney
162 General, not later than the time when notice is provided to the resident.

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

177 (i) (1) Notwithstanding the provisions of subsections (g) and (h) of
178 this section, any person who owns, licenses or maintains computerized
179 data that includes personal information shall, subject to the provisions
180 of subsection (d) of this section, (A) promptly following the discovery
181 of any unauthorized access to, or any unauthorized use of, a computer
182 or computer network owned or controlled by such person that will
183 likely result in a massive breach of security, retain a third party who has
184 experience performing forensic examinations and analyses of
185 computers or computer networks to (i) perform a forensic examination
186 and analysis of the computer or computer network that was the subject
187 of such unauthorized access or use, and (ii) prepare a detailed forensic
188 report disclosing, at a minimum, (I) the results of the forensic
189 examination and analysis, and (II) how such unauthorized access or use
190 occurred, as well as the root causes of such unauthorized access or use,
191 to the extent the forensic examination and analysis revealed such
192 information, and (B) not later than sixty days following the discovery of
193 any unauthorized access to, or any unauthorized use of, a computer or
194 computer network that will likely result in a massive breach of security,
195 submit to the Attorney General, in a form and manner prescribed by the
196 Attorney General, a reasonable timeline to (i) prepare the detailed
197 forensic report, and (ii) submit such report to the Attorney General upon
198 request by the Attorney General.

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

208 (3) Any person who retains a third party to perform a forensic
209 examination and analysis and prepare a detailed forensic report for

210 submission to the Attorney General pursuant to subdivision (1) of this
211 subsection, or who fails to submit a detailed forensic report to the
212 Attorney General as set forth in subdivision (2) of this subsection, shall
213 bear the cost of the forensic examination and analysis performed, and of
214 the detailed forensic report submitted, pursuant to subdivision (1) or (2)
215 of this subsection, as applicable.

216 (4) Nothing in subdivisions (1) to (3), inclusive, of this subsection
217 shall be construed to prohibit any person who reports a massive breach
218 of security from (A) working with the third party retained pursuant to
219 subdivision (1) of this subsection to (i) investigate the unauthorized
220 access to, or unauthorized use of, the computer or computer network
221 owned or controlled by such person, or (ii) prepare the detailed forensic
222 report pursuant to subdivision (1) of this subsection, or (B) taking
223 appropriate measures to investigate or remediate the massive breach of
224 security.

225 (j) Nothing in this section shall be construed to provide that any
226 person who reports a breach of security or massive breach of security
227 has employed unreasonable data security. Any person who owns,
228 licenses or maintains personal information shall employ reasonable data
229 security.

230 [(i)] (k) All documents, materials and information provided in
231 response to an investigative demand issued pursuant to subsection (c)
232 of section 42-110d in connection with the investigation of a breach of
233 security, [as defined by this section] and all forensic reports prepared
234 pursuant to subsection (i) of this section, shall be exempt from public
235 disclosure under subsection (a) of section 1-210, provided the Attorney
236 General may make such documents, materials, [or] information or
237 forensic reports available to third parties in furtherance of such
238 investigation. To the extent any forensic report prepared pursuant to
239 subsection (i) of this section includes information subject to attorney-
240 client privilege or work product protection, submission of such report
241 to the Attorney General shall not constitute a waiver of such privilege
242 or protection.

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

246 (2) In addition to any penalty imposed under chapter 735a, any
 247 person who fails to submit a detailed forensic report to the Attorney
 248 General, upon request by the Attorney General and in a form and
 249 manner prescribed by the Attorney General, in accordance with the
 250 provisions of subsection (i) of this section shall be subject to a civil
 251 penalty in an amount not to exceed two hundred fifty thousand dollars.
 252 In determining the amount of the civil penalty to be imposed on such
 253 person, the court shall consider whether such person (A) is a small
 254 business or micro business, as such terms are defined in section 32-344,
 255 (B) is a nonprofit employer that employs (i) not more than five hundred
 256 employees, or (ii) fewer than fifty full-time employees, or (C)
 257 demonstrates financial distress.

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

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