

**Proposed Substitute
Bill No. 5310**

LCO No. 3416

AN ACT CONCERNING DATA PRIVACY BREACHES.

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

1 Section 1. Section 36a-701b of the general statutes, as amended by
2 section 231 of public act 19-117 and section 9 of public act 19-196, is
3 repealed and the following is substituted in lieu thereof (*Effective October*
4 *1, 2021*):

5 (a) For purposes of this section, (1) "breach of security" means
6 unauthorized access to or unauthorized acquisition of electronic files,
7 media, databases or computerized data, containing personal
8 information when access to the personal information has not been
9 secured by encryption or by any other method or technology that
10 renders the personal information unreadable or unusable; and (2)
11 "personal information" means (A) an individual's first name or first
12 initial and last name in combination with any one, or more, of the
13 following data: [(A)] (i) Social Security number; (ii) individual taxpayer
14 identification number; (iii) identity protection personal identification
15 number issued by the Internal Revenue Service; [(B)] (iv) driver's license
16 number, [or] state identification card number, passport number,
17 military identification number, or other identification number issued by
18 the government that is commonly used to verify identity; [(C)] (v) credit
19 or debit card number; [or (D)] (vi) financial account number in

20 combination with any required security code, access code or password
21 that would permit access to such financial account; (vii) medical
22 information regarding an individual's medical history, mental or
23 physical condition, or medical treatment or diagnosis by a health care
24 professional; (viii) health insurance policy number or subscriber
25 identification number, or any unique identifier used by a health insurer
26 to identify the individual; or (ix) biometric information consisting of
27 data generated by electronic measurements of an individual's unique
28 physical characteristics used to authenticate or ascertain the individual's
29 identity, such as a fingerprint, voice print, retina or iris image; or (B)
30 user name or electronic mail address, in combination with a password
31 or security question and answer that would permit access to an online
32 account. "Personal information" does not include publicly available
33 information that is lawfully made available to the general public from
34 federal, state or local government records or widely distributed media.

35 (b) (1) Any person who [conducts business in this state, and who, in
36 the ordinary course of such person's business,] owns, licenses or
37 maintains computerized data that includes personal information, shall
38 provide notice of any breach of security following the discovery of the
39 breach to any resident of this state whose personal information was
40 breached or is reasonably believed to have been breached. Such notice
41 shall be made without unreasonable delay but not later than [ninety]
42 sixty days after the discovery of such breach, unless a shorter time is
43 required under federal law, subject to the provisions of subsection (d) of
44 this section, [and the completion of an investigation by such person to
45 determine the nature and scope of the incident, to identify the
46 individuals affected, or to restore the reasonable integrity of the data
47 system.] If the person identifies additional residents of this state whose
48 personal information was breached or reasonably believed to have been
49 breached following sixty days after the discovery of such breach, the
50 person shall proceed in good faith to notify such additional residents as
51 expediently as possible. Such notification shall not be required if, after
52 an appropriate investigation [and consultation with relevant federal,
53 state and local agencies responsible for law enforcement,] the person

54 reasonably determines that the breach will not likely result in harm to
55 the individuals whose personal information has been acquired [and] or
56 accessed.

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

59 (A) The person who [conducts business in this state, and who, in the
60 ordinary course of such person's business,] owns, licenses or maintains
61 computerized data that includes personal information, shall, not later
62 than the time when notice is provided to the resident, also provide
63 notice of the breach of security to the Attorney General; and

64 (B) The person who [conducts business in this state, and who, in the
65 ordinary course of such person's business,] owns or licenses
66 computerized data that includes personal information, shall offer to
67 each resident whose personal information under [subparagraph (B)(i) of
68 subdivision (9) of subsection (b) of section 38a-38 or personal
69 information as defined in] clause (i) or (ii) of subparagraph (A) of
70 subdivision (2) 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 for
74 a period of not less than twenty-four months. Such person shall provide
75 all 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 maintains computerized data that includes
79 personal information that the person does not own shall notify the
80 owner or licensee of the information of any breach of the security of the
81 data immediately following its discovery, if the personal information of
82 a resident of this state was breached or is reasonably believed to have
83 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 notification be delayed.
88 Any such delayed notification shall be made after such law enforcement
89 agency determines that notification will not compromise the criminal
90 investigation and so notifies the person of such determination.

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

107 (f) (1) In the event of a breach of login credentials under
108 subparagraph (B) of subdivision (2) of subsection (a) of this section,
109 notice to a resident may be provided in electronic or other form that
110 directs the resident whose personal information was breached or is
111 reasonably believed to have been breached to promptly change any
112 password or security questions and answer, as applicable, or to take
113 other appropriate steps to protect the affected online account and all
114 other online accounts for which the resident uses the same user name or
115 electronic mail address and password or security question and answer.

116 (2) Any person that furnishes an electronic mail account shall not

117 comply with this section by providing notification to the electronic mail
118 account that was breached or reasonably believed to have been
119 breached if the person cannot reasonably verify the affected resident's
120 receipt of such notification. In such an event, the person shall provide
121 notice by another method described in this section or by clear and
122 conspicuous notice delivered to the resident online when the resident is
123 connected to the online account from an Internet protocol address or
124 online location from which the person knows the resident customarily
125 accesses the account.

126 [(f)] (g) Any person that maintains such person's own security breach
127 procedures as part of an information security policy for the treatment of
128 personal information and otherwise complies with the timing
129 requirements of this section, shall be deemed to be in compliance with
130 the security breach notification requirements of this section, provided
131 such person notifies, as applicable, residents of this state, owners and
132 licensees in accordance with such person's policies in the event of a
133 breach of security and in the case of notice to a resident, such person
134 also notifies the Attorney General not later than the time when notice is
135 provided to the resident. Any person that maintains such a security
136 breach procedure pursuant to the rules, regulations, procedures or
137 guidelines established by the primary or functional regulator, as defined
138 in 15 USC 6809(2), shall be deemed to be in compliance with the security
139 breach notification requirements of this section, provided (1) such
140 person notifies, as applicable, such residents of this state, owners, and
141 licensees required to be notified under and in accordance with the
142 policies or the rules, regulations, procedures or guidelines established
143 by the primary or functional regulator in the event of a breach of
144 security, and (2) if notice is given to a resident of this state in accordance
145 with subdivision (1) of this subsection regarding a breach of security,
146 such person also notifies the Attorney General not later than the time
147 when notice is provided to the resident.

148 (h) Any person that is subject to and in compliance with the privacy
149 and security standards under the Health Insurance Portability and

150 Accountability Act of 1996 and the Health Information Technology for
151 Economic and Clinical Health Act ("HITECH") shall be deemed to be in
152 compliance with this section, provided that (1) any person required to
153 provide notification to Connecticut residents pursuant to HITECH shall
154 also provide notice to the Attorney General not later than the time when
155 notice is provided to such residents if notification to the Attorney
156 General would otherwise be required under subparagraph (A) of
157 subdivision (2) of subsection (b) of this section, and (2) the person
158 otherwise complies with the requirements of subparagraph (B) of
159 subdivision (2) of subsection (b) of this section.

160 (i) All documents, materials and information provided in response to
161 an investigative demand issued pursuant to subsection (c) of section 42-
162 110d in connection with the investigation of a breach of security as
163 defined by this section shall be exempt from public disclosure under
164 subsection (a) of section 1-210, provided the Attorney General may
165 make such documents, materials or information available to third
166 parties in furtherance of such investigation.

167 [(g)] (j) Failure to comply with the requirements of this section shall
168 constitute an unfair trade practice for purposes of section 42-110b and
169 shall be enforced by the Attorney General.

This act shall take effect as follows and shall amend the following sections:		
---	--	--

Section 1	October 1, 2021	36a-701b
-----------	-----------------	----------