



General Assembly

January Session, 2021

***Raised Bill No. 5310***

LCO No. 1361



Referred to Committee on GENERAL LAW

Introduced by:  
(GL)

***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3 repealed and the following is substituted in lieu thereof (*Effective October*  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; [(B)] (ii) individual  
14 taxpayer identification number; (iii) identity protection personal  
15 identification number issued by the Internal Revenue Service; (iv)  
16 driver's license number, [or] state identification card number, passport

17 number, military identification number or other identification number  
18 issued by the government that is 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 and used to authenticate or ascertain the  
29 individual's identity, such as a fingerprint, voice print, retina or iris  
30 image; and (B) user name or electronic mail address, in combination  
31 with a password or security question and answer that would permit  
32 access to an online account. "Personal information" does not include  
33 publicly available information that is lawfully made available to the  
34 general public from federal, state or local government records or widely  
35 distributed media.

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

51 completed within sixty days after the discovery of such breach, the  
52 person shall provide preliminary substitute notice, consistent with  
53 subparagraphs (A) to (C), inclusive, of subdivision (4) of subsection (e)  
54 of this section, and shall proceed in good faith to work to identify  
55 affected residents and provide direct notice as expeditiously was possible,  
56 consistent with subdivisions (1) to (3), inclusive, of subsection (e) of this  
57 section. Notification shall not be required if, after an appropriate  
58 investigation, [and consultation with relevant federal, state and local  
59 agencies responsible for law enforcement,] the person reasonably  
60 determines that the breach will not likely result in harm to the  
61 individuals whose personal information has been acquired [and] or  
62 accessed.

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

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

70 (B) The person who [conducts business in this state, and who, in the  
71 ordinary course of such person's business,] owns or licenses  
72 computerized data that includes personal information, shall offer to  
73 each resident whose [nonpublic] personal information under  
74 [subparagraph (B)(i) of subdivision (9) of subsection (b) of section 38a-  
75 38 or personal information as defined in subparagraph (A) of  
76 subdivision (2) of subsection (a)] clause (i) or (ii) of subparagraph (A) of  
77 subdivision (2) of subsection (a) of this section was breached or is  
78 reasonably believed to have been breached, appropriate identity theft  
79 prevention services and, if applicable, identity theft mitigation services.  
80 Such service or services shall be provided at no cost to such resident for  
81 a period of not less than twenty-four months. Such person shall provide  
82 all information necessary for such resident to enroll in such service or  
83 services and shall include information on how such resident can place a

84 credit freeze on such resident's credit file.

85 (c) Any person that maintains computerized data that includes  
86 personal information that the person does not own shall notify the  
87 owner or licensee of the information of any breach of the security of the  
88 data immediately following its discovery, if the personal information of  
89 a resident of this state was breached or is reasonably believed to have  
90 been breached.

91 (d) Any notification required by this section shall be delayed for a  
92 reasonable period of time if a law enforcement agency determines that  
93 the notification will impede a criminal investigation and such law  
94 enforcement agency has made a request that the notification be delayed.  
95 Any such delayed notification shall be made after such law enforcement  
96 agency determines that notification will not compromise the criminal  
97 investigation and so notifies the person of such determination.

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

114 (f) (1) In the event of a breach of login credentials under  
115 subparagraph (B) of subdivision (2) of subsection (a) of this section,

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

123 (2) Any person that furnishes an email account shall not comply with  
124 this section by providing notification to the email account that was  
125 breached or reasonably believed to have been breached. The person  
126 shall provide notice by another method described in this section or by  
127 clear and conspicuous notice delivered to the resident online when the  
128 resident is connected to the online account from an Internet Protocol  
129 address or online location from which the person knows the resident  
130 customarily access the account.

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

150 with subdivision (1) of this subsection regarding a breach of security,  
151 such person also notifies the Attorney General not later than the time  
152 when notice is provided to the resident.

153 (h) Any person that is subject to and in compliance with the privacy  
154 and security standards under the Health Insurance Portability and  
155 Accountability Act of 1996 and the Health Information Technology for  
156 Economic and Clinical Health Act shall be deemed to be in compliance  
157 with the provisions of this section, provided that (1) any person required  
158 to provide notification to residents of this state pursuant to the Health  
159 Information Technology for Economic and Clinical Health Act shall also  
160 provide notice to the Attorney General not later than the time when such  
161 notice is provided to such residents and (2) the person otherwise  
162 complies with the requirements of subparagraph (B) of subdivision (2)  
163 of subsection (b) of this section.

164 (i) All documents, materials and information provided in response to  
165 an investigative demand in connection with the investigation of a  
166 breach of security, as defined in subsection (a) of this section, shall be  
167 exempt from public disclosure under subsection (a) of section 1-210,  
168 provided that the Attorney General may make such documents,  
169 materials or information available to third parties in furtherance of such  
170 investigation.

171 ~~[(g)]~~ (j) Failure to comply with the requirements of this section shall  
172 constitute an unfair trade practice for purposes of section 42-110b and  
173 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

**Statement of Purpose:**

To expand the data privacy breach notification statute to protect consumers.

*[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.]*