

Representative Marc K. Roberts proposes the following substitute bill:

DATA PRIVACY AMENDMENTS

2020 GENERAL SESSION

STATE OF UTAH

Chief Sponsor: Marc K. Roberts

Senate Sponsor: Todd Weiler

LONG TITLE

General Description:

This bill creates affirmative defenses to certain causes of action arising out of a data breach.

Highlighted Provisions:

This bill:

- ▶ defines terms;
 - ▶ creates affirmative defenses to causes of action arising out a data breach involving personal information, restricted information, or both personal information and restricted information;
 - ▶ provides that an entity may not claim an affirmative defense if the entity had notice of a threat or hazard;
 - ▶ establishes the requirements for asserting an affirmative defense;
 - ▶ provides that the creation of an affirmative defense does not create a cause of action for failure to comply with the requirements for asserting the affirmative defense;
- and
- ▶ provides a severability clause.

Money Appropriated in this Bill:

None



26 **Other Special Clauses:**

27 None

28 **Utah Code Sections Affected:**

29 ENACTS:

30 **78B-4-701**, Utah Code Annotated 1953

31 **78B-4-702**, Utah Code Annotated 1953

32 **78B-4-703**, Utah Code Annotated 1953

33 **78B-4-704**, Utah Code Annotated 1953

34 **78B-4-705**, Utah Code Annotated 1953



36 *Be it enacted by the Legislature of the state of Utah:*

37 Section 1. Section **78B-4-701** is enacted to read:

38 **Part 7. Cybersecurity Affirmative Defense Act**

39 **78B-4-701. Definitions.**

40 As used in this part:

41 (1) (a) "Business" means:

42 (i) an association;

43 (ii) a corporation;

44 (iii) a limited liability company;

45 (iv) a limited liability partnership;

46 (v) a sole proprietorship;

47 (vi) another group, however organized and whether operating for profit or not for
48 profit; or

49 (vii) a parent or subsidiary of any of the entities described in Subsections (1)(a)(i)
50 through (vi).

51 (b) "Business" includes a financial institution organized, chartered, or holding a license
52 authorizing operation under the laws of this state, another state, or another country.

53 (2) "Covered entity" means a business that accesses, maintains, communicates, or
54 processes personal information or restricted information in or through one or more systems,
55 networks, or services located in or outside of this state.

56 (3) (a) "Data breach" means the unauthorized access to or acquisition of electronic data

57 that:

58 (i) compromises the security or confidentiality of personal information or restricted
59 information owned by or licensed to a covered entity; and

60 (ii) causes, is reasonably believed to have caused, or is reasonably believed will cause a
61 material risk of identity theft or other fraud to an individual or an individual's property.

62 (b) "Data breach" does not include:

63 (i) good faith acquisition of personal information or restricted information by the
64 covered entity's employee or agent for a purpose of the covered entity if the personal
65 information or restricted information is not used for an unlawful purpose or subjected to further
66 unauthorized disclosure; or

67 (ii) acquisition of personal information or restricted information pursuant to:

68 (A) a search warrant, subpoena, or other court order; or

69 (B) a subpoena, order, or duty of a federal or state agency.

70 (4) (a) "Data item" means:

71 (i) a social security number;

72 (ii) a driver license number or state identification number; or

73 (iii) a financial account number or credit or debit card number when combined with
74 any required security code, access code, or password that is necessary to permit access to an
75 individual's financial account.

76 (b) "Data item" does not include an item described in Subsection (4)(a) if the item is
77 encrypted, redacted, or altered by any method or technology that makes the item unreadable.

78 (5) "Encrypted" means transformed, using an algorithmic process, into a form that has
79 a low probability of assigning meaning without the use of a confidential process, access key, or
80 password.

81 (6) "Individual's name" means:

82 (a) the individual's first name and last name; or

83 (b) the individual's last name and the initial of the individual's first name.

84 (7) "PCI data security standard" means the Payment Card Industry Data Security
85 Standard.

86 (8) (a) "Personal information" means an individual's name when combined with one or
87 more data items.

88 (b) "Personal information" does not include publicly available information that is
89 lawfully made available to the general public from federal, state, or local records or any of the
90 following media that are widely distributed:

91 (i) a news, editorial, or advertising statement published in a bona fide newspaper,
92 journal, magazine, or broadcast over radio or television;

93 (ii) a gathering or furnishing of information or news by a bona fide reporter,
94 correspondent, or news bureau to news media described in Subsection (8)(b)(i);

95 (iii) a publication designed for and distributed to members of a bona fide association or
96 charitable or fraternal nonprofit corporation; or

97 (iv) any type of media that is substantially similar in nature to any item, entity, or
98 activity described in Subsections (8)(b)(i) through (iii).

99 (9) "Redact" means to alter or truncate a data item so that no more than the last four
100 digits of a social security number, driver license number, state identification number, financial
101 account number, or credit or debit card number is accessible.

102 (10) "Restricted information" means any information, other than personal information,
103 about an individual that:

104 (a) (i) alone, or in combination with other information, including personal information,
105 can be used to distinguish or trace the individual's identity; or

106 (ii) is linked or linkable to an individual;

107 (b) is not encrypted, redacted, or altered by a method or a technology that makes the
108 information unreadable; and

109 (c) if accessed or acquired without authority, is likely to result in a material risk of
110 identity theft or fraud to the individual or the individual's property.

111 Section 2. Section **78B-4-702** is enacted to read:

112 **78B-4-702. Affirmative defense for a data breach of cyber data.**

113 (1) A covered entity that creates, maintains, and complies with a written cybersecurity
114 program that meets the requirements of Subsection (5) and is in place at the time of a data
115 breach of the covered entity has an affirmative defense to a claim that:

116 (a) is brought under the laws of this state or in the courts of this state;

117 (b) alleges that the covered entity failed to implement reasonable information security
118 controls;

119 (c) alleges that the failure described in Subsection (1)(b) resulted in a data breach of
120 personal information; and

121 (d) does not allege a data breach of restricted information.

122 (2) A covered entity that creates, maintains, and complies with a written cybersecurity
123 program that meets the requirements of Subsection (6) and is in place at the time of a data
124 breach of the covered entity has an affirmative defense to a claim that:

125 (a) is brought under the laws of this state or in the courts of this state; and

126 (b) alleges that the covered entity failed to implement reasonable information security
127 controls that resulted in a data breach of personal information and restricted information.

128 (3) A covered entity has an affirmative defense to a claim that the covered entity failed
129 to appropriately respond to a data breach if:

130 (a) (i) for a data breach of personal information, the covered entity creates, maintains,
131 and complies with a written cybersecurity program that meets the requirements of Subsection
132 (5) and is in place at the time of the data breach; or

133 (ii) for a data breach of personal information and restricted information, the covered
134 entity creates, maintains, and complies with a written cybersecurity program that meets the
135 requirements of Subsection (6) and is in place at the time of the data breach; and

136 (b) the written cybersecurity program had protocols at the time of the data breach for
137 responding to a data breach that complied with the written cybersecurity program under
138 Subsection (3)(a) and the covered entity followed the protocols.

139 (4) A covered entity has an affirmative defense to a claim that the covered entity failed
140 to appropriately notify an individual whose personal information or restricted information was
141 compromised in a data breach if:

142 (a) (i) for a data breach of personal information, the covered entity creates, maintains,
143 and complies with a written cybersecurity program that meets the requirements of Subsection
144 (5) and is in place at the time of the data breach; or

145 (ii) for a data breach of personal information and restricted information, the covered
146 entity creates, maintains, and complies with a written cybersecurity program that meets the
147 requirements of Subsection (6) and is in place at the time of the data breach; and

148 (b) the written cybersecurity program had protocols at the time of the data breach for
149 notifying an individual about a data breach that complied with the requirements for a written

150 cybersecurity program under Subsection (4)(a) and the covered entity followed the protocols.

151 (5) A written cybersecurity program described in Subsections (1) and (2) shall contain
152 administrative, technical, and physical safeguards to protect personal information, including:

153 (a) being designed to:

154 (i) protect the security and confidentiality of personal information;

155 (ii) protect against any anticipated threat or hazard to the security or integrity of
156 personal information; and

157 (iii) protect against a data breach of personal information;

158 (b) conforming to an industry recognized cybersecurity framework as described in
159 Section 78B-4-703; and

160 (c) being of an appropriate scale and scope in light of the following factors:

161 (i) the size and complexity of the covered entity;

162 (ii) the nature and scope of the activities of the covered entity;

163 (iii) the sensitivity of the information to be protected;

164 (iv) the cost and availability of tools to improve information security and reduce
165 vulnerability; and

166 (v) the resources available to the covered entity.

167 (6) A written cybersecurity program described in Subsection (2) shall meet the
168 requirements described in Subsection (5), except that the requirements of Subsection (5) shall
169 apply to both personal information and restricted information.

170 (7) A covered entity may not claim an affirmative defense under Subsections (1), (2),
171 (3), or (4) if:

172 (a) the covered entity had actual notice of a threat or hazard to the security or integrity
173 of personal information or restricted information;

174 (b) the covered entity did not act in a reasonable amount of time to take known
175 remedial efforts to protect the information against the threat or hazard; and

176 (c) the threat or hazard resulted in the data breach.

177 Section 3. Section 78B-4-703 is enacted to read:

178 **78B-4-703. Components of a cybersecurity program eligible for an affirmative**
179 **defense.**

180 (1) Subject to Subsection (2), a covered entity's written cybersecurity program

181 conforms to an industry recognized cybersecurity framework if the written cybersecurity
182 program:

183 (a) is designed to protect the type of personal information and restricted information
184 obtained in the data breach;

185 (b) conforms to the current version of any of the following frameworks or publications,
186 or any combination of the following frameworks or publications:

187 (i) NIST special publication 800-171;

188 (ii) NIST special publications 800-53 and 800-53a;

189 (iii) the Federal Risk and Authorization Management Program Security Assessment
190 Framework;

191 (iv) the Center for Internet Security Critical Security Controls for Effective Cyber
192 Defense; or

193 (v) the International Organization for Standardization/International Electrotechnical
194 Commission 27000 Family - Information security management systems;

195 (c) for personal information or restricted information obtained in the data breach that is
196 regulated by the federal government or state government, complies with the requirements of the
197 regulation, including:

198 (i) the security requirements of the Health Insurance Portability and Accountability Act
199 of 1996, as described in 45 C.F.R. Part 164, Subpart C;

200 (ii) Title V of the Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, as amended;

201 (iii) the Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283;

202 (iv) the Health Information Technology for Economic and Clinical Health Act, as set
203 forth in 45 C.F.R. Part 164;

204 (v) Title 13, Chapter 44, Protection of Personal Information Act; or

205 (vi) any other applicable federal or state regulation; and

206 (d) for personal information or restricted information obtained in the data breach that is
207 the type of information intended to be protected by the PCI data security standard, complies
208 with the current version of the PCI data security standard.

209 (2) If an industry recognized cybersecurity framework described in Subsection (1) is
210 revised, a covered entity with a written cybersecurity program that relies upon that industry

211 recognized cybersecurity framework shall conform to the revised version of the framework in a

212 reasonable amount of time, taking into consideration the urgency of the revision in terms of:

213 (a) risks to the security of personal information or restricted information;

214 (b) the cost and effort of complying with the revised version; and

215 (c) any other relevant factor.

216 Section 4. Section **78B-4-704** is enacted to read:

217 **78B-4-704. No cause of action.**

218 This part does not create a private cause of action, including a class action, if a covered
219 entity fails to comply with a provision of this part.

220 Section 5. Section **78B-4-705** is enacted to read:

221 **78B-4-705. Severability clause.**

222 If any provision of this part, or the application of any provision of this part to any
223 person or circumstance, is held invalid, the remainder of this part shall be given effect without
224 the invalid provision or application.