

**DATA SECURITY AMENDMENTS**

2021 GENERAL SESSION

STATE OF UTAH

**Chief Sponsor: Walt Brooks**

Senate Sponsor: Wayne A. Harper

---

**LONG TITLE**

**General Description:**

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

**Highlighted Provisions:**

This bill:

- ▶ defines terms;
- ▶ creates affirmative defenses to causes of action arising out of a breach of system security;
- ▶ provides that a person may not claim an affirmative defense if the person had notice of a threat or hazard;
- ▶ establishes the requirements for asserting an affirmative defense for a breach of system security;
- ▶ 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;
- ▶ addresses a choice of law provision in an agreement; and
- ▶ provides a severability clause.

**Money Appropriated in this Bill:**

None

**Other Special Clauses:**

None

**Utah Code Sections Affected:**

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
- 35 [78B-4-706](#), Utah Code Annotated 1953



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

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

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

40 **78B-4-701. Definitions.**

41 As used in this part:

42 (1) "Breach of system security" means the same as that term is defined in Section  
43 13-44-102.

44 (2) "NIST" means the National Institute for Standards and Technology in the United  
45 States Department of Commerce.

46 (3) "PCI data security standard" means the Payment Card Industry Data Security  
47 Standard.

48 (4) (a) "Person" means:

49 (i) an individual;

50 (ii) an association;

51 (iii) a corporation;

52 (iv) a joint stock company;

53 (v) a partnership;

54 (vi) a business trust; or

55 (vii) any unincorporated organization.

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

58 (5) "Personal information" means the same as that term is defined in Section  
59 13-44-102.

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

61 **78B-4-702. Affirmative defense for a breach of system security.**

62 (1) A person that creates, maintains, and reasonably complies with a written  
63 cybersecurity program that meets the requirements of Subsection (4), and is in place at the time  
64 of a breach of system security of the person, has an affirmative defense to a claim that:

- 65 (a) is brought under the laws of this state or in the courts of this state; and
- 66 (b) alleges that the person failed to implement reasonable information security controls  
67 that resulted in the breach of system security.

68 (2) A person has an affirmative defense to a claim that the person failed to  
69 appropriately respond to a breach of system security if:

- 70 (a) the person creates, maintains, and reasonably complies with a written cybersecurity  
71 program that meets the requirements of Subsection (4) and is in place at the time of the breach  
72 of system security; and
- 73 (b) the written cybersecurity program had protocols at the time of the breach of system  
74 security for responding to a breach of system security that reasonably complied with the written  
75 cybersecurity program under Subsection (2)(a) and the person followed the protocols.

76 (3) A person has an affirmative defense to a claim that the person failed to  
77 appropriately notify an individual whose personal information was compromised in a breach of  
78 system security if:

- 79 (a) the person creates, maintains, and reasonably complies with a written cybersecurity  
80 program that meets the requirements of Subsection (4) and is in place at the time of the breach  
81 of system security; and
- 82 (b) the written cybersecurity program had protocols at the time of the breach of system  
83 security for notifying an individual about a breach of system security that reasonably complied  
84 with the requirements for a written cybersecurity program under Subsection (3)(a) and the  
85 person followed the protocols.

86 (4) A written cybersecurity program described in Subsections (1), (2), and (3) shall  
87 provide administrative, technical, and physical safeguards to protect personal information,  
88 including:

89 (a) being designed to:

90 (i) protect the security, confidentiality, and integrity of personal information;

91 (ii) protect against any anticipated threat or hazard to the security, confidentiality, or  
92 integrity of personal information; and

93 (iii) protect against a breach of system security;

94 (b) reasonably conforming to a recognized cybersecurity framework as described in  
95 Subsection 78B-4-703(1); and

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

97 (i) the size and complexity of the person;

98 (ii) the nature and scope of the activities of the person;

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

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

102 (v) the resources available to the person.

103 (5) (a) Subject to Subsection (5)(b), a person may not claim an affirmative defense  
104 under Subsection (1), (2), or (3) if:

105 (i) the person had actual notice of a threat or hazard to the security, confidentiality, or  
106 integrity of personal information;

107 (ii) the person did not act in a reasonable amount of time to take known remedial  
108 efforts to protect the personal information against the threat or hazard; and

109 (iii) the threat or hazard resulted in the breach of system security.

110 (b) A risk assessment to improve the security, confidentiality, or integrity of personal  
111 information is not an actual notice of a threat or hazard to the security, confidentiality, or  
112 integrity of personal information.

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

114 78B-4-703. Components of a cybersecurity program eligible for an affirmative  
115 defense.

116 (1) Subject to Subsection (3), a person's written cybersecurity program reasonably  
117 conforms to a recognized cybersecurity framework if the written cybersecurity program:

118 (a) is designed to protect the type of personal information obtained in the breach of  
119 system security; and

120 (b) (i) is a reasonable security program described in Subsection (2);

121 (ii) reasonably conforms to the current version of any of the following frameworks or  
122 publications, or any combination of the following frameworks or publications:

123 (A) NIST special publication 800-171;

124 (B) NIST special publications 800-53 and 800-53a;

125 (C) the Federal Risk and Authorization Management Program Security Assessment  
126 Framework;

127 (D) the Center for Internet Security Critical Security Controls for Effective Cyber  
128 Defense; or

129 (E) the International Organization for Standardization/International Electrotechnical  
130 Commission 27000 Family - Information security management systems;

131 (iii) for personal information obtained in the breach of the system security that is  
132 regulated by the federal government or state government, reasonably complies with the  
133 requirements of the regulation, including:

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

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

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

138 (D) the Health Information Technology for Economic and Clinical Health Act, as  
139 provided in 45 C.F.R. Part 164;

140 (E) Title 13, Chapter 44, Protection of Personal Information Act; or

141 (F) any other applicable federal or state regulation; or

142 (iv) for personal information obtained in the breach of system security that is the type  
143 of information intended to be protected by the PCI data security standard, reasonably complies  
144 with the current version of the PCI data security standard.

145 (2) A written cybersecurity program is a reasonable security program under Subsection  
146 (1)(b)(i) if:

147 (a) the person coordinates, or designates an employee of the person to coordinate, a  
148 program that provides the administrative, technical, and physical safeguards described in  
149 Subsections 78B-4-702(4)(a) and (c);

150 (b) the program under Subsection (2)(a) has practices and procedures to detect,  
151 prevent, and respond to a breach of system security;

152 (c) the person, or an employee of the person, trains, and manages employees in the  
153 practices and procedures under Subsection (2)(b);

154 (d) the person, or an employee of the person, conducts risk assessments to test and  
155 monitor the practice and procedures under Subsection (2)(b), including risk assessments on:

156 (i) the network and software design for the person;

157 (ii) information processing, transmission, and storage of personal information; and

158 (iii) the storage and disposal of personal information; and

159 (e) the person adjusts the practices and procedures under Subsection (2)(b) in light of  
160 changes or new circumstances needed to protect the security, confidentiality, and integrity of  
161 personal information.

162 (3) (a) If a recognized cybersecurity framework described in Subsection (1)(b)(ii) or  
163 (iv) is revised, a person with a written cybersecurity program that relies upon that recognized  
164 cybersecurity framework shall reasonably conform to the revised version of the framework no  
165 later than one year after the day in which the revised version of the framework is published.

166 (b) If a recognized cybersecurity framework described in Subsection (1)(b)(iii) is  
167 amended, a person with a written cybersecurity program that relies upon that recognized  
168 cybersecurity framework shall reasonably conform to the amended regulation of the framework  
169 in a reasonable amount of time, taking into consideration the urgency of the amendment in

170 terms of:

171 (i) risks to the security of personal information;

172 (ii) the cost and effort of complying with the amended regulation; and

173 (iii) any other relevant factor.

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

175 **78B-4-704. No cause of action.**

176 This part may not be construed to create a private cause of action, including a class  
177 action, if a person fails to comply with a provision of this part.

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

179 **78B-4-705. Choice of law.**

180 A choice of law provision in an agreement that designates this state as the governing  
181 law shall apply this part, if applicable, to the fullest extent possible in a civil action brought  
182 against a person regardless of whether the civil action is brought in this state or another state.

183 Section 6. Section **78B-4-706** is enacted to read:

184 **78B-4-706. Severability clause.**

185 If any provision of this part, or the application of any provision of this part to any  
186 person or circumstance, is held invalid, the remainder of this part shall be given effect without  
187 the invalid provision or application.