

**Representative Walt Brooks** proposes the following substitute bill:

**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



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

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 and confidentiality of personal information;

91 (ii) protect against any anticipated threat or hazard to the security or integrity of

92 personal information; and

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

94 (b) reasonably conforming to an industry recognized cybersecurity framework as

95 described in Section [78B-4-703](#); 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 or integrity of

106 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 of personal information is not an actual

111 notice of a threat or hazard to the security or integrity of personal information.

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

113 **78B-4-703. Components of a cybersecurity program eligible for an affirmative**

114 **defense.**

115 (1) Subject to Subsection (2), a person's written cybersecurity program reasonably

116 conforms to an industry recognized cybersecurity framework if the written cybersecurity

117 program:

118 (a) is designed to protect the type of personal information obtained in the breach of

119 system security; and  
120 (b) (i) reasonably conforms to the current version of any of the following frameworks  
121 or publications, or any combination of the following frameworks or publications:  
122 (A) the framework for improving critical infrastructure developed by NIST;  
123 (B) NIST special publication 800-171;  
124 (C) NIST special publications 800-53 and 800-53a;  
125 (D) the Federal Risk and Authorization Management Program Security Assessment  
126 Framework;  
127 (E) the Center for Internet Security Critical Security Controls for Effective Cyber  
128 Defense; or  
129 (F) the International Organization for Standardization/International Electrotechnical  
130 Commission 27000 Family - Information security management systems;  
131 (ii) 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 (iii) 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) If an industry recognized cybersecurity framework described in Subsection  
146 (1)(b)(i) or (ii) is revised, a person with a written cybersecurity program that relies upon that  
147 industry recognized cybersecurity framework shall reasonably conform to the revised version  
148 of the framework no later than one year after the day in which the revised version of the  
149 framework is published.

150 (b) If an industry recognized cybersecurity framework described in Subsection  
151 (1)(b)(ii) is amended, a person with a written cybersecurity program that relies upon that  
152 industry recognized cybersecurity framework shall reasonably conform to the amended  
153 regulation of the framework in a reasonable amount of time, taking into consideration the  
154 urgency of the amendment in terms of:

- 155 (i) risks to the security of personal information;
- 156 (ii) the cost and effort of complying with the amended regulation; and
- 157 (iii) any other relevant factor.

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

159 **78B-4-704. No cause of action.**

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

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

163 **78B-4-705. Choice of law.**

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

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

168 **78B-4-706. Severability clause.**

169 If any provision of this part, or the application of any provision of this part to any  
170 person or circumstance, is held invalid, the remainder of this part shall be given effect without  
171 the invalid provision or application.