HB0080S01 compared with HB0080

~~{deleted text}~~ shows text that was in HB0080 but was deleted in HB0080S01.

inserted text shows text that was not in HB0080 but was inserted into HB0080S01.

DISCLAIMER: This document is provided to assist you in your comparison of the two bills. Sometimes this automated comparison will NOT be completely accurate. Therefore, you need to read the actual bills. This automatically generated document could contain inaccuracies caused by: limitations of the compare program; bad input data; or other causes.

Representative Walt Brooks proposes the following substitute bill:

DATA SECURITY AMENDMENTS

2021 GENERAL SESSION

STATE OF UTAH

Chief Sponsor: Walt Brooks

Senate Sponsor: ____________

LONG TITLE

General Description:

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

Highlighted Provisions:

This bill:

- defines terms;
- creates affirmative defenses to causes of action arising out of a ~~{data }~~breach ~~{involving personal information, restricted information, or both personal information and restricted information}~~of system security;
- provides that ~~{an entity}~~a person may not claim an affirmative defense if the ~~{entity}~~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:

78B-4-701, Utah Code Annotated 1953

78B-4-702, Utah Code Annotated 1953

78B-4-703, Utah Code Annotated 1953

78B-4-704, Utah Code Annotated 1953

78B-4-705, Utah Code Annotated 1953

78B-4-706, Utah Code Annotated 1953

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

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

Part 7. Cybersecurity Affirmative Defense Act

78B-4-701. Definitions.

As used in this part:

(1) ~~{(a) "Business" means:~~

~~(i) an association;~~

~~(ii) a corporation;~~

~~(iii) a limited liability company;~~

~~(iv) a limited liability partnership;~~

~~(v) a sole proprietorship;~~

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

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

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

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

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

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

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

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

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

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

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

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

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

~~(i) a social security number;~~

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

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

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

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

~~password.~~

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

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

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

~~(7)}~~ "Breach of system security" means the same as that term is defined in Section 13-44-102.

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

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

(~~{8) (a}~~4) (a) "Person" means:

(i) an individual;

(ii) an association;

(iii) a corporation;

(iv) a joint stock company;

(v) a partnership;

(vi) a business trust; or

(vii) any unincorporated organization.

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

(5) "Personal information" means ~~{an individual's name when combined with one or more data items.~~

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

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

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

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

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

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

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

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

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

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

~~(c) if accessed or acquired without authority, is likely to result in a material risk of identity theft or fraud to the individual or the individual's property}~~the same as that term is defined in Section 13-44-102.

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

78B-4-702. Affirmative defense for a ~~{data }~~breach of ~~{cyber data}~~system security.

(1) A ~~{covered entity}~~person that creates, maintains, and reasonably complies with a written cybersecurity program that meets the requirements of Subsection (~~{5}~~4), and is in place at the time of a ~~{data }~~breach of system security of the ~~{covered entity}~~person, has an affirmative defense to a claim that:

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

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

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

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

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

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

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

~~(3) A covered entity}~~the breach of system security.

(2) A person has an affirmative defense to a claim that the ~~{covered entity}~~person failed to appropriately respond to a ~~{data }~~breach~~{ if:~~

~~(a) (i) for a data breach of personal information, the covered entity}~~ of system security if:

(a) the person creates, maintains, and reasonably complies with a written cybersecurity program that meets the requirements of Subsection (~~{5}~~4) and is in place at the time of the ~~{data breach; or~~

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

(b) the written cybersecurity program had protocols at the time of the ~~{data }~~breach of system security for responding to a ~~{data }~~breach of system security that reasonably complied with the written cybersecurity program under Subsection (~~{3}~~2)(a) and the ~~{covered entity}~~person followed the protocols.

(~~{4}~~3) A ~~{covered entity}~~person has an affirmative defense to a claim that the ~~{covered entity}~~person failed to appropriately notify an individual whose personal information ~~{or restricted information }~~was compromised in a ~~{data }~~breach~~{ if:~~

~~(a) (i) for a data breach of personal information, the covered entity}~~ of system security if:

(a) the person creates, maintains, and reasonably complies with a written cybersecurity program that meets the requirements of Subsection (~~{5}~~4) and is in place at the time of the ~~{data breach; or~~

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

(b) the written cybersecurity program had protocols at the time of the ~~{data }~~breach of system security for notifying an individual about a ~~{data }~~breach of system security that reasonably complied with the requirements for a written cybersecurity program under Subsection (~~{4}~~3)(a) and the ~~{covered entity}~~person followed the protocols.

(~~{5}~~4) A written cybersecurity program described in Subsections (1), (2), and (~~{2}~~3) shall ~~{contain}~~provide administrative, technical, and physical safeguards to protect personal information, including:

(a) being designed to:

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

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

(iii) protect against a ~~{data }~~breach of ~~{personal information}~~system security;

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

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

(i) the size and complexity of the ~~{covered entity}~~person;

(ii) the nature and scope of the activities of the ~~{covered entity}~~person;

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

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

(v) the resources available to the ~~{covered entity.~~

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

~~(7) A covered entity}~~person.

(5) (a) Subject to Subsection (5)(b), a person may not claim an affirmative defense under Subsection (1), (2), ~~{(3), }~~or (~~{4}~~3) if:

(~~{a}~~i) the ~~{covered entity}~~person had actual notice of a threat or hazard to the security or integrity of personal~~{ information or restricted}~~ information;

(~~{b}~~ii) the ~~{covered entity}~~person did not act in a reasonable amount of time to take known remedial efforts to protect the personal information against the threat or hazard; and

(~~{c}~~iii) the threat or hazard resulted in the ~~{data }~~breach of system security.

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

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

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

(1) Subject to Subsection (2), a ~~{covered entity's}~~person's written cybersecurity program reasonably conforms to an industry recognized cybersecurity framework if the written cybersecurity program:

(a) is designed to protect the type of personal information ~~{and restricted information }~~obtained in the ~~{data }~~breach of system security; and

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

(A) the framework for improving critical infrastructure developed by NIST;

(~~{i}~~B) NIST special publication 800-171;

(~~{ii}~~C) NIST special publications 800-53 and 800-53a;

(~~{iii}~~D) the Federal Risk and Authorization Management Program Security Assessment Framework;

(~~{iv}~~E) the Center for Internet Security Critical Security Controls for Effective Cyber Defense; or

(~~{v}~~F) the International Organization for Standardization/International Electrotechnical Commission 27000 Family - Information security management systems;

(~~{c}~~ii) for personal information ~~{or restricted information }~~obtained in the ~~{data }~~breach of the system security that is regulated by the federal government or state government, reasonably complies with the requirements of the regulation, including:

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

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

(~~{iii}~~C) the Federal Information Security Modernization Act of 2014, Pub. L. No.

113-283;

(~~{iv}~~D) the Health Information Technology for Economic and Clinical Health Act, as ~~{set forth}~~provided in 45 C.F.R. Part 164;

(~~{v}~~E) Title 13, Chapter 44, Protection of Personal Information Act; or

(~~{vi}~~F) any other applicable federal or state regulation; ~~{and}~~or

(~~{d}~~iii) for personal information ~~{or restricted information }~~obtained in the ~~{data }~~breach of system security that is the type of information intended to be protected by the PCI data security standard, reasonably complies with the current version of the PCI data security standard.

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

(~~{2}~~b) If an industry recognized cybersecurity framework described in Subsection (1)(b)(ii) is ~~{revised}~~amended, a ~~{covered entity}~~person with a written cybersecurity program that relies upon that industry recognized cybersecurity framework shall reasonably conform to the ~~{revised version}~~amended regulation of the framework in a reasonable amount of time, taking into consideration the urgency of the ~~{revision}~~amendment in terms of:

(~~{a}~~i) risks to the security of personal~~{ information or restricted}~~ information;

(~~{b}~~ii) the cost and effort of complying with the ~~{revised version}~~amended regulation; and

(~~{c}~~iii) any other relevant factor.

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

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

This part ~~{does}~~may not be construed to create a private cause of action, including a class action, if a ~~{covered entity}~~person fails to comply with a provision of this part.

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

78B-4-705. Choice of law.

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

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

~~{78B-4-705}~~78B-4-706. Severability clause.

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