LEGISLATIVE GENERAL COUNSEL
₵ Approved for Filing: J. Carlton ₵
₵ 12-30-20 12:16 PM ₵

H.B. 80

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.

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;
- 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

Other Special Clauses:

None

H.B. 80

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

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

(8) (a) "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.

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

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

(1) A covered entity that creates, maintains, and complies with a written cybersecurity program that meets the requirements of Subsection (5) 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;

(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 failed to implement reasonable information security controls that resulted in a data breach of personal information and restricted information.

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

(a) (i) for a data breach of personal information, the covered entity creates, maintains, and complies with a written cybersecurity program that meets the requirements of Subsection (5) 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; and

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

(4) A covered entity has an affirmative defense to a claim that the covered entity 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 creates, maintains, and complies with a written cybersecurity program that meets the requirements of Subsection (5) 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; and

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

(5) A written cybersecurity program described in Subsections (1) and (2) shall contain

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;

(b) 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;

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

(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 may not claim an affirmative defense under Subsection (1), (2), (3), or (4) if:

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

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

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

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 written cybersecurity program 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;

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

(i) NIST special publication 800-171;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(c) any other relevant factor.

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

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

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

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

78B-4-705. 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.