Senate Study Bill 1095 - Introduced

SENATE FILE _____
BY (PROPOSED COMMITTEE
ON TECHNOLOGY BILL BY
CHAIRPERSON COURNOYER)

A BILL FOR

An Act relating to affirmative defenses for entities using cybersecurity programs and electronic transactions recorded by blockchain technology.

BE IT ENACTED BY THE GENERAL ASSEMBLY OF THE STATE OF IOWA:

Section 1. Section 554D.103, subsections 7, 8, and 15, Code 2023, are amended to read as follows:

7. "*Electronic record*" means a record created, generated, sent, communicated, received, or stored by electronic means. "*Electronic record*" includes any record or contract secured through distributed ledger technology or blockchain technology.

8. "*Electronic signature*" means an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record. "*Electronic signature*" includes a signature that is secured through distributed ledger technology or blockchain technology.

15. "*State*" means a state of the United States, the District of Columbia, Puerto Rico, the United States Virgin Islands, or any territory or insular possession subject to the jurisdiction of the United States. "*State*" includes an Indian tribe or band, or Alaskan ~~native~~ Native village, which is recognized by federal law or formally acknowledged by a state.

Sec. 2. NEW SECTION. **554G.1 Definitions.**

As used in this chapter:

1. "*Business*" means any limited liability company, limited liability partnership, corporation, sole proprietorship, association, or other group, however organized and whether operating for profit or not for profit, including a financial institution organized, chartered, or holding a license authorizing operation under the laws of this state, any other state, the United States, or any other country, or the parent or subsidiary of any of the foregoing.

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 this state.

3. "*Data breach*" means unauthorized access to and acquisition of computerized data that compromises the security or confidentiality of personal information or restricted

information owned by or licensed to a covered entity and that causes, reasonably is believed to have caused, or reasonably is believed will cause a material risk of identity theft or other fraud to person or property. *"Data breach"* does not include any of the following:

a. Good-faith acquisition of personal information or restricted information by the covered entity's employee or agent for the purposes of the covered entity, provided that the personal information or restricted information is not used for an unlawful purpose or subject to further unauthorized disclosure.

b. Acquisition of personal information or restricted information pursuant to a search warrant, subpoena, or other court order, or pursuant to a subpoena, order, or duty of a regulatory state agency.

4. *"Encrypted"* means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

5. *"Individual"* means a natural person.

6. *a. "Personal information"* means an individual's name, consisting of the individual's first name or first initial and last name, in combination with and linked to any one or more of the following data elements, when the data elements are not encrypted, redacted, or altered by any method or technology in such a manner that the data elements are unreadable:

(1) Social security number.

(2) Driver's license number or state identification card number.

(3) Account number or credit or debit card number, in combination with and linked to any required security code, access code, or password that would permit access to an individual's financial account.

b. "Personal information" does not include publicly available information that is lawfully made available to the

general public from federal, state, or local government records or any of the following media that are widely distributed:

(1) Any news, editorial, or advertising statement published in any bona fide newspaper, journal, or magazine, or broadcast over radio or television.

(2) Any gathering or furnishing of information or news by any bona fide reporter, correspondent, or news bureau to news media identified in this paragraph.

(3) Any publication designed for and distributed to members of any bona fide association or charitable or fraternal nonprofit corporation.

(4) Any type of media similar in nature to any item, entity, or activity identified in this paragraph.

7. *"Redacted"* means altered or truncated so that no more than the last four digits of a social security number, driver's license number, state identification card number, account number, or credit or debit card number is accessible as part of the data.

8. *"Restricted information"* means any information about an individual, other than personal information, that, alone or in combination with other information, including personal information, can be used to distinguish or trace the individual's identity or that is linked or linkable to an individual, if the information is not encrypted, redacted, or altered by any method or technology in such a manner that the information is unreadable, and the breach of which is likely to result in a material risk of identity theft or other fraud to person or property.

Sec. 3. NEW SECTION. **554G.2 Affirmative defenses.**

1. A covered entity seeking an affirmative defense under this chapter shall do one of the following:

a. Create, maintain, and comply with a written cybersecurity program that contains administrative, technical, and physical safeguards for the protection of personal information and that reasonably conforms to an industry-recognized cybersecurity

framework, as described in section 554G.3.

b. Create, maintain, and comply with a written cybersecurity program that contains administrative, technical, and physical safeguards for the protection of both personal information and restricted information and that reasonably conforms to an industry-recognized cybersecurity framework, as described in section 554G.3.

2. A covered entity's cybersecurity program shall be designed to do all of the following with respect to the information described in subsection 1, paragraph *"a"* or *"b"*, as applicable:

a. Protect the security and confidentiality of the information.

b. Protect against any anticipated threats or hazards to the security or integrity of the information.

c. Protect against unauthorized access to and acquisition of the information that is likely to result in a material risk of identity theft or other fraud to the individual to whom the information relates.

3. The scale and scope of a covered entity's cybersecurity program under subsection 1, paragraph *"a"* or *"b"*, as applicable, is appropriate if the cybersecurity program is based on all of the following factors:

a. The size and complexity of the covered entity.

b. The nature and scope of the activities of the covered entity.

c. The sensitivity of the information to be protected.

d. The cost and availability of tools to improve information security and reduce vulnerabilities.

e. The resources available to the covered entity.

4. *a.* A covered entity that satisfies subsection 1, paragraph *"a"*, and subsections 2 and 3, is entitled to an affirmative defense to any cause of action sounding in tort that is brought under the laws of this state or in the courts of this state and that alleges that the failure to implement

reasonable information security controls resulted in a data breach concerning personal information.

b. A covered entity that satisfies subsection 1, paragraph "*b*", and subsections 2 and 3, is entitled to an affirmative defense to any cause of action sounding in tort that is brought under the laws of this state or in the courts of this state and that alleges that the failure to implement reasonable information security controls resulted in a data breach concerning personal information or restricted information.

Sec. 4. NEW SECTION. **554G.3 Cybersecurity program framework.**

1. A covered entity's cybersecurity program, as described in section 554G.2, reasonably conforms to an industry-recognized cybersecurity framework for purposes of section 554G.2 if any of the following are true:

a. (1) The cybersecurity program reasonably conforms to the current version of any of the following or any combination of the following, subject to subparagraph (2) and subsection 2:

(a) The framework for improving critical infrastructure cybersecurity developed by the national institute of standards and technology.

(b) National institute of standards and technology special publication 800-171.

(c) National institute of standards and technology special publications 800-53 and 800-53a.

(d) The federal risk and authorization management program security assessment framework.

(e) The center for internet security critical security controls for effective cyber defense.

(f) The international organization for standardization/international electrotechnical commission 27000 family — information security management systems.

(2) When a final revision to a framework listed in subparagraph (1) is published, a covered entity whose cybersecurity program reasonably conforms to that framework

shall reasonably conform to the revised framework not later than one year after the publication date stated in the revision.

b. (1) The covered entity is regulated by the state, by the federal government, or both, or is otherwise subject to the requirements of any of the laws or regulations listed below, and the cybersecurity program reasonably conforms to the entirety of the current version of any of the following, subject to subparagraph (2):

(a) The security requirements of the federal Health Insurance Portability and Accountability Act of 1996, as set forth in 45 C.F.R. pt. 164, subpt. C.

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

(c) The federal Information Security Modernization Act of 2014, Pub. L. No. 113-283.

(d) The federal Health Information Technology for Economic and Clinical Health Act as set forth in 45 C.F.R. pt. 162.

(2) When a framework listed in subparagraph (1) is amended, a covered entity whose cybersecurity program reasonably conforms to that framework shall reasonably conform to the amended framework not later than one year after the effective date of the amended framework.

c. (1) The cybersecurity program reasonably complies with both the current version of the payment card industry data security standard and conforms to the current version of another applicable industry-recognized cybersecurity framework listed in paragraph *"a"*, subject to subparagraph (2) and subsection 2.

(2) When a final revision to the payment card industry data security standard is published, a covered entity whose cybersecurity program reasonably complies with that standard shall reasonably comply with the revised standard not later than one year after the publication date stated in the revision.

2. If a covered entity's cybersecurity program reasonably conforms to a combination of industry-recognized cybersecurity frameworks, or complies with a standard, as in the case of the payment card industry data security standard, as described in subsection 1, paragraph "a" or "c", and two or more of those frameworks are revised, the covered entity whose cybersecurity program reasonably conforms to or complies with, as applicable, those frameworks shall reasonably conform to or comply with, as applicable, all of the revised frameworks not later than one year after the latest publication date stated in the revisions.

Sec. 5. NEW SECTION. **554G.4 Causes of actions.**

This chapter shall not be construed to provide a private right of action, including a class action, with respect to any act or practice regulated under those sections.

EXPLANATION

The inclusion of this explanation does not constitute agreement with the explanation's substance by the members of the general assembly.

This bill relates to cybersecurity programs and blockchain technology. The bill changes the definitions of "electronic record" and "electronic signature" in the uniform electronic transactions Act to include blockchain technology.

The bill creates affirmative defenses for entities using cybersecurity programs and provides definitions. The bill provides that a covered entity seeking an affirmative defense must use a cybersecurity program for the protection of personal information or both personal information and restricted information and the cybersecurity program must reasonably conform to an industry-recognized cybersecurity framework. A cybersecurity program must protect the security and confidentiality of the information, protect against any anticipated threats to the information, and protect against unauthorized access to and acquisition of the information that is likely to result in a material risk of identity theft. A cybersecurity program scale and scope should be based upon the size and complexity of the covered entity, the nature

and scope of the covered entity's activities, sensitivity of the information, and the cost and availability of tools and resources to improve information security. A covered entity that satisfies the above requirements is entitled to an affirmative defense to a tort claim that alleges that the failure to implement reasonable information security controls resulted in a data breach concerning personal information or restricted information.

The bill provides industry-recognized cybersecurity frameworks that the covered entity should follow and reasonably comply to in order to qualify for the affirmative defense.

The bill does not provide a private right to action, including a class action.