House File 2302 - Introduced

HOUSE FILE 2302
BY COMMITTEE ON INFORMATION TECHNOLOGY

(SUCCESSOR TO HSB 555)

A BILL FOR

An Act relating to affirmative defenses for entities using cybersecurity programs.

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

Section 1. Section 554D.103, subsections 4, 5, 8, 9, and 16, Code 2022, are amended to read as follows:

4. "*Contract*" means the total legal obligation resulting from the parties' agreement as affected by this chapter and other applicable law. ~~"*Contract*" includes any contract secured through distributed ledger technology and a smart contract.~~

~~5. "*Distributed ledger technology*" means an electronic record of transactions or other data to which all of the following apply:~~

~~*a.* The electronic record is uniformly ordered.~~

~~*b.* The electronic record is redundantly maintained or processed by one or more computers or machines to guarantee the consistency or nonrepudiation of the recorded transactions or other data.~~

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

9. "*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.~~

~~16. "*Smart contract*" means an event-driven program or computerized transaction protocol that runs on a distributed, decentralized, shared, and replicated ledger that executes the terms of a contract. For purposes of this subsection, "*executes the terms of a contract*" may include taking custody over and instructing the transfer of assets.~~

Sec. 2. Section 554D.108, subsection 2, Code 2022, is amended to read as follows:

2. A contract shall not be denied legal effect or enforceability solely because an electronic record was used in its formation ~~or because the contract is a smart contract or contains a smart contract provision~~.

Sec. 3. NEW SECTION. **554E.1 Definitions.**

As used in this chapter:

1. *"Account"* means the same as defined in section 554.9102.

2. *"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.

3. *"Contract"* means the same as defined in section 554D.103.

4. *"Covered entity"* means a business that accesses, receives, stores, 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.

5. *"Data breach"* means an intentional or unintentional action that could result in electronic records owned, licensed to, or otherwise protected by a covered entity being viewed, copied, modified, transmitted, or destroyed in a manner that is reasonably believed to have or may cause material risk of identity theft, fraud, or other injury or damage 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 or disclosure 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.

6. *"Distributed ledger technology"* means an electronic

record of transactions or other data to which all of the following apply:

a. The electronic record is uniformly ordered.

b. The electronic record is redundantly maintained or processed by one or more computers or machines to guarantee the consistency or nonrepudiation of the recorded transactions or other data.

7. *"Electronic"* means the same as defined in section 554D.103.

8. *"Electronic record"* means the same as defined in section 554D.103.

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

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

11. *"Maximum probable loss"* means the greatest damage expectation that could reasonably occur from a data breach. For purposes of this subsection, *"damage expectation"* means the total value of possible damage multiplied by the probability that damage would occur.

12. *a. "Personal information"* means any information relating to an individual who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, social security number, driver's license number or state identification card number, passport number, account number or credit or debit card number, location data, biometric data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that individual.

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, television, or the internet.

(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 business.

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

13. *"Record"* means the same as defined in section 554D.103.

14. *"Redacted"* means altered, truncated, or anonymized so that, when applied to personal information, the data can no longer be attributed to a specific individual without the use of additional information.

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

16. *"Smart contract"* means an event-driven program or computerized transaction protocol that runs on a distributed, decentralized, shared, and replicated ledger that executes the terms of a contract. For purposes of this subsection, *"executes the terms of a contract"* may include taking custody over and instructing the transfer of assets.

17. *"Transaction"* means a sale, trade, exchange, transfer, payment, or conversion of virtual currency or other digital asset or any other property or any other action or set of

actions occurring between two or more persons relating to the conduct of business, commercial, or governmental affairs.

Sec. 4. NEW SECTION. **554E.2 Distributed ledger technology — ownership of information.**

1. A record shall not be denied legal effect or enforceability solely because the record is created, generated, sent, communicated, received, recorded, or stored by means of distributed ledger technology or a smart contract.

2. A signature shall not be denied legal effect or enforceability solely because the signature is created, generated, sent, communicated, received, recorded, or stored by means of distributed ledger technology or a smart contract.

3. A contract shall not be denied legal effect or enforceability solely for any of the following:

a. The contract is created, generated, sent, communicated, received, executed, signed, adopted, recorded, or stored by means of distributed ledger technology or a smart contract.

b. The contract contains a smart contract term.

c. An electronic record, distributed ledger technology, or smart contract was used in the contract's formation.

4. A person who, in engaging in or affecting interstate or foreign commerce, uses distributed ledger technology to secure information that the person owns or has the right to use retains the same rights of ownership or use with respect to such information as before the person secured the information using distributed ledger technology. This subsection does not apply to the use of distributed ledger technology to secure information in connection with a transaction to the extent that the terms of the transaction expressly provide for the transfer of rights of ownership or use with respect to such information.

Sec. 5. NEW SECTION. **554E.3 Affirmative defenses.**

1. A covered entity seeking an affirmative defense under this chapter shall create, maintain, and comply with a written cybersecurity program that contains administrative, technical, operational, and physical safeguards for the protection of both

personal information and restricted information.

2. A covered entity's cybersecurity program shall be designed to do all of the following:

a. Continually evaluate and mitigate any reasonably anticipated internal or external threats or hazards that could lead to a data breach.

b. Periodically evaluate no less than annually the maximum probable loss attainable from a data breach.

c. Communicate to any affected parties the extent of any risk posed and any actions the affected parties could take to reduce any damages if a data breach is known to have occurred.

3. The scale and scope of a covered entity's cybersecurity program is appropriate if the cost to operate the cybersecurity program is no less than the covered entity's most recently calculated maximum probable loss value.

4. *a.* A covered entity that satisfies all requirements of this section 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.

b. A covered entity satisfies all requirements of this section if its cybersecurity program reasonably conforms to an industry-recognized cybersecurity framework, as described in section 554E.4.

Sec. 6. NEW SECTION. **554E.4 Cybersecurity program framework.**

1. A covered entity's cybersecurity program, as described in section 554E.3, reasonably conforms to an industry-recognized cybersecurity framework for purposes of section 554E.3 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 the elements of its cybersecurity program to the revised framework within the time frame provided in the relevant framework upon which the covered entity intends to rely to support its affirmative defense, but in no event 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 the elements of its cybersecurity program to the amended framework within the time frame provided in the relevant framework upon which the covered entity intends to rely to support its affirmative defense, but in no event 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 the elements of its cybersecurity program with the revised standard within the time frame provided in the relevant framework upon which the covered entity intends to rely to support its affirmative defense, but in no event 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 the elements of its cybersecurity program to or comply with, as applicable, all of

the revised frameworks within the time frames provided in the relevant frameworks but in no event later than one year after the latest publication date stated in the revisions.

Sec. 7. NEW SECTION. **554E.5 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.

Sec. 8. REPEAL. Section 554D.106A, Code 2022, is repealed.

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, affirmative defenses, and distributed ledger technology.

The bill provides that a record or signature shall not be denied legal effect because it is created or stored by means of distributed ledger technology or smart contract, as those terms are defined in the bill. The bill provides in new Code section 554E.2 that the ownership of the secure information remains with the person who provided the signature, not the distributed ledger technology owner, and repeals a similar provision in Code section 554D.106A.

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 and restricted information and the cybersecurity program must reasonably conform to an industry-recognized cybersecurity framework. A cybersecurity program must continually evaluate and mitigate reasonably anticipated threats, periodically evaluate the maximum probable loss attainable from a data breach, and communicate to affected parties the risk posed and actions the affected parties could take to reduce damages if a data breach has occurred. The scale and scope of a cybersecurity program is appropriate if the cost to operate the program is no less than the covered

entity's maximum probable loss value. A covered entity that satisfies these requirements and that reasonably conforms to an industry-recognized cybersecurity framework 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 details industry-recognized cybersecurity frameworks that the covered entity may 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.