LEGISLATURE OF THE STATE OF IDAHO

Sixty-eighth Legislature First Regular Session - 2025

IN THE HOUSE OF REPRESENTATIVES

HOUSE BILL NO. 117

BY BUSINESS COMMITTEE

AN ACT

RELATING TO THE INSURANCE DATA SECURITY ACT; AMENDING TITLE 41, IDAHO CODE, BY THE ADDITION OF A NEW CHAPTER 67, TITLE 41, IDAHO CODE, TO PROVIDE A SHORT TITLE, TO DEFINE TERMS, TO PROVIDE THAT LICENSEES SHALL ESTABLISH INFORMATION SECURITY PROGRAMS, TO PROVIDE FOR AN INVESTIGATION OF A CYBERSECURITY EVENT, TO PROVIDE FOR NOTICE OF A CYBERSECURITY EVENT, TO PROVIDE FOR THE DIRECTOR'S POWER TO EXAMINE AND INVESTIGATE THE AFFAIRS OF A LICENSEE, TO PROVIDE FOR CONFIDENTIALITY AND SHARING OF DOCUMENTS, MATERIALS, AND OTHER INFORMATION, TO PROVIDE EXCEPTIONS, TO PROVIDE THAT THERE SHALL BE NO PRIVATE CAUSE OF ACTION FOR A VIOLATION, TO PROVIDE FOR PENALTIES, TO PROVIDE THAT STATE STANDARDS AND REQUIREMENTS SHALL BE EXCLUSIVE, TO PROVIDE RULEMAKING AUTHORITY, TO PROVIDE FOR CONSIDERATIONS WHEN ADMINISTERING, TO PROVIDE AN EFFECTIVE DATE, AND TO PROVIDE SEVERABILITY; AND DECLARING AN EMERGENCY AND PROVIDING AN EFFECTIVE DATE.

Be It Enacted by the Legislature of the State of Idaho:

SECTION 1. That Title 41, Idaho Code, be, and the same is hereby amended by the addition thereto of a NEW CHAPTER, to be known and designated as Chapter 67, Title 41, Idaho Code, and to read as follows:

CHAPTER 67

INSURANCE DATA SECURITY ACT

41-6701. SHORT TITLE. This chapter shall be known and may be cited as the "Insurance Data Security Act."

41-6702. DEFINITIONS. As used in this chapter:

(1) "Authorized individual" means an individual known to and screened by the licensee and determined to be necessary and appropriate to have access to the nonpublic information held by the licensee and its information systems.

(2) "Consumer" means an individual, including but not limited to applicants, policyholders, insureds, beneficiaries, claimants, and certificate holders, who is a resident of this state and whose nonpublic information is in a licensee's possession, custody, or control.

(3) "Cybersecurity event" means an event resulting in unauthorized access to, disruption of, or misuse of an information system or nonpublic information stored on such information system. The term "cybersecurity event" does not include:

(a) The unauthorized acquisition of encrypted nonpublic information if the encryption, process, or key is not also acquired, released, or used without authorization; or

(b) An event with regard to which the licensee has determined that the nonpublic information accessed by an unauthorized person has not been used or released and has been returned or destroyed.

(4) "Encrypted" means the transformation of data into a form that results in a low probability of assigning meaning without the use of a protective process or key.

(5) "Information security program" means the administrative, technical, and physical safeguards that a licensee uses to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle nonpublic information.

(6) "Information system" means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of electronic nonpublic information, as well as any specialized system such as industrial process controls systems, telephone switching and private branch exchange systems, and environmental control systems.

(7) "Licensee" means any person who is licensed, authorized to operate, or registered, or who is required to be licensed, authorized, or registered, pursuant to the insurance laws of this state but does not include a purchasing group or a risk retention group chartered and licensed in a state other than this state or a person acting as an assuming insurer domiciled in another state or jurisdiction.

(8) "Nonpublic information" means electronic information that is not publicly available information and is:

(a) Business-related information of a licensee, the tampering with which, or unauthorized disclosure, access, or use of which, would cause a material adverse impact to the business, operations, or security of the licensee;

(b) Any information concerning a consumer that because of name, number, or other identifier can be used to identify such consumer, in combination with any one (1) or more of the following data elements:

(i) Social security number;

(ii) Driver's license number or nondriver identification card number;

(iii) Financial account number or credit or debit card number;

(iv) Any security code, access code, or password that would permit access to a consumer's financial account; or

(v) Biometric records; or

(c) Any information or data, except age or gender, in any form or medium created by or derived from a health care provider or a consumer that identifies a particular consumer and that relates to:

(i) The past, present, or future physical, mental, or behavioral health or condition of any consumer or a member of the consumer's family;

(ii) The provision of health care to any consumer; or

(iii) Payment for the provision of health care to any consumer.

(9) "Person" has the same meaning as provided in section 41-104, Idaho Code.

(10)(a) "Publicly available information" means any information that a licensee has a reasonable basis to believe is lawfully made available to

the general public from: federal, state, or local government records; widely distributed media; or disclosures to the general public that are required to be made by federal, state, or local law.

(b) For the purposes of this subsection, a licensee has a reasonable basis to believe that information is lawfully made available to the general public if the licensee has taken steps to determine:

(i) That the information is of the type that is available to the general public; and

(ii) Whether a consumer can direct that the information not be made available to the general public and, if so, that such consumer has not done so.

(11) "State" means the state of Idaho or, when used in a context signifying a jurisdiction other than the state of Idaho, any state, district, territory, commonwealth, or possession of the United States of America.

(12) "Third-party service provider" means a person, not otherwise defined as a licensee, that contracts with a licensee to maintain, process, or store nonpublic information or otherwise is permitted access to nonpublic information through its provision of services to the licensee.

41-6703. INFORMATION SECURITY PROGRAM. (1) Commensurate with the size and complexity of the licensee, the nature and scope of the licensee's activities, including its use of third-party service providers, and the sensitivity of the nonpublic information used by the licensee or in the licensee's possession, custody, or control, each licensee must develop, implement, and maintain a comprehensive written information security program based on the licensee's risk assessment that contains administrative, technical, and physical safeguards for the protection of nonpublic information and the licensee's information system.

(2) A licensee must require that any of its third-party service providers implement appropriate administrative, technical, and physical measures to protect and secure the information systems and nonpublic information that are accessible to, or held by, a third-party service provider. Nonpublic information is not accessible to, or held by, a third-party service provider within the meaning of this section if it is encrypted and the associated protective process or key necessary to assign meaning to the nonpublic information is not within the possession of the third-party service provider.

(3) As part of its information security program, each licensee must establish a written incident response plan designed to promptly respond to, and recover from, any cybersecurity event that compromises the confidentiality, integrity, or availability of nonpublic information in its possession, the licensee's information systems, or the continuing functionality of any aspect of the licensee's business or operations.

(4) Each licensee must maintain all records supporting its information security program for a period of five (5) years. To the extent a licensee has identified areas that require material improvement, the licensee must document the identification and the remedial efforts planned and underway to address such areas.

41-6704. INVESTIGATION OF A CYBERSECURITY EVENT. (1) If a licensee learns that a cybersecurity event has or may have occurred, such licensee or third-party service provider designated to act on behalf of the licensee shall conduct a prompt investigation.

(2) During the investigation, the licensee or third-party service provider designated to act on behalf of the licensee shall, to the extent possible:

(a) Determine whether a cybersecurity event has occurred;

(b) Assess the nature and scope of the cybersecurity event;

(c) Identify any nonpublic information that may have been involved in the cybersecurity event; and

(d) Perform or oversee reasonable measures to restore the security of the information systems compromised in the cybersecurity event in order to prevent further unauthorized acquisition, release, or use of nonpublic information in the licensee's possession, custody, or control.

(3) If a licensee learns that a cybersecurity event has or may have occurred that impacted the licensee's nonpublic information in a system maintained by a third-party service provider, the licensee shall complete the steps provided in subsection (2) of this section or make reasonable efforts to confirm and document that the third-party service provider has completed such steps.

(4) A licensee shall maintain records concerning all cybersecurity events for a period of at least five (5) years from the date of the cybersecurity event.

41-6705. NOTICE OF A CYBERSECURITY EVENT. (1) Each licensee must notify the director as promptly, in the form and manner prescribed by the director, as reasonably practicable but not later than ten (10) business days after a determination that a cybersecurity event has occurred when either:

(a) This state is the licensee's state of domicile, in the case of an insurer, or this state is the licensee's home state, in the case of a producer, as those terms are defined in section 41-1003, Idaho Code, and the cybersecurity event has a reasonable likelihood of materially harming:

(i) Any consumer residing in this state; or

(ii) Any material part of the normal operations of the licensee; or

(b) The licensee reasonably believes that the nonpublic information involved is of two hundred fifty (250) or more consumers residing in this state and that the event is either:

(i) A cybersecurity event impacting the licensee of which notice is required to be provided to any government body, self-regulatory agency, or any other supervisory body pursuant to any state or federal law; or

(ii) A cybersecurity event that has a reasonable likelihood of materially harming:

1. Any consumer residing in this state; or

2. Any material part of the normal operations of the licensee.

(2) A licensee shall notify each consumer residing in this state without unreasonable delay after a determination that a cybersecurity event has occurred that is reasonably likely to result in material harm to that consumer. Except as provided in subsection (5) of this section, a licensee that determines a cybersecurity event has occurred affecting data owned or licensed by another licensee must provide a notice to the owner or licensor of the data affected by the cybersecurity event in place of the notification to affected consumers.

(a) The licensee shall provide a copy of the notice sent to consumers to the director.

(b) In determining whether a cybersecurity event is reasonably likely to result in material harm to consumers residing in this state pursuant to this subsection, a licensee shall act with the care an ordinarily prudent person in like position would exercise under similar circumstances.

(c) A licensee may delay providing notice without violating the provisions of this subsection if either:

(i) A delay is necessary in order for the licensee to take any measures necessary to determine the scope of the cybersecurity event and restore the reasonable integrity of the information system. However, the licensee must provide the notice required pursuant to this section without unreasonable delay after the licensee completes the measures necessary to determine the scope of the cybersecurity event and restore the reasonable integrity of the information system; or

(ii) A law enforcement agency determines and advises the licensee that providing a notice will impede a criminal or civil investigation or jeopardize homeland or national security. However, the licensee must provide the notice required pursuant to this section without unreasonable delay after the law enforcement agency determines that providing the notice will no longer impede the investigation or jeopardize homeland or national security.

(3) In the case of a cybersecurity event impacting a licensee's nonpublic information in a system maintained by a third-party service provider, of which the licensee has become aware, the licensee must treat such event as it would pursuant to subsection (1) of this section unless the third-party service provider provides the notice required pursuant to subsection (1) of this section to the director.

(a) The computation of the licensee's deadlines shall begin on the day after the third-party service provider notifies the licensee of the cybersecurity event or the licensee otherwise has actual knowledge of the cybersecurity event, whichever is sooner.

(b) Nothing in this chapter prevents or abrogates an agreement between a licensee and another licensee, a third-party service provider, or any other party to fulfill any of the investigation requirements imposed pursuant to section 41-6704, Idaho Code, or notice requirements imposed pursuant to this section.

(4) As to notice of cybersecurity events of reinsurers to insurers:

(a) In the case of a cybersecurity event involving nonpublic information that is used by or in the possession, custody, or control of a

licensee acting as an assuming insurer, including an assuming insurer domiciled in another state or jurisdiction, and such licensee does not have a direct contractual relationship with the affected consumers:

(i) The assuming insurer must notify its affected ceding insurers and the insurance director of its state or jurisdiction of domicile within ten (10) business days of making the determination that a cybersecurity event has occurred; and

(ii) The ceding insurers that have a direct contractual relationship with affected consumers must fulfill the consumer notification requirements imposed pursuant to subsection (2) of this section and any other notification requirements relating to a cybersecurity event imposed pursuant to this section.

(b) In the case of a cybersecurity event involving nonpublic information that is in the possession, custody, or control of a third-party service provider of a licensee that is an assuming insurer, including an assuming insurer domiciled in another state or jurisdiction:

(i) The assuming insurer must notify its affected ceding insurers and the insurance director of its state or jurisdiction of domicile within ten (10) business days of receiving notice from its third-party service provider that a cybersecurity event has occurred; and

(ii) The ceding insurers that have a direct contractual relationship with affected consumers must fulfill the consumer notification requirements imposed pursuant to subsection (3) of this section and any other notification requirements relating to a cybersecurity event imposed pursuant to this section.

(c) Any licensee acting as an assuming insurer shall not have any other notice obligations relating to a cybersecurity event or other data breach pursuant to this section.

(5) In the case of a cybersecurity event involving nonpublic information that is in the possession, custody, or control of a licensee that is an insurer or its third-party service provider for which a consumer accessed the insurer's services through an independent insurance producer, and for which consumer notice is required pursuant to subsection (2) of this section, the insurer must notify the producers of record of all affected consumers of the cybersecurity event in a reasonable manner and at a time reasonably concurrent with the time at which notice is provided to the affected consumers. The insurer is excused from this obligation for any producer or producer's representative who is not authorized by law or contract to sell, solicit, or negotiate on behalf of the insurer and in those instances in which the insurer does not have the current producer of record information for any individual consumer.

41-6706. DIRECTOR'S POWER TO EXAMINE AND INVESTIGATE. (1) The director shall have the power to examine and investigate the affairs of any licensee to determine whether the licensee has been or is engaged in any conduct in violation of the provisions of this chapter. This power is in addition to the powers of the director pursuant to chapter 2, title 41, Idaho Code. Any such investigation or examination shall be conducted pursuant to chapter 2, title 41, Idaho Code.

(2) If the director has reason to believe that a licensee has been or is engaged in conduct in this state that violates the provisions of this chapter, the director may take action that is necessary or appropriate to enforce the provisions of this chapter.

41-6707. CONFIDENTIALITY AND SHARING OF DOCUMENTS, MATERIALS, AND OTHER INFORMATION. (1) Any documents, materials, or other information in the control or possession of the department that are furnished by a licensee or an employee or agent thereof acting on behalf of a licensee pursuant to section 41-6703 or 41-6705, Idaho Code, or that are obtained by the director in an investigation or examination pursuant to section 41-6706, Idaho Code, are confidential by law and privileged, are not subject to the Idaho public records act, chapter 1, title 74, Idaho Code, are not subject to subpoena, and are not subject to discovery or admissible as evidence in any private civil action. However, the director is authorized to use the documents, materials, or other information in the furtherance of any regulatory or legal action brought as a part of the director's duties.

(2) Neither the director nor any person who received documents, materials, or other information while acting under the authority of the director is permitted or required to testify in any private civil action concerning any confidential documents, materials, or information subject to the provisions of subsection (1) of this section.

(3) In order to assist in the performance of the director's duties under this chapter, the director may:

(a) Share documents, materials, or other information, including the confidential and privileged documents, materials, or information subject to the provisions of subsection (1) of this section, excluding nonpublic information as defined in section 41-6702(8)(b) and (c), Idaho Code, with other state, federal, and international regulatory agencies, with the national association of insurance commissioners, its affiliates or subsidiaries, and with state, federal, and international law enforcement authorities, provided that the recipient agrees in writing to maintain the confidentiality and privileged status of the document, material, or other information;

(b) Receive documents, materials, or information, including otherwise confidential and privileged documents, materials, or information, from the national association of insurance commissioners, its affiliates or subsidiaries and from regulatory and law enforcement officials of other foreign or domestic jurisdictions and must maintain as confidential or privileged any document, material, or information received with notice or the understanding that it is confidential or privileged under the laws of the jurisdiction that is the source of the document, material, or information;

(c) Share documents, materials, or other information subject to the provisions of subsection (1) of this section, excluding nonpublic information as defined in section 41-6702(8)(b) and (c), Idaho Code, with a third-party consultant or vendor, provided the consultant agrees in writing to maintain the confidentiality and privileged status of the documents, materials, or other information; and

(d) Enter into agreements governing sharing and use of information consistent with the provisions of this subsection.

(4) No waiver of any applicable privilege or claim of confidentiality in the documents, materials, or information will occur as a result of disclosure to the director pursuant to this section or as a result of sharing as authorized pursuant to subsection (3) of this section. This includes all protections from disclosure granted by the provisions of subsection (1) of this section, including from disclosure pursuant to the Idaho public records act, by subpoena, and through discovery or being admissible in evidence in any private civil action.

(5) Nothing in this chapter prohibits the director from releasing final, adjudicated actions that are open to public inspection pursuant to the Idaho public records act or to a database or other clearinghouse service maintained by the national association of insurance commissioners or its affiliates or subsidiaries.

41-6708. EXCEPTIONS. (1) The following exceptions shall apply to this chapter:

(a) A licensee is exempt from the provisions of section 41-6703, Idaho Code, if:

(i) The licensee has fewer than fifty (50) employees who work at least thirty (30) hours per week for the licensee;

(ii) The licensee has less than five million dollars ($5,000,000) in gross annual revenue; or

(iii) The licensee has less than ten million dollars ($10,000,000) in year-end total assets.

(b) A licensee that is subject to the health insurance portability and accountability act of 1996 (HIPAA) and any amendments thereto, that has established and maintains a written information security program pursuant to any statutes, rules, regulations, procedures, or guidelines established under HIPAA, and that maintains nonpublic information in the same manner as protected health information will be considered to meet the requirements of this chapter except for the director notification requirements pursuant to section 41-6705(1), Idaho Code.

(c) An employee, agent, representative, or designee of a licensee who is also a licensee is exempt from the provisions of sections 41-6703, 41-6704, and 41-6705, Idaho Code, and need not develop its own information security program to the extent that the employee, agent, representative, or designee is covered by the information security program of the other licensee.

(d) A licensee that is a financial institution or affiliated with a financial institution as defined in 15 U.S.C. 6809 that maintains an information security program in compliance with the interagency guidelines establishing standards for safeguarding customer information as set forth pursuant to 15 U.S.C. 6801 and 6805, the Gramm-Leach-Bliley act, will be considered to meet the requirements of section 41-6703, Idaho Code, with respect to establishing an information security program, provided that the information security program includes the protection of nonpublic information and the licensee's information system, and provided that the licensee produces, upon request, docu-

mentation satisfactory to the director that independently validates the financial institution or affiliated financial institution's adoption of an information security program that satisfies the interagency guidelines.

(e) A licensee that is in compliance with another jurisdiction's mandated written insurance data security requirements that are at least as restrictive as this chapter will be considered to meet the requirements of section 41-6703, Idaho Code, with respect to establishing an information security program.

(2) In the event that a licensee ceases to qualify for an exception, such licensee has one hundred eighty (180) days to comply with the provisions of this chapter.

41-6709. NO PRIVATE CAUSE OF ACTION. The provisions of this chapter shall not create or imply a private cause of action for violation of its provisions or any rules promulgated pursuant to it.

41-6710. PENALTIES. In the case of a violation of the provisions of this chapter, a licensee may be subject to civil penalties in accordance with section 41-117, Idaho Code.

41-6711. EXCLUSIVE STATE STANDARDS AND REQUIREMENTS. Notwithstanding any other provision of law to the contrary, the provisions of this chapter and any rules adopted pursuant to this chapter constitute the exclusive state standards and requirements applicable to licensees regarding an information security program, cybersecurity events, the security of nonpublic information, data security, investigation of cybersecurity events, notice of cybersecurity events, and notification to the director of cybersecurity events. The requirements of sections 28-51-104 through 28-51-107, Idaho Code, shall not apply to a licensee.

41-6712. RULEMAKING AUTHORITY. The director may, subject to legislative approval, promulgate such rules as are necessary to carry out the provisions of this chapter.

41-6713. CONSIDERATIONS WHEN ADMINISTERING. The director shall consider the nature, scale, and complexity of licensees in administering the provisions of this chapter and adopting rules pursuant to this chapter.

41-6714. EFFECTIVE DATE. This chapter shall take effect on July 1, 2025, provided that a licensee has until July 1, 2026, to comply with the provisions of section 41-6703, Idaho Code.

41-6715. SEVERABILITY. If any provision of this chapter or the application thereof to any person or circumstance is for any reason held to be invalid, the remainder of the chapter and the application of such provision to other persons or circumstances will not be affected thereby.

SECTION 2. An emergency existing therefor, which emergency is hereby declared to exist, this act shall be in full force and effect on and after July 1, 2025.