LEGISLATURE OF THE STATE OF IDAHO

Sixty-sixth Legislature First Regular Session - 2021

IN THE HOUSE OF REPRESENTATIVES

HOUSE BILL NO. 147, As Amended

BY BUSINESS COMMITTEE

AN ACT

RELATING TO THE INSURANCE DATA SECURITY ACT; AMENDING TITLE 41, IDAHO CODE, BY THE ADDITION OF A NEW CHAPTER 66, TITLE 41, IDAHO CODE, TO PROVIDE A SHORT TITLE, TO DEFINE TERMS, TO ESTABLISH PROVISIONS REGARDING AN INFORMATION SECURITY PROGRAM, TO PROVIDE FOR INVESTIGATION OF A CYBERSECURITY EVENT, TO PROVIDE FOR NOTICE OF A CYBERSECURITY EVENT, TO PROVIDE THAT THE DIRECTOR OF THE DEPARTMENT OF INSURANCE WILL HAVE THE POWER TO EXAMINE AND INVESTIGATE CERTAIN MATTERS, TO PROVIDE FOR CONFIDENTIALITY AND SHARING OF DOCUMENTS, MATERIALS, AND OTHER INFORMATION, TO PROVIDE EXCEPTIONS, TO PROVIDE THAT THE CHAPTER DOES NOT CREATE A PRIVATE CAUSE OF ACTION, TO PROVIDE FOR PENALTIES, TO ESTABLISH PROVISIONS REGARDING EXCLUSIVE STATE STANDARDS AND REQUIREMENTS, TO PROVIDE RULEMAKING AUTHORITY, TO PROVIDE CONSIDERATIONS IN ADMINISTERING THE CHAPTER, TO ESTABLISH PROVISIONS REGARDING THE EFFECTIVE DATE OF THE CHAPTER, AND TO PROVIDE SEVERABILITY.

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 66, Title 41, Idaho Code, and to read as follows:

CHAPTER 66

INSURANCE DATA SECURITY ACT

41-6601. SHORT TITLE. This chapter shall be known and may be cited as the "Insurance Data Security Act."

41-6602. 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) "Department" has the same meaning as provided in section 41-105, Idaho Code.

(5) "Director" has the same meaning as provided in section 41-105, Idaho Code.

(6) "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.

(7) "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.

(8) "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.

(9) "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 that is acting as an assuming insurer domiciled in another state or jurisdiction.

(10) "Multifactor authentication" means authentication through verification of at least two (2) of the following types of authentication factors:

(a) Knowledge factors, such as a password;

(b) Possession factors, such as a token, badge, or mobile phone; or

(c) Inherence factors, such as a biometric characteristic.

(11) "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 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.

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

(13) "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. For the purposes of this definition, 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:

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

(b) 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.

(14) "Risk assessment" means the risk assessment that each licensee is required to conduct under section 41-6603, Idaho Code.

(15) "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.

(16) "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.

41-6603. 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 design its information security program to:

(a) Protect the security and confidentiality of nonpublic information and the security of the information system;

(b) Protect against reasonably foreseeable threats or hazards to the security or integrity of nonpublic information and the information system;

(c) Protect against unauthorized access to or use of nonpublic information and minimize the likelihood of harm to any consumer; and

(d) Define and periodically reevaluate a schedule for retention of nonpublic information and a mechanism for its destruction when no longer needed.

(3) The licensee must do all of the following:

(a) Designate one (1) or more employees, an affiliate, or an outside vendor to act on behalf of the licensee who is responsible for the information security program;

(b) Identify reasonably foreseeable internal or external threats that could result in unauthorized access, transmission, disclosure, misuse, alteration, or destruction of nonpublic information, including the security of information systems and nonpublic information that are accessible to, or held by, third-party service providers;

(c) Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the nonpublic information;

(d) Assess the sufficiency of policies, procedures, information systems, and other safeguards in place to manage these threats, including consideration of threats in each relevant area of the licensee's operations, including:

(i) Employee training and management;

(ii) Information systems, including network and software design, as well as information classification, governance, processing, storage, transmission, and disposal; and

(iii) Detecting, preventing, and responding to attacks, intrusions, or other systems failures; and

(e) Implement information safeguards to manage the threats identified in its ongoing assessment and assess the effectiveness of the safeguards' key controls, systems, and procedures.

(4) Based on its risk assessment, the licensee must do the following:

(a) Design its information security program to mitigate the identified risks, commensurate with the size and complexity 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;

(b) Determine which of the following security measures are appropriate and implement such security measures:

(i) Place access controls on information systems, including controls to authenticate and permit access only to authorized individuals to protect against the unauthorized acquisition of nonpublic information;

(ii) Identify and manage the data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes in accordance with their relative importance to business objectives and the organization's risk strategy;

(iii) Restrict physical access to nonpublic information to authorized individuals only;

(iv) Protect by encryption or other appropriate means all nonpublic information while being transmitted over an external network and all nonpublic information stored on a laptop computer or other portable computing or storage device or media;

(v) Adopt secure development practices for in-house-developed applications utilized by the licensee and procedures for evaluating, assessing, or testing the security of externally developed applications utilized by the licensee;

(vi) Modify the information system in accordance with the licensee's information security program;

(vii) Utilize effective controls, which may include multifactor authentication procedures for any employee or authorized individual accessing nonpublic information;

(viii) Regularly test and monitor systems and procedures to detect actual and attempted attacks on, or intrusions into, information systems;

(ix) Include audit trails within the information security program designed to detect and respond to cybersecurity events and designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the licensee;

(x) Implement measures to protect against destruction, loss, or damage of nonpublic information due to environmental hazards, such as fire and water damage or other catastrophes or technological failures; and

(xi) Develop, implement, and maintain procedures for the secure disposal of nonpublic information in any format;

(c) Include cybersecurity risks in the licensee's enterprise risk management process;

(d) Stay informed regarding emerging threats or vulnerabilities and utilize reasonable security measures when sharing information relative to the character of the sharing and the type of information shared; and

(e) Provide its personnel with cybersecurity awareness training that is updated as necessary to reflect risks identified by the licensee in the risk assessment.

(5) If the licensee has a board of directors, the board or an appropriate committee of the board must, at a minimum, do the following:

(a) Require the licensee's executive management or its delegates to develop, implement, and maintain the licensee's information security program;

(b) Require the licensee's executive management or its delegates to report in writing at least annually all of the following information:

(i) The overall status of the information security program and the licensee's compliance with this chapter; and

(ii) Material matters related to the information security program, addressing issues such as risk assessment, risk management and control decisions, third-party service provider arrangements, results of testing, cybersecurity events or violations and management's responses thereto, and recommendations for changes in the information security program; and

(c) If executive management delegates any of its responsibilities under this section, it must oversee the development, implementation, and maintenance of the licensee's information security program prepared by the delegate and must receive a report from the delegate complying with the requirements of the report to the board of directors.

(6) A licensee must exercise due diligence in selecting its third-party service provider and must require a third-party service provider to implement appropriate administrative, technical, and physical measures to protect and secure the information systems and nonpublic information that are accessible to, or held by, the third-party service provider. Nonpublic information is not accessible to, or held by, the 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.

(7) The licensee must monitor, evaluate, and adjust, as appropriate, the information security program consistent with all of the following:

(a) Any relevant changes in technology;

(b) The sensitivity of its nonpublic information;

(c) Internal or external threats to information; and

(d) The licensee's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to information systems.

(8) 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. Such incident response plan must address the following areas:

(a) The internal process for responding to a cybersecurity event;

(b) The goals of the incident response plan;

(c) The definition of clear roles, responsibilities, and levels of decision-making authority;

(d) External and internal communications and information sharing;

(e) Identification of requirements for the remediation of any identified weaknesses in information systems and associated controls;

(f) Documentation and reporting regarding cybersecurity events and related incident response activities; and

(g) The evaluation and revision as necessary of the incident response plan following a cybersecurity event.

(9) Annually, each insurer domiciled in this state must submit to the director a written statement by April 15 certifying that the insurer is in compliance with the requirements set forth in this section. Each insurer must maintain for examination by the department all records, schedules, and data supporting this certificate for a period of five (5) years. To the extent an insurer has identified areas, systems, or processes that require material improvement, updating, or redesign, the insurer must document the identification and the remedial efforts planned and underway to address such areas, systems, or processes. Such documentation must be available for inspection by the director.

41-6604. INVESTIGATION OF A CYBERSECURITY EVENT. (1) If the licensee learns that a cybersecurity event has or may have occurred, the licensee or an outside vendor or service provider designated to act on behalf of the licensee must conduct a prompt investigation.

(2) During the investigation, the licensee or an outside vendor or service provider designated to act on behalf of the licensee must, 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 the 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 must complete the steps listed in subsection (2) of this section or make reasonable efforts to confirm and document that the third-party service provider has completed those steps.

(4) The licensee must maintain records concerning all cybersecurity events for a period of at least five (5) years from the date of the cybersecurity event and must produce those records upon demand of the director.

41-6605. NOTICE OF A CYBERSECURITY EVENT. (1) Each licensee must notify the director as promptly as possible but not later than five (5) business days after a determination that a cybersecurity event has occurred when either of the following criteria has been met:

(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 41-1002, 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 of the following:

(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) The licensee must provide as much of the following information as possible. The licensee must provide the information in electronic form, as directed by the director. The licensee has a continuing obligation to update and supplement initial and subsequent notifications to the director regard-

ing material changes to previously provided information relating to the cybersecurity event:

(a) The date of the cybersecurity event;

(b) The description of how the information was exposed, lost, stolen, or breached, including the specific roles and responsibilities of third-party service providers, if any;

(c) How the cybersecurity event was discovered;

(d) Whether any lost, stolen, or breached information has been recovered and, if so, how this was done;

(e) The identity of the source of the cybersecurity event;

(f) Whether the licensee has filed a police report or has notified any regulatory, government, or law enforcement agencies and, if so, when such notification was provided;

(g) The description of the specific types of information acquired without authorization. Specific types of information means particular data elements, including, for example, types of medical information, types of financial information, or types of information allowing identification of the consumer;

(h) The period during which the information system was compromised by the cybersecurity event;

(i) The number of total consumers in this state affected by the cybersecurity event. The licensee must provide the best estimate in the initial report to the director and update this estimate with each subsequent report to the director pursuant to this section;

(j) The results of any internal review identifying a lapse in either automated controls or internal procedures or confirming that all automated controls or internal procedures were followed;

(k) The description of efforts being undertaken to remediate the situation that permitted the cybersecurity event to occur;

(l) A copy of the licensee's privacy policy and a statement outlining the steps the licensee will take to investigate and notify consumers affected by the cybersecurity event; and

(m) The name of a contact person who is both familiar with the cybersecurity event and authorized to act for the licensee.

(3) A licensee must 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 (6) 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 must 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 under this subsection, a licensee must 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 this subsection if either of the following is met:

(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 under 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 under 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.

(4) 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 under subsection (1) of this section unless the third-party service provider provides the notice required under subsection (1) of this section to the director.

(a) The computation of the licensee's deadlines begins 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 under section 41-6604, Idaho Code, or notice requirements imposed under this section.

(5) 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 that is acting as an assuming insurer, including an assuming insurer domiciled in another state or jurisdiction, and that does not have a direct contractual relationship with the affected consumers, both of the following apply:

(i) The assuming insurer must notify its affected ceding insurers and the insurance director of its state or jurisdiction of domicile within five (5) 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 under subsection (3) of this section and any other notification requirements relating to a cybersecurity event imposed under 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, both of the following apply:

(i) The assuming insurer must notify its affected ceding insurers and the insurance director of its state or jurisdiction of domicile within five (5) 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 under subsection (3) of this section and any other notification requirements relating to a cybersecurity event imposed under this section.

(c) Any licensee acting as assuming insurer will have no other notice obligations relating to a cybersecurity event or other data breach under this section.

(6) 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 under subsection (3) of this section, the insurer must notify the producers of record of all affected consumers of the cybersecurity event no later than 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.

41-6606. DIRECTOR'S POWER TO EXAMINE AND INVESTIGATE. (1) The director has 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 this chapter. This power is in addition to the powers the director has under chapter 2, title 41, Idaho Code. Any such investigation or examination will 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 this chapter, the director may take action that is necessary or appropriate to enforce the provisions of this chapter.

41-6607. 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 41-6603 or 41-6605, Idaho Code, or that are obtained by the director in an investigation or examination pursuant to section 41-6606, Idaho Code, are confidential by law and privileged, are not subject to the Idaho public records act, chapter 1, title 74, Idaho Code, and are not subject to discovery or admissible in 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 subsection (1) of this section.

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

(a) May share documents, materials, or other information, including the confidential and privileged documents, materials, or information subject to subsection (1) of this section, excluding nonpublic information, 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) May 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) May share documents, materials, or other information subject to subsection (1) of this section, excluding nonpublic information, with a third-party consultant or vendor, provided the consultant agrees in writing to maintain the confidentiality and privileged status of the document, material, or other information; and

(d) May enter into agreements governing sharing and use of information consistent with 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 under this section or as a result of sharing as authorized in subsection (3) of this section. This includes all protections granted by 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 to a database or other clearinghouse service maintained by the national association of insurance commissioners or its affiliates or subsidiaries.

41-6608. EXCEPTIONS. (1) The following exceptions apply to this chapter:

(a) A licensee meeting the following criteria is exempt from the provisions of section 41-6603, Idaho Code:

(i) That has fewer than fifty (50) employees, excluding any independent contractors;

(ii) That has less than five million dollars ($5,000,000.00) in gross annual revenue; and

(iii) That has less than ten million dollars ($10,000,000.00) in year-end total assets.

(b) A licensee that is subject to the health insurance portability and accountability act of 1996 and any amendments thereto (HIPAA), that has established and maintains a written information security program pursuant to 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 in section 41-6605(1), Idaho Code.

(c) An employee, agent, representative, or designee of a licensee, who is also a licensee, is exempt from sections 41-6603, 41-6604, and 41-6605, 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 sections 501 and 505 of the Gramm-Leach-Bliley act, 15 U.S.C. 6801 and 6805, will be considered to meet the requirements of section 41-6603, 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, documentation 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 41-6603, 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 this chapter.

41-6609. NO PRIVATE CAUSE OF ACTION. This chapter does not create or imply a private cause of action for violation of its provisions or any rules promulgated pursuant to it.

41-6610. PENALTIES FOR VIOLATION OF CHAPTER. In the case of a violation of this chapter, a licensee may be subject to civil penalties in accordance with section 41-117, Idaho Code.

41-6611. EXCLUSIVE STATE STANDARDS AND REQUIREMENTS. Notwithstanding any other provision of law, 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, 28-51-105, 28-51-106, and 28-51-107, Idaho Code, do not apply to a licensee.

41-6612. RULEMAKING AUTHORITY. The director may promulgate such rules as are necessary to carry out the provisions of this chapter.

41-6613. CONSIDERATIONS IN ADMINISTERING CHAPTER. The director will consider the nature, scale, and complexity of licensees in administering this chapter and adopting rules pursuant to this chapter.

41-6614. EFFECTIVE DATE. This chapter takes effect on July 1, 2021, provided that a licensee has until July 1, 2022, to comply with section 41-6603, Idaho Code, except for subsection (6) of that section. A licensee has until July 1, 2023, to comply with section 41-6603(6), Idaho Code.

41-6615. 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.