SENATE BILL NO. 134

IN THE LEGISLATURE OF THE STATE OF ALASKA

THIRTY-THIRD LEGISLATURE - SECOND SESSION

BY SENATORS KAUFMAN, Dunbar, Giessel, Gray-Jackson, Claman

Introduced: 4/21/23
Referred: Labor & Commerce, Judiciary, Finance

A BILL

FOR AN ACT ENTITLED

"An Act relating to insurance data security; amending Rule 26, Alaska Rules of Civil Procedure, and Rules 402 and 501, Alaska Rules of Evidence; and providing for an effective date."

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF ALASKA:

*** Section 1.** AS 21.96 is amended by adding new sections to read:

Sec. 21.96.250. Risk assessment. (a) A licensee shall conduct a risk assessment to evaluate the security and confidentiality of nonpublic information. In conducting the risk assessment, the licensee shall

(1) identify reasonably foreseeable internal or external threats in each area of the licensee's operations 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;

(2) assess the likelihood and potential damage of the threats identified

in (1) of this subsection, taking into consideration the sensitivity of nonpublic information; and

(3) assess the sufficiency in each area of the licensee's operations of the licensee's policies, procedures, information systems, and other safeguards in place to manage the threats identified in (1) of this subsection, including the areas of

(A) employee training and management;

(B) network and software design, information classification, governance, processing, storage, transmission, and disposal; and

(C) detecting, preventing, and responding to attacks or intrusions on information systems and nonpublic information, or other information system failures.

(b) A licensee shall use the licensee's risk assessment to design the licensee's information security program required under AS 21.96.260(a).

Sec. 21.96.260. Information security program. (a) A licensee shall develop, implement, and maintain a comprehensive written information security program based on the licensee's risk assessment conducted under AS 21.96.250(a). A licensee shall designate one or more employees, an outside vendor, or a third-party service provider to act on behalf of the licensee as the person responsible for the licensee's information security program.

(b) A licensee's information security program must

(1) contain administrative, technical, and physical safeguards to protect the security and confidentiality of nonpublic information and the security of the licensee's information system;

(2) protect against a threat or hazard to the security or integrity of nonpublic information and the information system;

(3) protect against unauthorized access to or use of nonpublic information and minimize the likelihood of harm to a consumer;

(4) establish and periodically reevaluate a schedule for retention of nonpublic information; and

(5) establish and implement a mechanism for the destruction of nonpublic information when the information is no longer needed.

(c) In developing, implementing, and maintaining a licensee's information security program, the licensee shall

(1) based on the licensee's risk assessment conducted under AS 21.96.250(a), implement the following security measures if the licensee determines that the security measure is appropriate:

(A) place and use effective access controls on information systems, including controls to authenticate and permit access only by authorized individuals, to protect against the unauthorized acquisition of nonpublic information; the controls may include multi-factor authentication procedures;

(B) identify and manage the data, personnel, devices, information systems, and facilities that enable the organization to achieve its business objectives in accordance with the relative importance of the data, personnel, devices, information systems, and facilities to the organization's business objectives and risk strategy;

(C) allow only authorized individuals to access physical locations containing nonpublic information;

(D) protect by encryption or other appropriate means nonpublic information transmitted over an external network or stored on a laptop computer or other portable computing or storage device or media;

(E) adopt secure development practices for applications used by the licensee that are developed in-house; the licensee shall adopt procedures for evaluating, assessing, or testing the security of externally developed applications used by the licensee;

(F) modify information systems in accordance with the licensee's information security program;

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

(H) include audit trails inside the information security program that are designed to detect and respond to cybersecurity events and to

reconstruct material financial transactions sufficient to support normal operations and obligations of the licensee;

(I) implement measures to protect against destruction, loss, or damage of nonpublic information caused by environmental hazards, including fire and water damage, or other catastrophes or technological failures; and

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

(2) determine the cybersecurity risks to include in the licensee's risk management process;

(3) stay informed of emerging threats or vulnerabilities and, when sharing information, use reasonable security measures in accordance with the character of the sharing and the type of information shared;

(4) include cybersecurity risks in the licensee's enterprise risk management process;

(5) provide personnel of the licensee with cybersecurity awareness training that is updated as necessary to reflect the risks identified in the risk assessment;

(6) implement information safeguards to manage the threats identified in a risk assessment, and, not less than once a year, assess the effectiveness of the key controls, information systems, and procedures of the safeguards;

(7) exercise due diligence in selecting a third-party service provider;

(8) 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;

(9) monitor, evaluate, and adjust, as appropriate, the information security program consistent with relevant changes in technology, the sensitivity of its nonpublic information, internal or external threats to nonpublic information, and the licensee's own changing business arrangements, including mergers, acquisitions, alliances, joint ventures, outsourcing arrangements, and changes to information systems; and

(10) establish a written incident response plan designed to promptly respond to, and recover from, a cybersecurity event that compromises the confidentiality, integrity, or availability of nonpublic information in the licensee's possession, the licensee's information systems, or the continuing functionality of an aspect of the licensee's business or operations; the incident response plan must address the following:

(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) the licensee's internal process used for external and internal communication and information sharing;

(E) the identification of requirements for the remediation of an identified weakness in information systems and associated controls;

(F) the documentation and reporting of cybersecurity events and related incident response activities; and

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

(d) A licensee's board of directors or an appropriate committee of the licensee's board of directors shall, at a minimum, require that

(1) the licensee's executive management or the executive management's delegate develop, implement, and maintain the licensee's information security program; and

(2) at least once a year, the licensee's executive management or the executive management's delegate report to the licensee's board of directors or an appropriate committee of the licensee's board of directors the following in writing:

(A) the overall status of the information security program and the licensee's compliance with AS 21.96.250 - 21.96.399; and

(B) material matters related to the information security program, including risk assessment, risk management and control decisions,

third-party service provider arrangements, results of testing, cybersecurity events or violations, management's responses to the cybersecurity events or violations, and recommendations for changes in the information security program.

(e) If a licensee's executive management meets a requirement under (d) of this section through a delegate, the executive management shall oversee the development, implementation, and maintenance of the licensee's information security program prepared by the delegate. The delegate shall provide a report to the executive management that complies with the requirements of (d)(2) of this section.

(f) Each licensee who is an insurer domiciled in this state shall

(1) submit to the director a written statement by February 15 of each year certifying that the insurer is in compliance with the requirements under AS 21.96.250 and this section;

(2) maintain and allow the director to examine for a period of five years after the insurer submits the written statement described in (1) of this subsection all records, schedules, and data supporting the written statement; and

(3) provide documentation of any areas, information systems, or processes that the insurer has identified as requiring material improvement, updating, or redesign, and provide documentation of the remedial efforts planned and underway to address the areas, information systems, or processes; the insurer shall make the documentation available for examination by the director at the director's request.

(g) In this section,

(1) "authorized individual" means an individual known to and screened by the licensee and for whom the licensee has determined access to the nonpublic information held by the licensee and its information systems is appropriate and necessary;

(2) "multi-factor authentication" means authentication through verification of at least two of the following types of authentication factors:

(A) a knowledge factor, including a password;

(B) a possession factor, including a token or text message on a mobile telephone; or

(C) an inherence factor, including a biometric characteristic.

Sec. 21.96.270. Investigation of cybersecurity event. (a) If a licensee becomes aware that a cybersecurity event has or may have occurred, the licensee or an outside vendor or third-party service provider designated to act on behalf of the licensee shall promptly investigate the cybersecurity event. During the investigation, if the licensee, outside vendor, or third-party service provider determines that a cybersecurity event has occurred, the licensee, outside vendor, or third-party service provider shall, to the extent possible,

(1) assess the nature and scope of the cybersecurity event;

(2) identify nonpublic information that may have been involved in the cybersecurity event; and

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

(b) If a licensee becomes aware that a cybersecurity event has or may have occurred in an information system maintained by a third-party service provider, the licensee shall, to the extent possible, complete the actions described in (a) of this section or confirm and document that the third-party service provider has completed those actions.

(c) A licensee shall maintain records concerning all cybersecurity events for a period of at least five years from the date of the cybersecurity event and shall produce the records at the request of the director.

Sec. 21.96.280. Notification of cybersecurity event. (a) A licensee shall notify the director as soon as possible and not later than 72 hours after a licensee determines that a cybersecurity event has occurred, if

(1) the licensee is an insurer and domiciled in this state;

(2) the licensee is an insurance producer and this state is the licensee's home state as defined in AS 21.27.990; or

(3) the licensee reasonably believes that the cybersecurity event involves the nonpublic information of 250 or more consumers residing in this state and

the cybersecurity event

(A) affects the licensee, and a state or federal law requires the licensee to provide notice of the cybersecurity event to a government agency; or

(B) has a reasonable likelihood of materially harming a consumer residing in this state or a material part of the normal operation of the licensee.

(b) The notification to the director under (a) of this section must include, to the extent possible and in a form and format prescribed by the director, the following information:

(1) the date of the cybersecurity event;

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

(3) an explanation of how the cybersecurity event was discovered;

(4) whether the lost, stolen, or breached nonpublic information has been recovered and, if so, how the nonpublic information was recovered;

(5) the identity of the source of the cybersecurity event;

(6) whether the licensee has filed a police report, or has notified a regulatory, government, or law enforcement agency about the cybersecurity event and, if so, the time and date that the licensee notified the agency;

(7) a description of the specific types of information acquired without authorization, such as medical information, financial information, or information allowing identification of the consumer;

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

(9) the number of total consumers in this state affected by the cybersecurity event; the licensee shall provide the licensee's best estimate in the licensee's initial notification to the director under (a) of this section, and shall update the estimate with each subsequent notification to the director under (c) of this section;

(10) the results of an internal review identifying a lapse in either the

licensee's automated controls or internal procedures or confirming that the licensee followed all automated controls or internal procedures;

(11) a description of efforts the licensee is taking or has taken to remediate the situation that permitted the cybersecurity event to occur;

(12) 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

(13) the name of a contact person who is familiar with the cybersecurity event and authorized to act on behalf of the licensee.

(c) After a licensee provides notice of a cybersecurity event to the director under (a) of this section, the licensee shall, in a form, format, and frequency prescribed by the director, update and supplement the information provided under (b) of this section.

(d) In addition to the requirements of this section, a licensee shall comply with all applicable provisions of AS 45.48 (Alaska Personal Information Protection Act). If a licensee is required to notify the director of a cybersecurity event under (a) of this section and is also required to provide notice under AS 45.48, the licensee shall provide to the director a copy of the notice sent to consumers under AS 45.48.

(e) If a licensee becomes aware of a cybersecurity event that affects an information system maintained by a third-party service provider of the licensee, the licensee shall comply with the requirements of this section, except that the time prescribed in (a) of this section begins the day after the third-party service provider notifies the licensee of the cybersecurity event or the day after the date the licensee has actual knowledge of the cybersecurity event, whichever is earlier.

(f) A licensee acting as an assuming insurer that determines that a cybersecurity event has occurred shall, not later than 72 hours after the determination, notify the licensee's affected ceding insurers and the insurance supervisory official of the licensee's state of domicile if

(1) the cybersecurity event involves nonpublic information and the nonpublic information is information used by or in the possession, custody, or control of the licensee acting as an assuming insurer; and

(2) the licensee does not have a direct contractual relationship with a consumer affected by the cybersecurity event.

(g) A licensee acting as an assuming insurer that receives notification from the licensee's third-party service provider that a cybersecurity event has occurred shall, not later than 72 hours after receiving notification, notify the licensee's affected ceding insurers and the insurance supervisory official of the licensee's state of domicile if the cybersecurity event involves nonpublic information and the nonpublic information is in the possession, custody, or control of the third-party service provider.

(h) A ceding insurer notified under (f) or (g) of this section that has a direct contractual relationship with an affected consumer shall comply with this section and all applicable provisions of AS 45.48 (Alaska Personal Information Protection Act).

(i) A licensee that is an insurer and that becomes aware that a cybersecurity event involving nonpublic information has occurred shall, as soon as possible and in a form and format prescribed by the director, notify each independent insurance producer of record of a consumer affected by the cybersecurity event if

(1) the nonpublic information is in the possession, custody, or control of the licensee or the licensee's third-party service provider;

(2) the consumer accessed the insurer's services through the producer; and

(3) the insurer has the current producer of record information for the consumer.

Sec. 21.96.290. Confidentiality. (a) Any document, material, or information in the possession or control of the division that is provided by a licensee or an employee or agent acting on behalf of a licensee under AS 21.96.260(f) or 21.96.280(b)(2) - (5), (8), (10), or (11) or that is obtained by the director in an investigation or examination under AS 21.96.310

(1) is confidential and privileged;

(2) is not subject to inspection and copying under AS 40.25.110 - 40.25.220;

(3) may not be obtained by subpoena or discovery; and

(4) is not admissible in evidence in a private civil action.

(b) The director may use a document, material, or information described in (a) of this section in a regulatory or legal proceeding brought in the performance of the duties of the director under this title.

(c) The director or an individual acting under the authority of the director who receives a document, material, or information described in (a) of this section may not testify about the document, material, or information in a private civil action.

(d) In the performance of duties under AS 21.96.250 - 21.96.399, the director may

(1) disclose a document, material, or information, including a document, material, or information that is confidential and privileged or subject to (a) of this section, to state, federal, and international regulatory or law enforcement agencies, or to the National Association of Insurance Commissioners and its affiliates or subsidiaries, if the recipient agrees in writing to maintain the confidentiality and privileged status of the document, material, or information;

(2) receive a document, material, or information, including a document, material, or information that is confidential and privileged, from the National Association of Insurance Commissioners and its affiliates or subsidiaries, and from state, federal, and international regulatory or law enforcement agencies; the director shall maintain as confidential or privileged the document, material, or information if the entity that provided the director with the document, material, or information requests the director to do so or gives notice to the director that the document, material, or information is confidential or privileged under the law of the jurisdiction supplying it;

(3) disclose a document, material, or information that is subject to (a) of this section with a third-party service provider if the third-party service provider agrees in writing to maintain the confidentiality and privileged status of the document, material, or information; and

(4) enter into agreements consistent with this section governing the sharing and use of a document, material, or information that is confidential or privileged or subject to (a) of this section.

(e) A person does not waive a claim of privilege or confidentiality that the

person possesses by providing a document, material, or information to the director under AS 21.96.250 - 21.96.399 or by the disclosure, receipt, or sharing of a document, material, or information under (d) of this section.

Sec. 21.96.300. Applicability. (a) AS 21.96.250 and 21.96.260 do not apply to

(1) a licensee, including an independent contractor, with fewer than 10 employees;

(2) a licensee if the licensee is an employee, agent, representative, or designee of another licensee covered by an information security program.

(b) AS 21.96.250 - 21.96.399 do not apply to a licensee subject to the Health Insurance Portability and Accountability Act of 1996 (P.L. 104-191) if the licensee

(1) has established and maintains an information security program under statutes, regulations, procedures, or guidelines established under the Health Insurance Portability and Accountability Act of 1996 (P.L. 104-191);

(2) is in compliance with the statutes, regulations, procedures, and guidelines established under the Health Insurance Portability and Accountability Act of 1996 (P.L. 104-191); and

(3) submits to the director a written statement certifying that the licensee is in compliance with the statutes, regulations, procedures, and guidelines established under the Health Insurance Portability and Accountability Act of 1996 (P.L. 104-191).

(c) If a licensee no longer qualifies for an exception to the applicability of AS 21.96.250 - 21.96.399 under this section, the licensee shall comply with AS 21.96.250 - 21.96.399 within 180 days after the licensee no longer qualifies for the exception.

Sec. 21.96.310. Enforcement; penalties. (a) In addition to the director's power to examine or investigate under AS 21.06.120, the director may examine and investigate the affairs of a licensee to determine whether the licensee is or has been in violation of AS 21.96.250 - 21.96.399. The director shall conduct an examination or investigation under this section following the same procedures applicable to an examination or investigation under AS 21.06.120. The director may take necessary or appropriate action to enforce AS 21.96.250 - 21.96.399.

(b) In addition to any other penalty provided by law, a person who violates AS 21.96.250 - 21.96.399 is subject to the penalties provided under AS 21.27.440.

(c) AS 21.96.250 - 21.96.399 do not create or imply a private cause of action for a violation of AS 21.96.250 - 21.96.399.

Sec. 21.96.399. Definitions. In AS 21.96.250 - 21.96.399,

(1) "consumer" means an individual who is a resident of this state and whose nonpublic information is in a licensee's possession, custody, or control;

(2) "cybersecurity event"

(A) means an event resulting in unauthorized access to or disruption or misuse of an information system or information stored on the information system;

(B) does not include

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

(ii) an event in which the licensee has determined that nonpublic information accessed by an unauthorized person has not been used or released and has been returned or destroyed;

(3) "encrypt" means transforming of data into a form that results in a low probability of assigning meaning without the use of a protective process or key;

(4) "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;

(5) "information system" means

(A) a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of electronic information; or

(B) a specialized system that may include an industrial or process control system, a telephone switching and private branch exchange system, or an environmental control system;

(6) "licensee"

(A) means a person licensed, authorized to operate, or registered, or required to be licensed, authorized, or registered, under the insurance laws of this state;

(B) does not include a purchasing group or a risk retention group chartered and licensed in a state other than this state or a licensee that is acting as an assuming insurer that is domiciled in another state or jurisdiction;

(7) "nonpublic information" means information that is not publicly available information and that 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 effect to the business, operations, or security of the licensee;

(B) information concerning a consumer that, because of a name, number, personal mark, or other identifier, can be used to identify the consumer in combination with one or more of the following data elements:

(i) a social security number;

(ii) a driver's license number or identification card number;

(iii) an account, credit card, or debit card number;

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

(v) a biometric record; or

(C) 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 relates to

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

(ii) the provision of health care to a consumer; or

(iii) payment for the provision of health care to a consumer;

(8) "person" means an individual or a nongovernmental entity;

(9) "publicly available information" means information that a licensee has determined is made available to the general public from

(A) a federal, state, or local government record;

(B) a widely distributed media; or

(C) a disclosure to the general public that is required under federal, state, or local law;

(10) "third-party service provider" means a person that is not a licensee that, through a contract with a licensee, is permitted access to and maintains, processes, or stores nonpublic information through its provision of services to the licensee.

*** Sec. 2.** The uncodified law of the State of Alaska is amended by adding a new section to read:

INDIRECT COURT RULE AMENDMENTS. (a) AS 21.96.290(a)(3), enacted by sec. 1 of this Act, has the effect of changing Rule 26, Alaska Rules of Civil Procedure, by prohibiting discovery of evidence in the possession or control of the division of insurance that is provided by a licensee or an employee or agent acting on behalf of a licensee under AS 21.96.260(f) or 21.96.280(b)(2) - (5), (8), (10), or (11) or that is obtained by the director in an investigation or examination under AS 21.96.310.

(b) AS 21.96.290(a)(4) and (c), enacted by sec. 1 of this Act, have the effect of changing Rules 402 and 501, Alaska Rules of Evidence, by

(1) creating a new privilege that would prevent the director of the division of insurance, or an individual acting under the authority of the director, from being permitted or compelled to testify about confidential or privileged documents, materials, or information in a private civil action; and

(2) precluding admissibility of evidence in a private action of documents, materials, or other information in the possession or control of the division of insurance that is provided by a licensee or an employee or agent acting on behalf of a licensee under AS 21.96.260(f) or 21.96.280(b)(2) - (5), (8), (10), or (11) or that is obtained by the director in an investigation or examination under AS 21.96.310.

*** Sec. 3.** The uncodified law of the State of Alaska is amended by adding a new section to

read:

TRANSITION: REGULATIONS. The director of the division of insurance may adopt regulations necessary to implement this Act. The regulations take effect under AS 44.62 (Administrative Procedure Act), but not before the effective date of the law implemented by the regulation.

*** Sec. 4.** The uncodified law of the State of Alaska is amended by adding a new section to read:

CONDITIONAL EFFECT. AS 21.96.290(a)(3) and(4) and (c), enacted by sec. 1 of this Act, take effect only if sec. 2 of this Act receives the two-thirds majority vote of each house required by art. IV, sec. 15, Constitution of the State of Alaska.

*** Sec. 5.** Section 3 of this Act takes effect immediately under AS 01.10.070(c).

*** Sec. 6.** AS 21.96.250 and 21.96.260(a), (b), (c)(1) - (6), (9), and (10), and (d) - (g), enacted by sec. 1 of this Act, take effect January 1, 2025.

*** Sec. 7.** AS 21.96.260(c)(7) and (8), enacted by sec. 1 of this Act, take effect January 1, 2026.

*** Sec. 8.** Except as provided in secs. 5 - 7 of this Act, this Act takes effect January 1, 2024.