THE STATE of ALASKA
GOVERNOR MIKE DUNLEAVY

Department of Commerce, Community, and Economic Development

DIVISION OF INSURANCE
Anchorage Office

550 West Seventh Avenue, Suite 1560
Anchorage, Alaska 99501-3567
Main: 907.269.7900
Fax: 907.269.7910

BULLETIN B 24-11

TO: ALL LICENSEES AND ADMITTED INSURERS IN THE STATE OF ALASKA AND OTHER INTERESTED PARTIES

RE: ALASKA INSURANCE DATA SECURITY LAW

On August 29, 2024, Alaska Senate Bill (SB) 134 (Chapter 39, SLA 24) relating to insurance data security (Act) and amending Alaska Statute (AS) 21.23 was enacted. Under AS 21.23.240, the Act establishes standards for data security as well as investigation and notification requirements in the case of cybersecurity event for licensees of the Alaska Division of Insurance (Division). This bulletin is intended to provide licensees with guidance for compliance with the Act's provisions. The enrolled and enacted full text of SB 134 is found at internet address: https://www.akleg.gov/PDF/33/Bills/SB0134Z.PDF.

What are the provisions of the Act?

Scope: The Act has provisions that are effective January 1, 2025, January 1, 2026, and January 1, 2027, which are detailed below under "Effective Dates" and apply to Alaska insurance licensees, which includes licensed insurers, producers, and any other person licensed or required to be licensed, authorized or required to be authorized, or registered or required to be registered under AS 21.27, or holding a certificate of authority under AS 21.09. Pursuant to AS 21.23.300 of the Act, certain licensees may be exempt from the requirements of this Act (see below under "Applicability").

Risk Assessment: As explained in AS 21.23.250(a)-(b) of the Act, licensees shall conduct a risk assessment to evaluate the security and confidentiality of non-public information in its possession or held by third-parties. The risk assessment will be used to design the licensee's information security program required under AS 21.23.260(a).

Information Security Program: As explained in AS 21.23.260(a), licensees shall develop, implement and maintain a comprehensive written information security program (ISP) that complies with the ISP requirements of AS 21.23.260(b)-(c). The ISP must be based on the licensee's risk assessment and contain safeguards for the protection of nonpublic information and the licensee's information systems, commensurate with the size and complexity of the licensee, its activities, including use of third-party service providers, and the sensitivity of the nonpublic information used by the licensee that is in its possession, custody, or control. This section also

requires licensees to establish a written response plan designed to promptly respond to and recover from a cybersecurity event. The requirements for the response plan are detailed in this section. AS 21.23.260(d)-(e) provides the minimum requirements for a licensee's Board of Directors regarding oversight of the ISP.

Annual Certification of Information Security Program: AS 21.23.260(f) requires insurers to submit by February 15 of each year an annual statement to the Director certifying compliance with AS 21.23.250 and AS 21.23.260. Records and other documentation requirements are also outlined in this section. The first submission is due by February 15, 2026. The annual certification notification to the Director shall be reported in an electronic form which will be available on the Alaska Division of Insurance's website by January 1, 2025.

Investigation of cybersecurity event: AS 21.23.270(a)-(c) establishes requirements and obligations for a licensee and third-party service providers to promptly investigate if they learn a cybersecurity event has or may have occurred. The investigation shall cover to the extent possible the following, whenever applicable:

- assess the nature and scope of the cybersecurity event;
- identify any nonpublic information involved in the cybersecurity event;
- take steps to restore the security of the information compromised to prevent further unauthorized acquisition, release, or use of nonpublic information in the licensee's possession, custody, or control.

Licensees are required to maintain records concerning cybersecurity events for at least five years after the event and produce those records upon request of the Director.

Notification of cybersecurity event: The notification requirement applies to a licensee who is an insurer domiciled in Alaska, a licensee who is a producer whose home state is Alaska, or the licensee reasonably believes that the cybersecurity event involves the nonpublic information of 250 or more consumers residing in the state of Alaska as specified by AS 21.23.280(a)(3)(A-B). Unless a federal law enforcement official instructs the licensee not to distribute information regarding a cybersecurity event, a licensee shall notify the Director as promptly as possible, that a cybersecurity event has occurred, but in no event later than three (3) business days after the date of the cybersecurity event. Direction for licensees regarding notification is provided in AS 21.23.280(a)-(k), which also includes notification requirements involving third-party service providers, insurers, and licensees acting as an assuming insurer. Notification to the Director of a cybersecurity event shall be reported in an electronic form which will be available on the Alaska Division of Insurance's website by January 1, 2025.

Notification to Alaska Consumers: AS 21.23.280(d) requires each licensee to 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 the Director a copy of the notice sent to consumers under AS 45.48.

Confidentiality: AS 21.23.290(a)-(e) provides among other protections that materials, documents, or other information in the possession or control of the Division of Insurance, which is obtained in an investigation or examination, will be treated as confidential and privileged. However, the Director may use the information identified in this section in furtherance of a regulatory action and share or receive confidential documents under certain circumstances.

Applicability: Under AS 21.23.300(a)-(b) a licensee, including an independent contractor with fewer than 10 employees, or a licensee that is an employee, agent, representative, or designee of another licensee covered by an ISP, is not subject to AS 21.23.250 - 21.23.260. Also, AS 21.23.240 – 21.23.399 do not apply to licensees subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) if conditions are met as described in AS 21.23.300(b)(1)-(3). The information security program exemption certification to the Director shall be reported in an electronic form which will be available on the Alaska Division of Insurance's website by January 1, 2025.

Enforcement; penalties: Applicable penalties for violations determined by the Director of AS 21.23.240 – 21.23.399 are explained in AS 21.23.310(a)-(b).

Effective Dates:

Except as provided in the following provisions, this Act takes effect January 1, 2025.

Risk Assessment: AS 21.23.250 takes effect January 1, 2026.

Information Security Program: AS 21.23.260(a), (b), (c)(1) - (6) and (9) - (11), and (d) - (g),

take effect January 1, 2026.

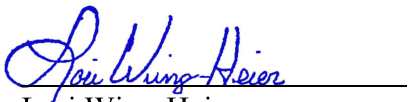
Information Security Program: AS 21.23.260(c)(7) and (8), take effect January 1, 2027.

Definitions: AS 21.23.399 provides the meaning of terminology used in this Act.

Forms related to the requirements in the Act can be found at
https://www.commerce.alaska.gov/web/ins/CyberSecurity.

Questions regarding this bulletin should be directed to Chief Investigator Alex Romero at
alex.romero2@alaska.gov or 907-269-7918.

Dated December 19, 2024.



Lori Wing-Heier
Director of Insurance