



---

**BULLETIN NO. 2024-10**

---

**TO: ALL PERSONS AND ORGANIZATIONS SUBJECT TO THE JURISDICTION OF THE INSURANCE COMMISSIONER**

**RE: INSURANCE DATA SECURITY ACT (SB 543, 2024 SESSION)**

**FROM: GLEN MULREADY, INSURANCE COMMISSIONER**

**DATE: October 17, 2024**

---

The purpose of this bulletin is to inform all persons and nongovernmental entities who are licensed, registered, or otherwise authorized to operate pursuant to Title 36 of Oklahoma Statutes of important new requirements enacted by Senate Bill 543, which creates the Insurance Data Security Act, 36 O.S. § 670 – 679. **Disclaimer:** *The following overview does not include every legislative change made by Senate Bill 543. Please refer to the [Oklahoma Supreme Court Network \(OSCN\) webpage](#) to view all changes.*

**Legislative Changes effective July 1, 2024**

**36 O.S. § 670**

Notwithstanding any other provision of law, the provisions of the Act shall be the exclusive state law for licensees subject to the jurisdiction of the Insurance Commissioner for data security, the investigation of a cybersecurity event, and notification to the Commissioner.

**36 O.S. § 673(E)(2).**

**Annual Report of Status** – This provision requires each licensee with a board of directors to file an annual report on the status of, and material matters related to, the information security program required by the Act. The first submission deadline is July 1, 2025. Additional information on this requirement and instructions for filing will be published in a separate bulletin at a later date.

**36 O.S. § 673(I).**

**Data Security Attestation of Compliance** – “Annually, each insurer domiciled in this state shall submit to the Commissioner a written statement by April 15, certifying that the insurer complies with the requirements set forth in this section. Each insurer shall maintain, for examination by the Insurance 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 shall document the identification and the remedial efforts planned and underway to address such areas, systems, or processes. The documentation shall be available for inspection by the Commissioner upon request.”

The Data Security Attestation form can be found on the Oklahoma Insurance Department website at: <https://www.oid.ok.gov/regulated-entities/financial/market-conduct-regulation/>. The Data Security Attestation form must be filed by emailing the completed form to [OIDRegulatoryReporting@oid.ok.gov](mailto:OIDRegulatoryReporting@oid.ok.gov).

Because licensees have until July 1, 2025, to come into compliance with all the requirements of 36 O.S. § 673, the first deadline for submission of the Form is July 1, 2025, with subsequent Forms to be due by April 15<sup>th</sup> of each following year.

### **36 O.S. § 675**

**Cybersecurity Event Notification** – 36 O.S. § 675(A) and (B) require every licensee to notify the Insurance Commissioner without unreasonable delay, but not later than three business days, from a determination that a cybersecurity event involving nonpublic information that is in the possession of a licensee has occurred when either of the following criteria has been met:

- This state is the state of domicile of the licensee, in the case of an insurer, or this state is the home state of the licensee, in the case of a producer, and the cybersecurity event has a reasonable likelihood of materially harming any material part of the normal operations of the licensee or any consumer residing in this state; or
- The licensee reasonably believes that the nonpublic information involved is of two hundred fifty (250) or more consumers residing in this state and is either of the following:
  - 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
  - a cybersecurity event that has a reasonable likelihood of materially harming:
    - any consumer residing in this state, or
    - any material part of the normal operation or operations of the licensee.

The licensee making the notification shall provide as much of the following information as possible, electronically in the manner and form prescribed by the Commissioner, along with any applicable fees:

- Date of the cybersecurity event;
- Description of how the information was exposed, lost, stolen, or breached including, but not limited to, the specific roles and responsibilities of third-party service providers, if any;
- How the cybersecurity event was discovered;
- Whether any lost, stolen, or breached information has been recovered and, if so, how this was done;
- The identity of the source of the cybersecurity event;
- 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;
- Description of the specific types of information acquired without authorization. The term “specific types of information” means particular data elements including, but not limited to, types of medical information, financial information, or information allowing identification of the consumer;
- The period during which the information system was compromised by the cybersecurity event;
- The number of total consumers in this state affected by the cybersecurity event. The licensee shall provide the best estimate in the initial report to the Commissioner and update this estimate with each subsequent report to the Commissioner pursuant to this section;
- 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;
- Description of efforts being undertaken to remediate the situation which permitted the cybersecurity event to occur;
- A copy of the privacy policy of the licensee and a statement outlining the steps the licensee will take to investigate and notify consumers affected by the cybersecurity event; and

- Name of a contact person who is both familiar with the cybersecurity event and authorized to act for the licensee.

The Cybersecurity Event Notification form can be found on the Oklahoma Insurance Department website at: <https://www.oid.ok.gov/regulated-entities/financial/market-conduct-regulation/>.

### **36 O.S. § 678(B)**

**Exceptions** - The Insurance Data Security Act does not apply to the following licensees:

- A licensee with less than Five Million Dollars (\$5,000,000.00) in gross annual revenue is exempt from this act (Note: This includes all income, not just premiums written);
- A licensee subject to the Health Insurance Portability and Accountability Act, Pub. L. 104–191, 110 Stat. 1936, as amended, that has established and maintains an information security program pursuant to such statutes, rules, regulations, procedures, or guidelines established thereunder, will be considered to meet the requirements of Section 4 of this act, provided that the licensee is compliant with and submits a written statement to the Commissioner certifying its compliance with the same;
- A licensee subject to Title V of the federal Gramm-Leach-Bliley Act of 1999 (15 U.S.C. Sections 6801-6809 and 6821-6827) that has established and maintains an information security program pursuant to such, statutes, rules, regulations, procedures, or guidelines established thereunder, will be considered to meet the requirements of Section 4 of this act, provided that the licensee is compliant with and submits a written statement to the Commissioner certifying its compliance with the same; and
- An employee, agent, representative, or designee of a licensee, who is also a licensee, is exempt from this act and shall not be required to develop their own information security program to the extent that the employee, agent, representative, or designee is covered by the information security program of the licensee.

The scope of all required reporting shall encompass information from the previous calendar year. Pursuant to 36 O.S. § 679, licensees shall have one (1) year from the effective date of the Act (July 1, 2024) to come into compliance with 36 O.S. § 673 and two (2) years from the effective date of the Act to come within compliance of 36 O.S. § 673(F).

The provisions of this act shall take precedence over any other state laws applicable to licensees for data security and the investigation of a cybersecurity event. The licensee shall have a continuing obligation to update and supplement initial and subsequent notifications to the Commissioner regarding material changes to previously provided information relating to the cybersecurity event.

A licensee shall comply with the procedures of the Security Breach Notification Act, 24 O.S. §§ 161, *et seq.*, to notify affected consumers and provide a copy of the notice sent to consumers under that statute to the Commissioner when a licensee is required to notify the Commissioner.

Questions concerning this bulletin should be directed to the Oklahoma Insurance Department by email to [OIDRegulatoryReporting@oid.ok.gov](mailto:OIDRegulatoryReporting@oid.ok.gov).