Wisconsin Office of the
COMMISSIONER
OF INSURANCE

Tony Evers, Governor of Wisconsin
Mark Afable, Commissioner of Insurance

DATE: September 30, 2021

TO: All Insurers, Intermediaries, and Persons required to be licensed, authorized, or registered under Wis.Stat. chs. 600 to 655

FROM: Mark V. Afable, Commissioner of Insurance

SUBJECT: 2021 Wis. Act 73 relating to insurance data security requirements, New Law Update

The Office of the Commissioner of Insurance (OCI) is issuing this bulletin to ensure that licensees are aware of 2021 Wis. Act 73 which imposes new requirements related to insurance data security. The act creates subchapter IX of chapter 601 and generally requires that licensees develop and maintain an information security program, take certain steps to promptly investigate cybersecurity events, and notify OCI and consumers when a cybersecurity breach has occurred. This bulletin only highlights certain provisions of the law and licensees should review the law to ensure they are in compliance with all of its provisions. A copy of 2021 Wis. Act 73 may be found here.

Persons subject to the Act

The requirements of the act generally apply to a "licensee", which is defined as "a person licensed, authorized, or registered, or a person required to be licensed, authorized, or registered, under chs. 600 to 655." Wis. Stat. § 601.95(7). Risk retention groups chartered and licensed in another state and insurers acting as an assuming insurer domiciled in another state are exempt from the definition of licensee. It should be also noted that while the law generally applies to all licensees, certain requirements are limited to licensees domiciled in Wisconsin.

Information Security program

Wis. Stat. § 601.952 requires that a licensee develop, implement, and maintain a comprehensive information security program designed to protect the licensee's information systems and nonpublic information. The security program shall be based on a risk assessment conducted by the licensee that complies with Wis. Stat. § 601.952(2). This risk assessment includes identifying foreseeable threats to security, assessing the likelihood and potential damage of those threats, and assessing the sufficiency of safeguards in place to manage threats.

Based on this risk assessment, Wis. Stat. § 601.952(3) requires a licensee to design an information security system to mitigate identified threats commensurate with the size and complexity of the licensee and implement other security measures as appropriate. A licensee must also designate a person or persons as responsible for the licensee's information security system, stay informed regarding emerging threats, assess the effectiveness of security safeguards no less than annually, and include cybersecurity risk in the licensee's enterprise risk management process. The requirement to develop an information security program must be completed within one year after the effective date of this provision which is November 1, 2022.

Additional provisions require licensees to develop an incident response plan to respond to and recover from a cybersecurity breach. Wis.Stat. § 601.952(5). Licensees are also required to exercise due diligence in selecting third-party service providers and make reasonable efforts to ensure that third-party service providers employ appropriate security measures and reporting of cybersecurity events. Wis.Stat. § 601.952(6). The provisions addressing third-party service providers become effective two years after the effective date of these provisions which is November 1, 2023.

For licensees with a board of directors, the board or a committee of the board is required to oversee the development and implementation of the information security program. Executive management is required to report on information security programs to the board at least annually. Wis. Stat. § 601.952(7).

Wis. Stat § 601.952(8) requires that licensees provide an annual certification to OCI that the licensee is in compliance with the information security program requirements of Wis. Stat. § 601.952. Licensees must maintain records that support the certification for at least five years and shall produce the records upon demand of OCI. The certification requirement only applies to licensees who are domiciled in the state of Wisconsin. Annual certifications are required to be provided to OCI not later than March 1st with the first certification required to be filed on March 1, 2023.

Information on the procedure for providing the annual certification will be provided at a later date.

The requirements of Wis. Stat. § 601.952 do not apply to licensees:

- Who have less than $10 million in total assets; or
- Less than $5 million in gross annual revenue; or
- Fewer than 50 employees which includes independent contractors that work at least 30 hours per week.

Investigation of a Cybersecurity Event

The law defines “Cybersecurity event” as “an event resulting in the unauthorized access to, or disruption or misuse of, an information system or the nonpublic information stored on an information system.” The term does not include the unauthorized acquisition of encrypted nonpublic information if the encryption process or key is not also acquired nor the unauthorized acquisition of nonpublic information if the licensee determines that the nonpublic information has not been used or released and has been returned to the licensee or destroyed.

Under Wis.Stat. § 601.953(1) if a licensee learns that a cybersecurity event involving its information systems has occurred, the licensee must conduct a prompt investigation that, at a minimum, includes the following:

- An assessment of the nature and the scope of the event;
- Identification of any non-public information that may have been involved; and
- The performance of reasonable measures to restore security;

If a licensee knows that a cybersecurity event has occurred in the information systems maintained by a third party, the licensee must make reasonable efforts to confirm the third-party

provider conducted an investigation consistent with this section or document the third-party provider's failure to cooperate. Wis.Stat. § 601.953(2). Records related to a cybersecurity event must be maintained for at least 5 years and be available to OCI upon request. Wis.Stat. § 601.953(3).

Notification of Cybersecurity Event

Wis. Stat § 601.954 outlines the requirements for licensees to provide notice to OCI of a cybersecurity event involving nonpublic information.

For licensees domiciled in Wisconsin, notice must be given when there is a reasonable likelihood of material harm to consumers, regardless of the number of consumers affected, or the operations of the licensee.

For all licensees, notice must be given to OCI if the cybersecurity event involves at least 250 consumers and either:

- Notice is required to be provided to a governmental or supervisory entity under state or federal law; or
- There is a reasonable likelihood of material harm to consumers or the operations of the licensee.

Notification must be provided as promptly as possible but no later than three business days after the determination that a cybersecurity event involving nonpublic information has occurred. For example, if a licensee learns that there has been unauthorized access to a computer system storing nonpublic information, notice must be given to OCI no later than three business days after the licensee learns of that event.

That notification to OCI must include:

- The date and source of the cybersecurity event.
- A description as to how the cybersecurity event was discovered.
- A description as to how nonpublic information was exposed including the specific data elements exposed, and an explanation and status of recovery efforts of the information.
- The number of consumers affected.
- A description of the efforts to address the cause of the cybersecurity event.
- The results of any internal review of the cybersecurity event.
- Whether the licensee notified a governmental body or supervisory entity.
- A copy of the licensee's policy and steps the licensee will take to investigate and notify affected consumers.
- The name of the contact person who is familiar with the cybersecurity event and authorized to act on behalf of the licensee.

Licensees should not wait to provide notice to OCI until an investigation has been completed and all of this detailed information is known. The law requires a licensee to supplement this information as additional information becomes available and notice must be given within three business days of learning of the cybersecurity event even if the full details of the event are unknown at that time.

Until additional processes are put in place, licensees should continue to follow OCI's December 4, 2006 bulletin on reporting Information Security Incidents. OCI will provide additional updates when the reporting process is changed.

If a licensee knows the nonpublic information of a consumer has been acquired by a person not authorized to have such information, the licensee must notify each affected consumer and shall indicate that licensee knows of the unauthorized acquisition of nonpublic information pertaining to that consumer. If a licensee is required to notify 1,000 or more consumers due to a single event, notice must be provided to the consumer reporting agencies.

Notice must be given to affected consumers within a reasonable time not to exceed 45 days after the licensee becomes aware of the unauthorized acquisition of nonpublic information. Upon written request of the consumer, a licensee must identify the nonpublic information that was acquired. A licensee must also provide a copy of the consumer notice to OCI.

For assuming insurers, notification must be given to the ceding insurer and the commissioner of the assuming insurer's state of domicile not later than three business days after learning of the cybersecurity event. A ceding insurer who has a direct contractual relationship with the consumer is required to comply with the notice requirements of this section.

Confidentiality

Information produced to OCI under this subchapter is considered to be confidential, proprietary and containing trade secrets. The information is not subject to open records requirements, not subject to subpoena or discovery and is not admissible as evidence in private civil action.

General Exceptions

The requirements of this subchapter do not apply to an employee or agent of a licensee to the extent that person is covered by the information security program of the licensee.

Licensees are considered to meet the information security program requirements of the Act if:

- The licensee is affiliated with a depository institution and complies with interagency security guidelines as set forth in 15 USC 6801 and 6805;
- The licensee is affiliated with a broker or dealer and complies with FINRA information security program requirements;
- A licensee is affiliated with an entity established pursuant to the federal Farm Credit Act and complies with information security program requirements set forth by the Farm Credit Administration;
- A licensee who is subject to HIPAA privacy rules as set forth in 45 CFR parts 160 and 164 and who maintains nonpublic information in the same manner as protected health information.

Licensees who cease to qualify for an exemption have 180 days to comply with this subchapter.

Effective Date

The requirements of the law generally take effect on November 1, 2021, except where specific effective dates apply as noted in this bulletin.

Any questions concerning this bulletin should be directed to Sarah Smith at Sarah.Smith2@wisconsin.gov.