Wis. Stat. § 601.954

This document is current through Act 142 of the 2023-2024 Legislative Session

LexisNexis® Wisconsin Annotated Statutes > Insurance (Chs. 600 — 655) > Chapter 601. Insurance — Administration (Subchs. I — IX) > Subchapter IX Insurance Data Security (§§ 601.95 — 601.956)

601.954. Notification of a cybersecurity event.

(1)

(a) Notification to the commissioner. A licensee shall notify the commissioner that a cybersecurity event involving nonpublic information has occurred if any of the following conditions is met:

1. The licensee is domiciled in this state and the cybersecurity event has a reasonable likelihood of materially harming a consumer or a material part of the normal operations of the licensee.

2. The cybersecurity event is any of the following and the licensee reasonably believes that the cybersecurity event involves the nonpublic information of at least 250 consumers:

a. A cybersecurity event for which notice is required to be provided to a government body, self-regulatory agency, or other supervisory entity under state or federal law.

b. A cybersecurity event that has a reasonable likelihood of materially harming a consumer or a material part of the normal operations of the licensee.

(b) A licensee shall provide the notification under par. (a) in electronic form and as promptly as possible, but no later than 3 business days from the determination that the cybersecurity event occurred. In the notification, the licensee shall provide as much of the following information as possible:

1. The date and source of the cybersecurity event and the time period during which information systems were compromised by the cybersecurity event.

2. A description of how the cybersecurity event was discovered.

3. A description of how the nonpublic information was exposed, lost, stolen, or breached and an explanation of how the information has been, or is in the process of being, recovered.

4. A description of the specific data elements, including types of medical, financial, and personally identifiable information, that were acquired without authorization.

5. The number of consumers affected by the cybersecurity event.

6. A description of efforts to address the circumstances that allowed the cybersecurity event to occur.

7. The results of any internal review related to the cybersecurity event, including the identification of a lapse in automated controls or internal procedures.

8. Whether the licensee notified a government body, self-regulatory agency, or other supervisory entity of the cybersecurity event and, if applicable, the date the notification was provided.

9. A copy of the licensee's privacy policy and a statement outlining the steps the licensee will take, or has taken, to investigate and notify consumers affected by the cybersecurity event.

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

(c) The licensee shall update and supplement the information provided under par. (b) to address material changes to the information as additional information becomes available to the licensee.

(2)

(a) Notice to consumers and producers of record. Notice to consumers. If a licensee knows that nonpublic information of a consumer in the licensee's possession has been acquired by a person whom the licensee has not authorized to acquire the nonpublic information, the licensee shall make reasonable efforts to notify each consumer who is the subject of the nonpublic information. The notice shall indicate that the licensee knows of the unauthorized acquisition of nonpublic information pertaining to the consumer.

(b) Notice to consumer reporting agencies. If, as the result of a single incident, a licensee is required under par. (a) to notify 1,000 or more consumers, the licensee shall without unreasonable delay notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 USC 1681a (p), of the timing, distribution, and content of the notices sent to the consumers.

(c) Exceptions. Notwithstanding pars. (a) and (b), a licensee is not required to provide notice of the acquisition of nonpublic information if any of the following applies:

1. The acquisition of nonpublic information does not create a material risk of identity theft or fraud to the individual who is the subject of the nonpublic information.

2. The nonpublic information was acquired in good faith by an employee or agent of the licensee and is used for a lawful purpose of the licensee.

(d) Timing and manner of notice; other requirements.

1. Subject to par. (h), a licensee shall provide the notice required under par. (a) within a reasonable time, not to exceed 45 days after the licensee learns of the acquisition of nonpublic information. A determination as to reasonableness under this subdivision shall include consideration of the number of notices that the licensee must provide and the methods of communication available to the licensee.

2. A licensee shall provide the notice required under par. (a) by mail or by a method the licensee has previously employed to communicate with the consumer who is the subject of the nonpublic information. If a licensee cannot with reasonable diligence determine the mailing address of the subject of the nonpublic information, and if the licensee has not previously communicated with the subject of the nonpublic information, the licensee shall provide notice by a method reasonably calculated to provide actual notice to the subject of the nonpublic information.

3. Upon written request by a consumer who has received a notice under par. (a), the licensee that provided the notice shall identify the nonpublic information that was acquired.

(e) Notice to commissioner. A licensee shall provide to the commissioner a form of any notice sent under this subsection.

(f) Exceptions for certain entities. This subsection does not apply to any of the following:

1. An entity that is subject to, and in compliance with, the privacy and security requirements of 15 USC 6801 to 6827, or a person that has a contractual obligation to such an entity, if the entity or person has in effect a policy concerning breaches of information security.

2. An entity that is described in 45 CFR 164.104 (a), if the entity complies with the requirements of 45 CFR part 164.

(g) Effect on civil claims. Failure to comply with this section is not negligence or a breach of any duty, but may be evidence of negligence or a breach of a legal duty.

(h) Request by law enforcement not to notify. A law enforcement agency may, in order to protect an investigation or homeland security, ask a licensee not to provide a notice that is otherwise required under par. (a) or (i) for any period of time and the notification process required under this subsection shall begin at the end of that time period. Notwithstanding pars. (a), (d), and (i), if a licensee receives such a request, the licensee may not provide notice of or publicize an unauthorized acquisition of nonpublic information, except as authorized by the law enforcement agency that made the request.

(i) Notice to producer of record. If the licensee is an insurer whose services are accessed by consumers through an independent insurance producer, the licensee shall notify the producer of record of any consumers whose nonpublic information has been acquired without authorization or affected by a cybersecurity event no later than the date at which notice is provided in par. (d), except that notice is not required to a producer of record who is not authorized by law or contract to sell, solicit, or negotiate on behalf of the licensee or if the licensee does not have the current producer of record information for a consumer.

(3) Third-party service providers. If the licensee has knowledge of a cybersecurity event involving nonpublic information on an information system maintained by a 3rd-party service provider and any of the conditions in sub. (1) (a) are met, the licensee shall provide notice to the commissioner no later than 3 days after the earlier of the date the 3rd-party service provider notifies the licensee of the cybersecurity event or the licensee has actual knowledge of the cybersecurity event. The licensee is not required to comply with this subsection if the 3rd-party service provider provides notice under sub. (1).

(4) Reinsurers. In the event of a cybersecurity event involving nonpublic information, or involving nonpublic information on an information system maintained by a 3rd-party service provider, a licensee who is acting as an assuming insurer and who does not have a direct contractual relationship with the consumers affected by the cybersecurity event shall, if any of the conditions in sub. (1) (a) are met, notify the ceding insurer and the commissioner of the licensee's state of domicile of the cybersecurity event no later than 3 business days after learning of the cybersecurity event. The licensee shall have no other notice obligations relating to a cybersecurity event or other data breach under this section or any other law of this state. A ceding insurer who has a direct contractual relationship with the affected consumers shall comply with the notification requirements under this section.

History

2021 a. 240, § 30, effective April 10, 2022; 2021 a. 73, § 7, effective November 1, 2021.

End of Document