State of Wisconsin
2021 - 2022 LEGISLATURE

LRB-1531/1
EKL:kjf

2021 SENATE BILL 160

February 24, 2021 - Introduced by Senators TESTIN, RINGHAND, FEYEN and MARKLEIN, cosponsored by Representatives PETERSEN, RAMTHUN, BROOKS, STEFFEN, DITTRICH, TUSLER, DOYLE, SPIROS, MURPHY, PETRYK, KNODL, ROZAR, VORPAGEL, ARMSTRONG, KUGLITSCH, TRANEL, SNYDER and MOSES. Referred to Committee on Insurance, Licensing and Forestry.

AN ACT ***to create*** 601.465 (3) (f), subchapter IX (title) of chapter 601 [precedes 601.95], 601.95, 601.951, 601.952, 601.953, 601.954, 601.955 and 601.956 of the statutes; **relating to:** imposing requirements related to insurance data cybersecurity and granting rule-making authority.

Analysis by the Legislative Reference Bureau

This bill imposes requirements relating to the protection of nonpublic information on insurers and other persons regulated by the Office of the Commissioner of Insurance (licensees). The bill defines "nonpublic information" to mean nonpublic electronic information in the possession, custody, or control of a licensee that is either information concerning a Wisconsin resident that can be used to identify the individual in combination with another data element, such as a Social Security number, or certain health-related information that can be used to identify a Wisconsin resident.

Under the bill, a licensee must conduct a risk assessment and develop an information security program based on the assessment. The risk assessment must identify and assess reasonably foreseeable threats that could result in unauthorized access to or transmission, disclosure, misuse, alteration, or destruction of nonpublic information. The information security program must contain safeguards for the protection of the licensee's information systems and nonpublic information and be designed to mitigate threats, commensurate with the size and complexity of the licensee, the nature and scope of the licensee's activities, and the sensitivity of the nonpublic information. The bill requires the licensee to take specified risk mitigation

actions and to monitor, evaluate, and adjust the information security program as appropriate.

The bill also requires that a licensee develop an incident response plan to promptly respond to, and recover from, a cybersecurity event that compromises the confidentiality, integrity, or availability of nonpublic information, the licensee's information systems, or the continuing functionality of the licensee's business or operations. Under the bill, "cybersecurity event" generally means an event resulting in the unauthorized access to, or disruption or misuse of, an information system or nonpublic information stored on an information system.

The bill further requires that a licensee exercise due diligence in selecting third–party service providers and make reasonable efforts to require that a service provider implement measures to protect and secure information systems and nonpublic information and report the occurrence of any cybersecurity event.

Under the bill, the above requirements do not apply to a licensee who has less than $10 million in year–end total assets, less than $5 million in gross annual revenue, or fewer than 25 full–time employees. However, the commissioner may issue an order to require compliance by an otherwise exempt licensee if warranted by the licensee's circumstances. A licensee who is not exempt from the requirements must annually certify to the commissioner that the licensee has complied with them.

Additionally, if a licensee knows that a cybersecurity event has or may have occurred, the bill requires that the licensee conduct a prompt investigation to assess the nature and scope of the event and take related actions, including the performance of reasonable measures to restore the security of affected information systems. If the cybersecurity event involves an information system maintained by a third–party service provider, the licensee must comply with the investigation requirements or make reasonable efforts to confirm that the service provider has either complied with the requirements or failed to cooperate with the investigation.

Under the bill, a licensee must notify the commissioner of a cybersecurity event if either of the following conditions is met:

1. The licensee is domiciled in Wisconsin and the cybersecurity event has a reasonable likelihood of materially harming a Wisconsin resident or a material part of the licensee's normal operations.

2. The licensee reasonably believes that the cybersecurity event involves the nonpublic information of at least 250 Wisconsin residents, and the cybersecurity event either must be reported to a government entity under federal or state law or has a reasonable likelihood of materially harming a Wisconsin resident or a material part of the licensee's normal operations.

The notification must provide specified information about the cybersecurity event, including details about the event and its discovery, a description of the accessed nonpublic information, the number of affected Wisconsin residents, and the licensee's efforts to address the circumstances that allowed the event to occur. The licensee is required to update the commissioner on material changes to the information and as additional information becomes available. If the cybersecurity event involves a third–party service provider, the licensee must notify the commissioner of the event unless the service provider does so.

Under the bill, the commissioner has the power to examine and investigate the affairs of a licensee to determine whether a violation of any of the above requirements has occurred. A licensee must generally keep records relating to the requirements for at least five years and produce them upon demand of the commissioner. Any documents, materials, and other information from a licensee that are in the possession or control of the commissioner are confidential and privileged.

For further information see the state fiscal estimate, which will be printed as an appendix to this bill.

The people of the state of Wisconsin, represented in senate and assembly, do enact as follows:

SECTION 1. 601.465 (3) (f) of the statutes is created to read:

601.465 **(3)** (f) All information protected under s. 601.955, which is subject only to the confidentiality provisions in s. 601.955.

SECTION 2. Subchapter IX (title) of chapter 601 [precedes 601.95] of the statutes is created to read:

CHAPTER 601

SUBCHAPTER IX

INSURANCE DATA SECURITY

SECTION 3. 601.95 of the statutes is created to read:

601.95 Definitions. In this subchapter:

(1) "Authorized individual" means an individual who is known to and screened by a licensee and whose access to the licensee's information system or nonpublic information is determined by the licensee to be necessary and appropriate.

(2) "Consumer" means an individual who is a resident of this state and whose nonpublic information is in the possession, custody, or control of a licensee.

(3) "Cybersecurity event" means 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, except that a "cybersecurity event" does not include any of the following:

(a) The unauthorized acquisition of encrypted nonpublic information if the encryption process or key is not also acquired, released, or used without authorization.

(b) 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.

(4) "Encrypted" means the transformation of data into a form that results in a low probability of assigning meaning without the use of a protective process or key.

(5) "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.

(6) "Information system" means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of nonpublic information, as well as any specialized system, including an industrial or process controls system, telephone switching and private branch exchange system, and environmental control system.

(7) "Licensee" means a person licensed, authorized, or registered, or a person required to be licensed, authorized, or registered, under chs. 600 to 655, other than a purchasing or risk retention group that is chartered and licensed in another state or a person acting as an assuming insurer that is domiciled in another state or jurisdiction.

(8) "Multifactor authentication" means authentication through verification of at least 2 of the following types of authentication factors:

(a) Knowledge factor, including a password.

(b) Possession factor, including a token or text message on a mobile phone.

(c) Inherence factor, including a biometric characteristic.

(9) "Nonpublic information" means electronic information in the possession, custody, or control of a licensee that is not publicly available information and is any of the following:

(a) Information concerning a consumer that can be used to identify the consumer, in combination with at least one of the following data elements:

1. Social security number.

2. Driver's license number or nondriver identification card number.

3. Financial account number or credit or debit card number.

4. Security code, access code, or password that permits access to a financial account.

5. Biometric records.

(b) Information or data, other than information or data regarding age or gender, in any form or medium created by or derived from a health care provider or a consumer that can be used to identify the consumer and that relates to any of the following:

1. The physical, mental, or behavioral health or condition of the consumer or a member of the consumer's family.

2. The provision of health care to the consumer.

3. Payment for the provision of health care to the consumer.

(10) "Publicly available information" means information that a licensee has a reasonable basis to believe is lawfully made available to the general public from

federal, state, or local government records, widely distributed media, or disclosures required by federal, state, or local law.

(11) "Third–party service provider" means a person other than a licensee who contracts with a licensee to maintain, process, or store nonpublic information or is otherwise permitted access to nonpublic information through its provision of services to the licensee.

SECTION 4. 601.951 of the statutes is created to read:

601.951 General provisions. **(1)** EXCLUSIVE STATE STANDARDS. This subchapter establishes the exclusive state standards applicable to licensees for data security, the investigation of a cybersecurity event, and notification of a cybersecurity event to the commissioner.

(2) EXCEPTIONS TO APPLICABILITY. (a) This subchapter does not apply to a person who is an employee, agent, representative, or designee of a licensee and who is also a licensee to the extent that the person is covered by the information security program of the other licensee and the other licensee has complied with this subchapter on behalf of the person.

(b) A licensee affiliated with a depository institution that maintains an information security program in compliance with the interagency guidelines establishing information security standards as set forth pursuant to 15 USC 6801 and 6805 shall be considered to meet the requirements of this subchapter, provided that the licensee produces, upon request of the commissioner, documentation satisfactory to the commissioner that independently validates the adoption by the affiliated depository institution of an information security program that satisfies the interagency guidelines.

(c) This subchapter, except for s. 601.954 (1), does not apply to a licensee who is subject to and governed by 45 CFR Parts 160 and 164 and who maintains nonpublic information in the same manner as protected health information under 45 CFR Parts 160 and 164.

(d) If a licensee ceases to qualify for an exception under par. (a) to (c), the licensee shall have 180 days to comply with this subchapter.

(3) AGREEMENTS BETWEEN PARTIES. Nothing in this subchapter shall prevent or abrogate an agreement between a licensee and another licensee, a 3rd–party service provider, or another party to fulfill any of the requirements under s. 601.953 or 601.954.

(4) PRIVATE CAUSE OF ACTION. This subchapter may not be construed to create or imply a private cause of action for violation of its provisions or to curtail a private cause of action that otherwise exists in the absence of this subchapter.

(5) RULES. The commissioner may promulgate rules that are necessary to carry out the provisions of this subchapter.

SECTION 5. 601.952 of the statutes is created to read:

601.952 Information security program. **(1)** IMPLEMENTATION OF PROGRAM. No later than one year after the effective date of this subsection .... [LRB inserts date], a licensee shall develop, implement, and maintain a comprehensive written information security program based on the licensee's risk assessment under sub. (2) and consistent with the conditions of sub. (3) (a). The program shall contain administrative, technical, and physical safeguards for the protection of the licensee's information systems and nonpublic information. The licensee shall design the program to do all of the following:

(a) Protect against threats and hazards to the security and integrity of the information systems and nonpublic information.

(b) Protect against unauthorized access to and use of nonpublic information and minimize the likelihood of harm to a consumer from the unauthorized access or use.

(c) Establish and periodically reevaluate a schedule for retention and disposal of nonpublic information and establish a mechanism for the destruction of nonpublic information that is no longer needed.

(2) RISK ASSESSMENT. The licensee shall conduct a risk assessment under which the licensee shall do all of the following:

(a) Identify reasonably foreseeable internal and external threats that could result in unauthorized access to or transmission, disclosure, misuse, alteration, or destruction of nonpublic information, including nonpublic information that is accessible to or held by 3rd–party service providers of the licensee.

(b) Assess the likelihood and potential damage of the threats identified under par. (a), taking into consideration the sensitivity of the nonpublic information.

(c) Assess the sufficiency of policies, procedures, information systems, and other safeguards to manage the threats identified under par. (a) in each relevant area of the licensee's operations, including all of the following:

1. Employee training and management.

2. Information systems, including the classification, governance, processing, storage, transmission, and disposal of information.

3. Processes for detecting, preventing, and responding to attacks, intrusions, and other system failures.

(3) RISK MANAGEMENT. Based on the risk assessment under sub. (2), the licensee shall do all of the following:

(a) Design an information security program to mitigate the identified threats, commensurate with the size and complexity of the licensee, the nature and scope of the licensee's activities, including its use of 3rd–party service providers, and the sensitivity of the nonpublic information.

(b) Implement the following security measures, as appropriate:

1. Place access controls on information systems.

2. Identify and manage the data, personnel, devices, systems, and facilities that enable the licensee to achieve its business purposes, taking into consideration the relative importance of the data, personnel, devices, systems, and facilities to the business objectives and risk strategy of the licensee.

3. Restrict physical access to nonpublic information to authorized individuals only.

4. Protect, by encryption or other means, nonpublic information being transmitted over an external network and nonpublic information stored on a portable computer or storage device or media.

5. Adopt secure development practices for applications that are developed in–house and utilized by the licensee.

6. Modify information systems in accordance with the licensee's information security program.

7. Utilize effective controls, which may include multifactor authentication procedures for employees accessing nonpublic information.

8. Implement regular testing and monitoring of systems and procedures to detect actual and attempted attacks on, or intrusions into, an information system.

9. Include audit trails within the information security program that are designed to detect and respond to cybersecurity events and to reconstruct material financial transactions sufficient to support the normal operations and obligations of the licensee.

10. Implement measures to protect against the destruction, loss, or damage of nonpublic information due to environmental hazards, natural and other disasters, and technological failures.

11. Develop, implement, and maintain practices for the secure disposal of nonpublic information in all formats.

(c) Designate at least one employee, affiliate, or outside vendor as responsible for the information security program.

(d) Stay informed regarding emerging threats and vulnerabilities and implement safeguards to manage the threats and vulnerabilities.

(e) No less than annually, assess the effectiveness of security safeguards, including key controls, systems, and procedures.

(f) Include cybersecurity risks in the licensee's enterprise risk management process.

(g) Utilize reasonable security measures when sharing information, taking into consideration the character of the sharing and the type of information shared.

(h) Provide personnel with cybersecurity awareness training that is updated as necessary.

(4) PROGRAM ADJUSTMENTS. The licensee shall monitor, evaluate, and adjust the information security program under sub. (1) consistent with changes in technology, the sensitivity of the nonpublic information, internal and external threats to nonpublic information, and changes to the licensee's business operations,

outsourcing arrangements, and information systems. If a licensee identifies areas, systems, or processes that require material improvement, updating, or redesign, the insurer shall document the identification and remedial efforts to address the areas, systems, or processes. The licensee shall maintain the documentation for a period of at least 5 years starting from the date the documentation was created and shall produce the documentation upon demand of the commissioner.

(5) INCIDENT RESPONSE PLAN. As part of its information security program, a licensee shall develop an incident response plan to promptly respond to, and recover from, a cybersecurity event that compromises the confidentiality, integrity, or availability of nonpublic information, the licensee's information systems, or the continuing functionality of any aspect of the licensee's business or operations. The incident response plan shall be in writing and address all of the following:

(a) The goals of the incident response plan.

(b) The internal process for responding to a cybersecurity event.

(c) The identification of clear roles, responsibilities, and levels of decision–making authority during and immediately following a cybersecurity event.

(d) The external and internal communications and information sharing during and immediately following a cybersecurity event.

(e) Requirements for the remediation of identified weaknesses in the information systems and associated controls.

(f) The reporting and documentation of a cybersecurity event and related incident response activities.

(g) The evaluation and revision of the incident response plan following a cybersecurity event.

(6) OVERSIGHT OF 3RD–PARTY SERVICE PROVIDER ARRANGEMENTS. No later than 2 years after the effective date of this subsection .... [LRB inserts date], a licensee shall exercise due diligence in selecting a 3rd–party service provider. The licensee shall make reasonable efforts to require a 3rd–party service provider to do all of the following:

(a) 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 3rd–party service provider.

(b) Report a cybersecurity event under s. 601.954.

(7) OVERSIGHT BY BOARD OF DIRECTORS. If a licensee has a board of directors, the board or an appropriate committee of the board shall, at a minimum, do all of the following:

(a) Require the licensee's executive management to develop, implement, and maintain the information security program under sub. (1).

(b) Oversee the development, implementation, and maintenance of the information security program.

(c) Require the licensee's executive management to report, at least annually, all of the following information to the board:

1. The overall status of the information security program and the licensee's compliance with this subchapter.

2. Material matters relating to the information security program, including issues relating to risk assessment, risk management and control decisions, 3rd–party service provider arrangements, and security testing.

3. Recommendations for modifications to the information security program.

(8) ANNUAL CERTIFICATION TO COMMISSIONER. Beginning in the year that is 2 years after the effective date of this subsection .... [LRB inserts date], a licensee who is domiciled in this state shall annually submit, no later than March 1, to the commissioner a written certification that the licensee is in compliance with the requirements of this section. The licensee shall maintain all records, schedules, and data supporting the certification for a period of at least 5 years and shall produce the records, schedules, and data upon demand of the commissioner.

(9) EXEMPTIONS. (a) This section does not apply to a licensee who meets any of the following criteria:

1. Has less than $10,000,000 in year–end total assets.

2. Has less than $5,000,000 in gross annual revenue.

3. Has fewer than 25 employees, including independent contractors, who work at least 30 hours a week for the licensee.

(b) The commissioner may issue an order to a licensee who is otherwise exempt under par. (a) to comply with this section if the commissioner determines that the order is warranted by the licensee's unique circumstances.

(c) A licensee who ceases to qualify for the exemption under par. (a) or who receives an order under par. (b) shall comply with this section no later than 180 days after the date the licensee ceases to qualify or receives the order.

SECTION 6. 601.953 of the statutes is created to read:

601.953 Investigation of cybersecurity event. **(1)** If a licensee learns that a cybersecurity event involving the licensee's information systems or nonpublic information has or may have occurred, the licensee, or an outside vendor or service provider designated to act on behalf of the licensee, shall conduct a prompt investigation that, at a minimum, includes all of the following:

(a) An assessment of the nature and scope of the cybersecurity event.

(b) The identification of any nonpublic information that was or may have been involved in the cybersecurity event.

(c) The performance of reasonable measures to restore the security of the licensee's information systems compromised in the cybersecurity event and prevent additional unauthorized acquisition, release, or use of nonpublic information.

(2) If a licensee knows that a cybersecurity event has or may have occurred in an information system maintained by a 3rd–party service provider, the licensee shall comply with sub. (1) or make reasonable efforts to confirm and document that the 3rd–party service provider has either complied with sub. (1) or failed to cooperate with the investigation under sub. (1).

(3) The licensee shall maintain records concerning a cybersecurity event for a period of at least 5 years starting from the date of the cybersecurity event and shall produce the records upon demand of the commissioner.

SECTION 7. 601.954 of the statutes is created to read:

601.954 Notification of a cybersecurity event. (1) NOTIFICATION TO THE COMMISSIONER. (a) 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) NOTICE TO CONSUMERS AND PRODUCERS OF RECORD. A licensee required to notify the commissioner under sub. (1) shall comply with s. 134.98, if applicable, and provide to the commissioner a copy of any notice sent under s. 134.98 (2). 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 affected by the cybersecurity event no later than the date at which notice is provided under s. 134.98, 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 an information system maintained by a 3rd–party service provider, 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 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 consumers affected by the cybersecurity event shall 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 and, if applicable, the requirements under s. 134.98.

SECTION 8. 601.955 of the statutes is created to read:

601.955 Confidentiality. (1) All of the following apply to documents, materials, and other information in the possession or control of the commissioner that are obtained by, created by, or disclosed to the commissioner or any other person under this subchapter:

(a) The documents, materials, and other information are considered proprietary and contain trade secrets.

(b) The documents, materials, and other information are confidential and privileged, and the privilege may not be constructively waived.

(c) The documents, materials, and other information are not open to inspection or copying under s. 19.35 (1).

(d) The documents, materials, and other information are not subject to subpoena or discovery and are not admissible as evidence in a private civil action.

(e) The commissioner may use the documents, materials, and other information in the furtherance of any regulatory or legal action brought as a part of the commissioner's official duties.

(f) The commissioner may not make the documents, materials, or other information public without first obtaining written consent of the licensee.

(g) Neither the commissioner nor any person who received the documents, materials, or other information may testify or be required to testify in any private civil action regarding the documents, materials, or other information.

(2) Notwithstanding sub. (1), the commissioner may share, upon request, the documents, materials, or other information with other state, federal, and international financial regulatory agencies if the recipient agrees in writing to maintain the confidentiality and privileged status of the documents, materials, or other information and has verified that it has the legal authority to maintain confidentiality. The commissioner may receive documents, materials, or other information related to this subchapter from other state, federal, and international financial regulatory agencies and shall maintain as confidential or privileged any documents, materials, or other information that is treated as confidential or privileged under the laws of the jurisdiction that is the source of the documents, materials, or other information. The sharing of documents under this subsection does not constitute a delegation of regulatory authority and does not act as a waiver of privilege.

(3) Notwithstanding sub. (1), the commissioner may share the documents, materials, or other information under this section with a 3rd–party consultant or

vendor if the consultant or vendor agrees in writing to maintain the confidentiality and privileged status of the documents, materials, and other information shared under this section.

(4) Nothing in this subchapter prohibits the commissioner from releasing final, adjudicated actions that are open to public inspection to a database or other clearinghouse service maintained by the National Association of Insurance Commissioners, its affiliates, or subsidiaries.

SECTION 9. 601.956 of the statutes is created to read:

601.956 Enforcement. The commissioner shall have the power to examine and investigate the affairs of any licensee to determine whether the licensee has engaged in conduct in violation of this subchapter and to take action that is necessary or appropriate to enforce the provisions of this subchapter. This power is in addition to the powers that the commissioner has under subch. IV of this chapter. An investigation or examination under this section shall be conducted under subchs. IV and V of this chapter.

SECTION 10. Effective date.

(1) This act takes effect on the first day of the 4th month beginning after publication.

(END)