

SENATE BILL NO. 2075

Introduced by

Industry, Business and Labor Committee

(At the request of the Insurance Commissioner)

1 A BILL ~~for an Act to amend and reenact section 26.1-02-33 of the North Dakota Century Code,~~
2 ~~relating to third-party software access to insurance policy information.~~ for an Act to create and
3 enact chapter 26.1-02.2 of the North Dakota Century Code, relating to insurance data and
4 security; and to provide for a legislative management study.

5 **BE IT ENACTED BY THE LEGISLATIVE ASSEMBLY OF NORTH DAKOTA:**

6 ~~— **SECTION 1. AMENDMENT.** Section 26.1-02-33 of the North Dakota Century Code is~~
7 ~~amended and reenacted as follows:~~

8 ~~— **26.1-02-33. Posting policy on internet.**~~

9 ~~— 1. An insurance policy and an endorsement that does not contain personally identifiable~~
10 ~~information may be mailed, delivered, or posted on the insurer's website. If the insurer~~
11 ~~elects to post an insurance policy and an endorsement on the insurer's website in lieu~~
12 ~~of mailing or delivering the policy and endorsement to the insured, the insurer shall~~
13 ~~comply with the following conditions:~~

14 ~~— a. The policy and an endorsement must be accessible to the insured and producer~~
15 ~~of record and remain that way while the policy is in force;~~

16 ~~— b. After the expiration of the policy, the insurer shall archive the expired policy and~~
17 ~~endorsement for a period of five years or other period required by law, and make~~
18 ~~the policy and endorsement available upon request;~~

19 ~~— c. The policy and endorsement must be posted in a manner that enables the~~
20 ~~insured and producer of record to print and save the policy and endorsement~~
21 ~~using a program or application that is widely available on the internet and free to~~
22 ~~use;~~

1 ~~_____ d. The insurer shall provide the following information in, or simultaneous with, each~~
2 ~~declaration page provided at the time of issuance of the initial policy and any~~
3 ~~renewals of the policy:~~

4 ~~_____ (1) A description of the exact policy and endorsement form purchased by the~~
5 ~~insured;~~

6 ~~_____ (2) A description of the insured's right to receive, upon request and without~~
7 ~~charge, a paper copy of the policy and endorsement by mail; and~~

8 ~~_____ (3) The internet address at which the policy and endorsement are posted;~~

9 ~~_____ e. The insurer, upon an insured's request and without charge, shall mail a paper~~
10 ~~copy of the policy and endorsement to the insured; and~~

11 ~~_____ f. The insurer shall provide notice, in the format preferred by the insured, of any~~
12 ~~change to the forms or endorsement; the insured's right to obtain, upon request~~
13 ~~and without charge, a paper copy of the forms or endorsement; and the internet~~
14 ~~address at which the forms or endorsement are posted.~~

15 ~~_____ 2. If the insurer provides the insured access to policy, endorsement, or other policy-~~
16 ~~related information by electronic means, the insurer may not restrict the insured from~~
17 ~~using third party software to access policy, endorsement, or other policy-related~~
18 ~~information. This subsection does not:~~

19 ~~_____ a. Prohibit an insurer from preventing access by malicious software; or~~

20 ~~_____ b. Require an insurer to provide policy information by electronic means.~~

21 ~~_____ 3. This section does not affect the timing or content of any disclosure or document~~
22 ~~required to be provided or made available to any insured under applicable law.~~

23 **SECTION 1.** Chapter 26.1-02.2 of the North Dakota Century Code is created and enacted
24 as follows:

25 **26.1-02.2-01 Definitions.**

26 **As used in this chapter:**

27 **1. "Authorized individual" means an individual known to and screened by the licensee**
28 **and determined to be necessary and appropriate to have access to the nonpublic**
29 **information held by the licensee and the licensee's information systems.**

30 **2. "Commissioner" means the insurance commissioner.**

- 1 3. "Consumer" means an individual, including an applicant, policyholder, insured,
2 beneficiary, claimant, and certificate holder, who is a resident of this state and whose
3 nonpublic information is in a licensee's possession, custody, or control.
- 4 4. "Cybersecurity event" means an event resulting in unauthorized access to, disruption,
5 or misuse of, an information system or nonpublic information stored on the information
6 system. The term does not include:
- 7 a. The unauthorized acquisition of encrypted nonpublic information if the encryption,
8 process, or key is not also acquired, released, or used without authorization; or
- 9 b. An event the licensee has determined that the nonpublic information accessed by
10 an unauthorized person has not been used or released and has been returned or
11 destroyed.
- 12 5. "Department" means the insurance department.
- 13 6. "Encrypted" means the transformation of data into a form that results in a low
14 probability of assigning meaning without the use of a protective process or key.
- 15 7. "Information security program" means the administrative, technical, and physical
16 safeguards a licensee uses to access, collect, distribute, process, protect, store, use,
17 transmit, dispose of, or otherwise handle nonpublic information.
- 18 8. "Information system" means a discrete set of electronic information resources
19 organized for the collection, processing, maintenance, use, sharing, dissemination, or
20 disposition of electronic nonpublic information, as well as any specialized system,
21 including industrial or process controls systems, telephone switching, private branch
22 exchange systems, and environmental control systems.
- 23 9. "Licensee" means any person licensed, authorized to operate, registered, or required
24 to be licensed, authorized, or registered pursuant to the insurance laws of this state.
25 The term does not include a purchasing group or a risk retention group chartered and
26 licensed in another state or a licensee that is acting as an assuming insurer that is
27 domiciled in another state or jurisdiction.
- 28 10. "Multi-factor authentication" means authentication through verification of at least two of
29 the following types of authentication factors:
- 30 a. Knowledge factors, including a password;
- 31 b. Possession factors, including a token or text message on a mobile phone; or

1 c. Inherence factors, including a biometric characteristic.

2 11. "Nonpublic information" means electronic information that is not publicly available
3 information and is:

4 a. Any information concerning a consumer which can be used to identify the
5 consumer because of name, number, personal mark, or other identifier in
6 combination with any one or more of the following data elements:

7 (1) Social security number;

8 (2) Driver's license number or nondriver identification card number;

9 (3) Financial account number or credit or debit card number;

10 (4) Any security code, access code, or password that would permit access to a
11 consumer's financial account; or

12 (5) Biometric records.

13 b. Any information or data, except age or gender, in any form or medium created by
14 or derived from a health care provider or a consumer which can be used to
15 identify a particular consumer and relates to:

16 (1) The past, present, or future physical, mental, or behavioral health or
17 condition of any consumer or a member of the consumer's family;

18 (2) The provision of health care to any consumer; or

19 (3) Payment for the provision of health care to any consumer.

20 12. "Person" means any individual or any nongovernmental entity, including any
21 nongovernmental partnership, corporation, branch, agency, or association.

22 13. "Publicly available information" means any information a licensee has a reasonable
23 basis to believe is lawfully made available to the general public from: federal, state, or
24 local government records; widely distributed media; or disclosures to the general
25 public which are required to be made by federal, state, or local law. A licensee has a
26 reasonable basis to believe that information is lawfully made available to the general
27 public if the licensee has taken steps to determine:

28 a. The information is of the type available to the general public; and

29 b. Whether a consumer can direct the information not be made available to the
30 general public and, if so, that the consumer has not done so.

1 14. "Risk assessment" means the risk assessment that each licensee is required to
2 conduct under section 26.1-02.2-03.

3 15. "Third-party service provider" means a person, not otherwise defined as a licensee,
4 that contracts with a licensee to maintain, process, store, or otherwise is permitted
5 access to nonpublic information through its provision of services to the licensee.

6 **26.1-02.2-02. Exclusive regulation.**

7 Notwithstanding any other provision of law, this chapter establishes the exclusive state
8 standards applicable to licensees for data security, the investigation of a cybersecurity event,
9 and notification to the commissioner.

10 **26.1-02.2-03. Information security program.**

11 1. Commensurate with the size and complexity of the licensee, the nature and scope of
12 the licensee's activities, including the licensee's use of third-party service providers,
13 and the sensitivity of the nonpublic information used by the licensee or in the
14 licensee's possession, custody, or control, each licensee shall develop, implement,
15 and maintain a comprehensive written information security program based on the
16 licensee's risk assessment that contains administrative, technical, and physical
17 safeguards for the protection of nonpublic information and the licensee's information
18 system.

19 2. A licensee's information security program must be designed to:

20 a. Protect the security and confidentiality of nonpublic information and the security
21 of the information system;

22 b. Protect against any threats or hazards to the security or integrity of nonpublic
23 information and the information system;

24 c. Protect against unauthorized access to or use of nonpublic information, and
25 minimize the likelihood of harm to any consumer; and

26 d. Define and periodically re-evaluate a schedule for retention of nonpublic
27 information and a mechanism for destruction if no longer needed.

28 3. The licensee shall:

29 a. Designate one or more employees, an affiliate, or an outside vendor designated
30 to act on behalf of the licensee which is responsible for the information security
31 program;

1 b. Identify reasonably foreseeable internal or external threats that could result in
2 unauthorized access, transmission, disclosure, misuse, alteration, or destruction
3 of nonpublic information, including the security of information systems and
4 nonpublic information accessible to, or held by, third-party service providers;

5 c. Assess the likelihood and potential damage of any threats, taking into
6 consideration the sensitivity of the nonpublic information;

7 d. Assess the sufficiency of policies, procedures, information systems, and other
8 safeguards in place to manage any threats, including consideration of threats in
9 each relevant area of the licensee's operations, including:

10 (1) Employee training and management;

11 (2) Information systems, including network and software design, as well as
12 information classification, governance, processing, storage, transmission,
13 and disposal; and

14 (3) Detecting, preventing, and responding to attacks, intrusions, or other
15 systems failures; and

16 e. Implement information safeguards to manage the threats identified in the
17 licensee's ongoing assessment and assess the effectiveness of the safeguards'
18 key controls, systems, and procedures on an annual basis.

19 4. Based on the licensee's risk assessment, the licensee shall:

20 a. Design the information security program to mitigate the identified risks,
21 commensurate with the size and complexity of the licensee, the nature and scope
22 of the licensee's activities, including the licensee's use of third-party service
23 providers, and the sensitivity of the nonpublic information used by the licensee or
24 in the licensee's possession, custody, or control.

25 b. Determine which security measures as provided under this subdivision are
26 appropriate and implement the security measures:

27 (1) Place access controls on information systems, including controls to
28 authenticate and permit access only to an authorized individual to protect
29 against the unauthorized acquisition of nonpublic information;

30 (2) Identify and manage the data, personnel, devices, systems, and facilities
31 that enable the organization to achieve business purposes in accordance

- 1 with the business' relative importance to business objectives and the
2 organization's risk strategy;
- 3 (3) Restrict physical access to nonpublic information only to an authorized
4 individual;
- 5 (4) Protect by encryption or other appropriate means, all nonpublic information
6 while being transmitted over an external network and all nonpublic
7 information stored on a laptop computer or other portable computing or
8 storage device or media;
- 9 (5) Adopt secure development practices for in-house developed applications
10 utilized by the licensee;
- 11 (6) Modify the information system in accordance with the licensee's information
12 security program;
- 13 (7) Utilize effective controls, which may include multi-factor authentication
14 procedures for employees accessing nonpublic information;
- 15 (8) Regularly test and monitor systems and procedures to detect actual and
16 attempted attacks on, or intrusions into, information systems;
- 17 (9) Include audit trails within the information security program designed to
18 detect and respond to cybersecurity events and designed to reconstruct
19 material financial transactions sufficient to support normal operations and
20 obligations of the licensee;
- 21 (10) Implement measures to protect against destruction, loss, or damage of
22 nonpublic information due to environmental hazards, including fire and
23 water damage or other catastrophes or technological failures; and
- 24 (11) Develop, implement, and maintain procedures for the secure disposal of
25 nonpublic information in any format.
- 26 c. Include cybersecurity risks in the licensee's enterprise risk management process.
27 d. Stay informed regarding emerging threats or vulnerabilities and use reasonable
28 security measures if sharing information relative to the character of the sharing
29 and the type of information shared; and

1 e. Provide cybersecurity awareness training to the licensee's personnel which is
2 updated as necessary to reflect risks identified by the licensee in the risk
3 assessment.

4 5. If the licensee has a board of directors, the board or an appropriate committee of the
5 board shall:

6 a. Require the licensee's executive management or the licensee's delegates to
7 develop, implement, and maintain the licensee's information security program;

8 b. Require the licensee's executive management or the licensee's delegates to
9 report the following information in writing on an annual basis:

10 (1) The overall status of the information security program and the licensee's
11 compliance with the provisions of this chapter; and

12 (2) Material matters related to the information security program, addressing
13 issues, including risk assessment, risk management and control decisions,
14 third-party service provider arrangements, results of testing, cybersecurity
15 events, or violations, and management's responses and recommendations
16 for changes in the information security program.

17 c. If executive management delegates any responsibilities under this section, the
18 executive management delegates shall oversee the development,
19 implementation, and maintenance of the licensee's information security program
20 prepared by the delegate and shall receive a report from the delegate complying
21 with the requirements of the report to the board of directors.

22 6. A licensee shall exercise due diligence in selecting its third-party service provider; and
23 a licensee shall require a third-party service provider to implement appropriate
24 administrative, technical, and physical measures to protect and secure the information
25 systems and nonpublic information accessible to, or held by, the third-party service
26 provider.

27 7. The licensee shall monitor, evaluate, and adjust, as appropriate, the information
28 security program consistent with any relevant changes in technology, the sensitivity of
29 its nonpublic information, internal or external threats to information, and the licensee's
30 own changing business arrangements, including mergers and acquisitions, alliances
31 and joint ventures, outsourcing arrangements, and changes to information systems.

1 8. As part of the licensee's information security program, a licensee shall establish a
2 written incident response plan designed to promptly respond to, and recover from, any
3 cybersecurity event that compromises the confidentiality, integrity, or availability of
4 nonpublic information in the licensee's possession. The incident response plan must
5 include the licensee's plan to recover the licensee's information systems and restore
6 continuous functionality of any aspect of the licensee's business or operations.

7 9. A licensee's incident response plan must address:

8 (1) The internal process for responding to a cybersecurity event;

9 (2) The goals of the incident response plan;

10 (3) The definition of clear roles, responsibilities, and levels of decisionmaking
11 authority;

12 (4) External and internal communications and information sharing;

13 (5) Identification of requirements for the remediation of any identified
14 weaknesses in information systems and associated controls;

15 (6) Documentation and reporting regarding cybersecurity events and related
16 incident response activities; and

17 (7) The evaluation and revision as necessary of the incident response plan
18 following a cybersecurity event.

19 10. Annually, an insurer domiciled in this state shall submit to the commissioner, a written
20 statement by April fifteenth, certifying the insurer is in compliance with the
21 requirements set forth in this section. An insurer shall maintain for examination by the
22 department all records, schedules, and data supporting this certificate for a period of
23 five years. To the extent an insurer has identified areas, systems, or processes that
24 require material improvement, updating, or redesign, the insurer shall document the
25 identification and the remedial efforts planned and underway to address the areas,
26 systems, or processes. The documentation must be available for inspection by the
27 commissioner.

28 **26.1-02.2-04. Investigation of a cybersecurity event.**

29 1. If a licensee learns a cybersecurity event has or may have occurred, the licensee, an
30 outside vendor, or service provider designated to act on behalf of the licensee, shall
31 conduct a prompt investigation.

1 2. During the investigation, the licensee or an outside vendor or service provider
2 designated to act on behalf of the licensee, shall:

3 a. Determine whether a cybersecurity event has occurred;

4 b. Assess the nature and scope of the cybersecurity event;

5 c. Identify any nonpublic information that may have been involved in the
6 cybersecurity event; and

7 d. Perform or oversee reasonable measures to restore the security of the
8 information systems compromised in the cybersecurity event in order to prevent
9 further unauthorized acquisition, release, or use of nonpublic information in the
10 licensee's possession, custody, or control.

11 3. If a licensee learns a cybersecurity event has or may have occurred in a system
12 maintained by a third-party service provider, the licensee shall complete the
13 requirements provided under subsection 2 or confirm and document that the
14 third-party service provider has completed the requirements.

15 4. The licensee shall maintain records concerning all cybersecurity events for a period of
16 at least five years from the date of the cybersecurity event and shall produce the
17 records upon demand of the commissioner.

18 **26.1-02.2-05. Notification of a cybersecurity event.**

19 1. A licensee shall notify the commissioner as promptly as possible, but no later than
20 three business days from a determination that a cybersecurity event involving
21 nonpublic information that is in the possession of a licensee has occurred if:

22 a. This state is the licensee's state of domicile, in the case of an insurer, or this state
23 is the licensee's home state, in the case of a producer as defined in chapter
24 26.1-26, and the cybersecurity event has a reasonable likelihood of materially
25 harming a consumer residing in this state or reasonable likelihood of materially
26 harming any material part of the normal operations of the licensee; or

27 b. The licensee reasonably believes the nonpublic information involved is of two
28 hundred fifty or more consumers residing in this state and is:

29 (1) A cybersecurity event impacting the licensee for which notice is required to
30 be provided to any government body, self-regulatory agency, or any other
31 supervisory body pursuant to any state or federal law; or

1 (2) A cybersecurity event that has a reasonable likelihood of materially harming
2 any consumer residing in this state or materially harming any part of the
3 normal operations of the licensee.

4 2. The licensee shall provide the notice required under this section in electronic form as
5 directed by the commissioner. The licensee shall update and supplement the initial
6 and any subsequent notifications to the commissioner regarding material changes to
7 previously provided information relating to the cybersecurity event. The licensee's
8 notice required under this section must include:

9 a. The date of the cybersecurity event;

10 b. Description of how the information was exposed, lost, stolen, or breached,
11 including the specific roles and responsibilities of third-party service providers, if
12 any;

13 c. How the cybersecurity event was discovered;

14 d. Whether any lost, stolen, or breached information has been recovered and if so,
15 how;

16 e. The identity of the source of the cybersecurity event;

17 f. Whether the licensee has filed a police report or has notified any regulatory,
18 government, or law enforcement agencies and, if so, when the notification was
19 provided;

20 g. Description of the specific types of information acquired without authorization.
21 Specific types of information means particular data elements, including medical
22 information, financial information, or any other information allowing identification
23 of the consumer;

24 h. The period during which the information system was compromised by the
25 cybersecurity event;

26 i. The total number of consumers in this state affected by the cybersecurity event.
27 The licensee shall provide the best estimate in the initial report to the
28 commissioner and update the estimate with a subsequent report to the
29 commissioner pursuant to this section;

1 j. The results of any internal review identifying a lapse in either automated controls
2 or internal procedures, or confirming that all automated controls or internal
3 procedures were followed;

4 k. Description of efforts being undertaken to remediate the situation that permitted
5 the cybersecurity event to occur;

6 l. A copy of the licensee's privacy policy and a statement outlining the steps the
7 licensee will take to investigate and notify consumers affected by the
8 cybersecurity event; and

9 m. Name of a contact person that is both familiar with the cybersecurity event and
10 authorized to act for the licensee.

11 3. The licensee shall comply with chapter 51-30, as applicable, and provide a copy of the
12 notice sent to consumers to the commissioner, when a licensee is required to notify
13 the commissioner under subsection 1.

14 4. In the case of a cybersecurity event in a system maintained by a third-party service
15 provider, of which the licensee has become aware, the licensee shall treat the event in
16 accordance with subsection 1 unless the third-party service provider provides the
17 notice required under chapter 26.1-02.2 to the commissioner.

18 a. The computation of licensee's deadlines under this subsection begin on the day
19 after the third-party service provider notifies the licensee of the cybersecurity
20 event or the licensee otherwise has actual knowledge of the cybersecurity event,
21 whichever is sooner.

22 b. Nothing in this chapter prevents or abrogates an agreement between a licensee
23 and another licensee, a third-party service provider, or any other party to fulfill
24 any of the investigation requirements imposed under section 26.1-02.2-04 or
25 notice requirements imposed under subsection 1.

26 5. If a cybersecurity event involving nonpublic information that is used by a licensee that
27 is acting as an assuming insurer or in the possession, custody, or control of a licensee
28 that is acting as an assuming insurer and that does not have a direct contractual
29 relationship with the affected consumers, the assuming insurer shall notify the
30 insurer's affected ceding insurers and the commissioner of the insurer's state of

1 domicile within three business days of making the determination that a cybersecurity
2 event has occurred.

3 6. The ceding insurer that has a direct contractual relationship with affected consumers
4 shall fulfill the consumer notification requirements imposed under chapter 51-30 and
5 any other notification requirements relating to a cybersecurity event imposed under
6 subsection 1.

7 7. If a cybersecurity event involving nonpublic information that is in the possession,
8 custody, or control of a third-party service provider of a licensee that is an assuming
9 insurer, the assuming insurer shall notify the insurer's affected ceding insurers and the
10 commissioner of the insurer's state of domicile within three business days of receiving
11 notice from its third-party service provider that a cybersecurity event has occurred.

12 8. The ceding insurers that have a direct contractual relationship with affected
13 consumers shall fulfill the consumer notification requirements imposed under chapter
14 51-30 and any other notification requirements relating to a cybersecurity event
15 imposed under subsection 1.

16 9. Any licensee acting as assuming insurer does not have any other notice obligations
17 relating to a cybersecurity event or other data breach under this section or any other
18 law of this state.

19 10. If a cybersecurity event involving nonpublic information that is in the possession,
20 custody, or control of a licensee that is an insurer or the insurer's third-party service
21 provider for which a consumer accessed the insurer's services through an
22 independent insurance producer, and for which consumer notice is required by chapter
23 51-30, the insurer shall notify the producers of record of all affected consumers of the
24 cybersecurity event no later than the time at which notice is provided to the affected
25 consumers. The insurer is excused from the obligation imposed under this subsection
26 for any producers that are not authorized by law or contract to sell, solicit, or negotiate
27 on behalf of the insurer, and those instances in which the insurer does not have the
28 current producer of record information for an individual consumer.

29 **26.1-02.2-06. Power of commissioner.**

30 1. The commissioner may examine and investigate the affairs of any licensee to
31 determine whether the licensee has been or is engaged in any conduct in violation of

1 this chapter. This power is in addition to the powers the commissioner has under
2 chapter 26.1-03. Any investigation or examination must be conducted pursuant to
3 chapter 26.1-03.

4 2. If the commissioner has reason to believe a licensee has been or is engaged in
5 conduct in this state which violates this chapter, the commissioner may take action
6 that is necessary or appropriate to enforce the provisions of this chapter.

7 **26.1-02.2-07. Confidentiality.**

8 1. Any documents, materials, or other information in the control or possession of the
9 department which are furnished by a licensee, or an employee or agent thereof acting
10 on behalf of a licensee pursuant to this chapter, or that are obtained by the
11 commissioner in an investigation or examination pursuant to section 26.1-02.2-06 are
12 confidential, not subject to chapter 44-04, not subject to subpoena, and are not subject
13 to discovery or admissible in evidence in any private civil action. The commissioner
14 may use the documents, materials, or other information in the furtherance of any
15 regulatory or legal action brought as a part of the commissioner's duties. The
16 commissioner may not otherwise make the documents, materials, or other information
17 public without the prior written consent of the licensee.

18 2. The commissioner or any person that received documents, materials, or other
19 information while acting under the authority of the commissioner may not be permitted
20 or required to testify in any private civil action concerning any confidential documents,
21 materials, or information subject to subsection 1.

22 3. In order to assist in the performance of the commissioner's duties the commissioner:
23 a. May share documents, materials, or other information, including the confidential
24 and privileged documents, materials, or information subject to subsection 1, with
25 other state, federal, and international regulatory agencies, with the national
26 association of insurance commissioners, and with state, federal, and international
27 law enforcement authorities, provided the recipient agrees in writing to maintain
28 the confidentiality and privileged status of the document, material, or other
29 information;
30 b. May receive documents, materials, or information, including otherwise
31 confidential and privileged documents, materials, or information, from the national

1 association of insurance commissioners, and from regulatory and law
2 enforcement officials of other foreign or domestic jurisdictions, and shall maintain
3 as confidential or privileged any document, material, or information received with
4 notice or the understanding that it is confidential or privileged under the laws of
5 the jurisdiction that is the source of the document, material, or information;

6 c. May share documents, materials, or other information subject to this section, with
7 a third-party consultant or vendor provided the consultant agrees in writing to
8 maintain the confidentiality and privileged status of the document, material, or
9 other information; and

10 d. May enter agreements governing sharing and use of information consistent with
11 this subsection.

12 4. A waiver of any applicable privilege or claim of confidentiality in the documents,
13 materials, or information does not occur as a result of disclosure to the commissioner
14 under this section or as a result of sharing as authorized in subsection 3.

15 5. Documents, materials, or other information in the possession or control of the national
16 association of insurance commissioners or a third-party consultant or vendor pursuant
17 to this chapter are confidential, not subject to chapter 44-04, not subject to subpoena,
18 and not subject to discovery or admissible in evidence in any private civil action.

19 **26.1-02.2-08. Exceptions.**

20 1. The following exceptions apply to this chapter:

21 a. A licensee with less than five million dollars in gross revenue or less than ten
22 million dollars in year-end assets is exempt from section 26.1-02.2-03.

23 b. During the period beginning on August 1, 2021, and ending on July 31, 2023, a
24 licensee with fewer than fifty employees, including independent contractors and
25 employees of affiliated companies having access to nonpublic information used
26 by the licensee or in the licensee's possession, custody, or control, is exempt
27 from section 26.1-02.2-03.

28 c. After July 31, 2023, a licensee with fewer than twenty-five employees, including
29 independent contractors and employees of affiliated companies having access to
30 nonpublic information used by the licensee or in the licensee's possession,
31 custody, or control is exempt from section 26.1-02.2-03.

1 d. An employee, agent, representative, or designee of a licensee, that also is a
2 licensee, is exempt from section 26.1-02.2-03 and is not required to develop an
3 information security program to the extent the employee, agent, representative,
4 or designee is covered by the information security program of the other licensee.

5 2. If a licensee ceases to qualify for an exception, the licensee has one hundred eighty
6 days to comply with this chapter.

7 **26.1-02.2-09. Penalties.**

8 In the case of a violation of this chapter, a licensee may be penalized in accordance with
9 section 26.1-01-03.3.

10 **26.1-02.2-10. Rules and regulations.**

11 The commissioner may adopt reasonable rules necessary for the implementation of this
12 chapter.

13 **26.1-02.2-11. Implementation dates.**

14 A licensee shall implement:

15 1. Subsections 1, 2, 3, 4, 5, 8, and 9 of section 26.1-02.2-03 no later than August 1,
16 2022; and

17 2. Subsections 6 and 7 of section 26.1-02.2-03 no later than August 1, 2023.

18 **SECTION 2. LEGISLATIVE MANAGEMENT STUDY - CYBER VULNERABILITIES OF**
19 **ENTITIES LICENSED BY THE INSURANCE DEPARTMENT.** During the 2021-22 interim, the
20 legislative management shall consider, with the assistance of the insurance department,
21 studying the North Dakota laws and practice of insurers making property and casualty
22 insurance policies and related information available to insureds by electronic means; the
23 feasibility and desirability of prohibiting insurers from restricting the conditions in which insureds
24 may access such information, including through software and agents of their choosing; and the
25 extent to which insurers conducting business in this state have sought to limit access to policies
26 and related information made available to insureds, whether such restrictions restrain
27 competition in the marketplace, balance with an analysis of the impact of such access on
28 potential cyber breaches, and loss of trade secret or proprietary information resulting from third-
29 party usage and software applications, and how the two competing considerations can be safely
30 and fairly reconciled. The legislative management shall report its findings and

Sixty-seventh
Legislative Assembly

- 1 recommendations, together with any legislation required to implement the recommendations, to
- 2 the sixty-eighth legislative assembly.