2021 SENATE INDUSTRY, BUSINESS AND LABOR

SB 2075

2021 SENATE STANDING COMMITTEE MINUTES

Industry, Business and Labor Committee
Fort Union Room, State Capitol

SB 2075
1/12/2021

Relating to third-party software access to insurance policy information

Chair Klein opened the hearing at 10:28. All members were present. Senators: Klein, Larsen, Burckhard, Kreun, Marcellais, Vedaa. a.m.

Discussion Topics:

- Allowing for comparisons of policies
- Comparison of policies helping consumers
- Dangers of third party access

Jon Godfread, Insurance Commissioner [10:28] testified in favor and submitted testimony #548.

Kent Blickensderfer, KPB Consulting [10:42] testified in favor and submitted testimony #567.

Chris Oen, NoDak Insurance [10:50] testified in opposition.

Steve Schneider, American Property Casualty Insurance Association [10:55] testified in opposition and submitted testimony #471.

John Ashenfelter, State Farm [10:58] testified in opposition and submitted testimony

#474. **Rob Novland** [11:05] testified in opposition.

Chair Klein closed the hearing at 11:12 a.m.

Gail Stanek, Committee Clerk

SENATE BILL NO. 2075

Presented by: **Jon Godfread**
North Dakota Insurance Commissioner
North Dakota Insurance Department

Before: **Senate Industry, Business and Labor**
Senator Jerry Klein, Chairman

Date: **January 12, 2021**

Good Morning Chairman Klein and members of the committee. My name is Jon Godfread, North Dakota Insurance Commissioner. I appear before you in support of Senate Bill No. 2075.

Before we go over the bill, I wanted to handout some proposed amendments that we have worked on in response to some of the concerns we have heard from the industry.

Also, I want to mention what this bill does NOT do, this bill does not create a new requirement for insurers to implement a new system or new process, it simply clarifies that if you have a system in place you cannot restrict licensed agents or authorized third parties from accessing their clients information on that system.

This bill does NOT prohibit insurers from blocking access to malicious software designed to cause harm, and the determination of what is a potentially malicious software is left up to the insurer to determine.

In our estimation Senate Bill 2075 is a consumer-friendly bill, in that it allows technology and technology companies to assist consumers when they compare and shop for their insurance. As you can imagine, when doing a risk analysis or a comparison of insurance policies very few people read their insurance policies, and even fewer fully understand what is contained in those policies. Technology can help in this area by doing a comparison risk analysis for the consumer (or their agent). The first step in any of this process is to get a copy of the current policy.

Think back 20 years ago, as a consumer when you wanted to shop for insurance what did you have to do? You had to first get a copy of your policy, or at minimum your declaration pages and then take them to an agent or company and get your quotes. This was a cumbersome activity and very few consumers went to this trouble of comparing their policies when shopping for coverage.

When consumers shop for insurance, they obviously want coverages that meet their needs and covers their risk exposures. Getting an apples to apples comparison can be an extremely difficult process. No matter how similar the policies seem, insurance (especially in the property and casualty market) is rarely exactly the same from company to company.

However, with the explosion of technology, a consumer can get a quote faster and can get a better comparison of their coverage. Last session NDCC §26.1-02-33 was introduced as a first step for a faster

comparison and a better consumer experience. NDCC §26.1-02-33, in short allows companies to post their polices for a consumer online. If a consumer wanted to understand their risk or shop for a new policy, they would still have to read the policy and understand it. Furthermore, if a consumer wanted to shop for a different company the consumer would print out their policy and then go to an agent's office to get a comparison quote. Technology has exploded and there are companies that can expedite this process. There are third party companies, that are licensed agents, that have the ability, if given permission by the consumer to go to a company's online portal and find the insurance policy, compare policies and do any kind of risk analysis that is needed.

A few companies have shut down access to these licensed agents or third parties trying to use the online portal. Even though these third parties and licensed agents have received the consumers permission. Some companies have blocked third parties and licensed agents IP addresses completely. This creates an anti-competitive environment. Senate Bill 2075 is a simple change that prohibits a company or insurer from preventing access to these third parties, however it does not impede a prohibition of preventing malicious software. In short, it's letting the good guys in while also keeping the good bad guys out.

Senate Bill 2075 allows for a more competitive market by allowing new technologies to be used.

We understand the concerns that will likely be raised, we can put those concerns into two buckets. First, this is new, and North Dakota would be the first state to prohibit an insurance company from preventing access to an authorized and licensed third-party access to a website. The belief that because something is new it should not be done is understandable but does not hold water in this instance. I serve as the chairman of the Innovation and Technology working group for the National Association of Insurance Commissioners, in that role I have spent a considerable amount of time reviewing how technology and the insurance industry interact, and what if any changes need to be made to more readily adapt to our changing landscape. Put simply, this is some low hanging fruit that can help consumers without putting any additional burden on our insurers.

Secondly, you will likely hear, even with the amendment that it will be impossible to distinguish a good actor from a bad actor. I believe this is blown out of proportion and would give you an example. Currently, a company can restrict access to one of these authorized and licensed services, and if that is done in good faith, that is understandable. However, currently even if the service can contact the company and shown they are not a malicious actor the company may continue blocking their access.

Here is another analogy, right now North Dakota Information Technology (NDIT) blocks certain websites from use from on state

systems, we would all agree this is important. However sometimes these websites really aren't corrupt and may be needed for research or other things. NDIT can be give permission to access these sites if they are provided the address and a reason access it needed.

NDIT would then review, make the determination that the site either is truly harmful or not and if not allow access. The same can be done here with these third parties.

In fact, these third parties have said in the past that they would be willing to write letters to insurance companies, giving them their IP address and stating what they're trying to do. This way the company can grant an access to their online portal.

Again nothing in this bill restricts the company from blocking malicious software or requires them to implement a new system to provide information in an electronic form, it just simply requires that if they do provide that information in an electronic format they cannot restrict access to parties that are authorized and licensed to act on behalf of the consumer.

This issue is important to ensure our consumers are more engaged in their policies and getting the information in the hands of the consumer and their agents to help them make decisions.

Thank you, Mr. Chairman and committee members, I am happy to attempt to answer any questions you might have.

Prepared by the North Dakota
Insurance Department
January 12, 2021

PROPOSED AMENDMENTS TO BILL NO. 2075

Page 2, Line 13, insert "<u>:" after "may not restrict the insured from"</u>

Page 2, Lines 14-17 replace with:

"<u>a. using third-party software to access policy, endorsement, or other policy related information; or</u>

<u>b. delegating the insured's authorization to access policy, endorsement, or other policy-related information using the insured's access credentials.</u>

<u>Nothing in this subsection prohibits an insurer from preventing access by malicious software designed to cause harm to a computer system or network. Nothing in this subsection requires an insurer to provide policy information by electronic means.</u>"

Page 2, line 19, after the period insert:

"**SECTION 2. AMENDMENT. Subsection 10 of Section 26.1-04-03 of the North Dakota Century Code is amended and reenacted as follows:**

10. Unfair handling of communications by insurance company.

<u>a.</u> Failing to adopt and implement reasonable standards for the prompt handling of written communications, primarily expressing grievances, received by the insurance company from insureds or claimants.

b. Restricting access to the policy, endorsements, or policy-related information in violation of section 26.1-02-33(2).”

Renumber accordingly

21.8047.01000

Sixty-seventh
Legislative Assembly
of North Dakota
Introduced by

SENATE BILL NO. 2075

Industry, Business and Labor Committee

(At the request of the Insurance Commissioner)

A BILL for an Act to amend and reenact section 26.1-02-33 of the North Dakota Century Code, relating to third-party software access to insurance policy information.

BE IT ENACTED BY THE LEGISLATIVE ASSEMBLY OF NORTH DAKOTA:

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

26.1-02-33. Posting policy on internet.

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

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

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

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

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

Sixty-seventh
Legislative Assembly

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

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

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

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

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

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

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

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

a. using third-party software to access policy, endorsement, or other policy-related information; or

b. delegating the insured's authorization to access policy, endorsement, or other policy-related information using the insured's access credentials.

Nothing in this subsection prohibits an insurer from preventing access by malicious software designed to cause harm to a computer system or network. Nothing in this subsection requires an insurer to provide policy information by electronic means.

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

SECTION 2. AMENDMENT. Subsection 10 of Section 26.1-04-03 of the North Dakota Century Code is amended and reenacted as follows:

10. Unfair handling of communications by insurance company.

a. Failing to adopt and implement reasonable standards for the prompt handling of written communications, primarily expressing grievances, received by the insurance company from insureds or claimants.

b. Restricting access to the policy, endorsements, or policy-related information in violation of section 26.1-02-33(2).

Testimony of Kent Blickensderfer, KPB Consulting, LLC, on Behalf of Trellis Technologies, Inc.
In Support of Senate Bill 2075

Before the Senate Industry, Business and Labor Committee
January 12, 2021

Chairman Klein and Members of the Committee:

Thank you for the opportunity to appear in support of Senate Bill 2075 on behalf of Trellis Technologies, Inc., a fast-growing insurance software provider and licensed insurance agency in North Dakota and every other state and the District of Columbia.

Trellis provides software that makes it easier for consumers to shop for insurance, easier for insurers to offer compelling insurance products, and easier for licensed agents to advise consumers on insurance decisions. Senate Bill 2075 would amend current law to ensure that consumers, insurers, and agents can use software platforms like Trellis' to obtain and deliver accurate insurance policy quotes.

The insurance market is not easy to navigate. From choosing the right insurer to selecting the right coverage, buying insurance is difficult for North Dakotans just trying to get auto or homeowners' policies at prices they can afford. Traditionally, buying insurance may have required multiple in-person meetings or lengthy telephone calls, filled with all sorts of information about opaque coverage limits and exclusions. It's a yearly or every-couple-of-years experience that none of us likes.

And so it is unsurprising that many consumers want easier ways to buy insurance. They want to be able to buy insurance online and, especially, they want to compare potential policies with their current policies. But consumers are worried that they might unintentionally buy a policy with less coverage, or subscribe to a payment plan that seems cheaper at first glance but costs more over the policy term than their current policies. Insurers and agents who want to sell insurance online likewise need to understand the coverages, exclusions, and premiums of the consumer's existing policy—but that's difficult without seeing the policy documents.

Trellis' platform, which is available to consumers, insurers, and agents, solves this information problem. The platform is straightforward. Most insurers make policy information available to their insureds on online portals. When these consumers want to comparison shop, they connect to their insurance online portals using Trellis' secure platform. Trellis then analyzes the policy information, providing the consumers, their agents, or their prospective insurers with an easy-to-understand summary of the existing policies' coverages, limits, exclusions, and rates. Trellis can also help connect the consumer to other insurers offering comparable policies, and can help the insurer or agent quote an accurate comparison. The platform provides consumers with the confidence that they are actually comparing apples to apples.

Trellis' platform is the internet-equivalent to having a knowledgeable advisor sit next to you as you read your policy documents, helping you understand the policies so that you can make the right decision about comparable insurance products. Trellis further protects consumers in two ways. First, Trellis is a licensed insurance agency in North Dakota, every other U.S. state, and the District of Columbia. Second, Trellis uses bank-grade encryption and the highest possible security measures to maintain consumers' privacy.

Some in the insurance industry, including at least one large national insurer, have embraced the Trellis platform, partnering with Trellis to better sell insurance products over the internet. We also see a tremendous benefit for insurance agents and brokers who can use Trellis to better counsel consumers. Unfortunately, however, a small corner of the national insurance market views Trellis and similar platforms as a competitive threat, trying to prevent consumers from using our platform through technology blocking. (None of these companies include North Dakota's domestic carriers, as far as we know.) It's a common story in any marketplace: as new technology tools develop that help consumers, most in the market embrace them while a small minority put their energies into trying to stop them rather than competing on the merits. Here, the anticompetitive insurers apparently see it as good business to make it harder for consumers to comparison shop. It's anti-consumer and contrary to North Dakota's history of protecting insurance consumers from industry overreach.

Senate Bill 2075 is a common-sense consumer protection amendment. Current law allows but does not require that insurers make insurance policy information available online. The proposed amendment *does not change* current law in this respect—there is and will not be any requirement that insurers make policy information available online. Rather, the proposed amendment provides that *if* an insurer puts policy information online, the insurer cannot go out of its way to stop consumers from using platforms like Trellis to view and analyze their policies.

The proposed amendment does not require that insurers *do* anything. They can still use the same security processes to prevent unauthorized access to their websites, like two-factor authentication or IP-location monitoring. They have no affirmative obligation to verify that the platform is acting on a consumer's behalf; authorization is presumed when the consumer provides their agent or software platform with their individual login credentials. And insurers do not have to allow malicious software designed to damage or hack their computer networks. Far from imposing burdensome obligations on insurers, the proposed amendment imposes no affirmative burdens at all. It's not telling insurers to do *anything*; it's telling them not to block their own policyholders when they're looking to compare alternatives.

The proposed amendment is an important protection for North Dakota consumers, insurers, and agents. It guarantees that insurers cannot use their technological advantages to stop consumers from getting advice about their current policies and comparison shopping for insurance. Like any competitive

marketplace, the insurance market works better for everyone, and especially North Dakota residents, if consumers have the tools that they need to make the right decisions from themselves and their families.

We thank the Commissioner for offering the proposed amendment and his tireless work on behalf of North Dakotans and insurance consumers. We respectfully ask that you give Senate Bill 2075 as amended a do-pass recommendation.

American Property Casualty Insurance Association
INSURING AMERICA apci.org

January 12, 2021

ND Senate Industry, Business and Labor Committee

ND SB 2075

The American Property Casualty Insurance Association (APCIA) is composed of over 1,200 member companies and 330 insurance groups and represents the broadest cross-section of home, auto, and business insurers of any national insurance trade association. In North Dakota, APCIA member insurers provide almost 69 percent of all the insurance purchased by the state's citizens and businesses.

We urge you not to support SB 2075 as it poses information privacy and security questions for regulators and insurers, which we believe cannot be fully answered yet.

Specifically, new subsection 2 [26.1-02-330] eliminates the ability of an insurer to "restrict the insured from using third-party software to access policy, endorsement, or other policy-related information."

Of primary concern to insurers is this provision which seems to guarantee that we must grant access to policy related information to third-parties regardless of their purpose in accessing the information. Perhaps even more important is that these third-parties may pose viral security threats which could undermine insurer's technological capacities by avoiding or evading the insurers' security protocols. Yet insurers would, if this bill became law, ostensibly be proscribed from stopping them.

Are there to be any disclosure obligations or regulation of these third-parties?

Will the Department of Insurance have access to their operational protocols?

Will the Insurance Commissioner be empowered to regulate them?

These are the questions, and they are important ones, for which there do not seem to be ready answers.

Therefore, we ask you to oppose this legislation.

Thank you.

Steve Schneider
Vice President, State Affairs
Midwest Region
APCIA
Steve.schneider@apci.org
312.782.7720

Chairman Klein and members of the Senate Industry, Business and Labor Committee, as associate general counsel who provides legal advice to State Farm Mutual Automobile Insurance and State Farm Fire and Casualty Company on operations, including policyholder accounts and billing/payment information, I appreciate the opportunity to offer the oral testimony in opposition of Senate Bill 2075.

2021 SENATE STANDING COMMITTEE MINUTES

Industry, Business and Labor Committee
Fort Union Room, State Capitol

SB 2075
2/2/2021

relating to third-party software access to insurance policy information

2:15 PM
Chair Klein opened the meeting at 2:16 p.m. All members were present. Senators Klein, Larsen, Burckhard, Vedaa, Kreun, and Marcellais.

Discussion Topics:
- State control and uniformity to security programs
- Cybersecurity

Jon Godfread, Insurance Commissioner discussed proposed amendments 21.8047.01002 [14:16].

Pat Ward, Association of ND Insurers and Member Companies confirmed agreement with amendments 21.8047.01002 to bill [14:34].
Levi Andrist, American Council of Life Insurance testified in support of amendments 21.8047.01002 [14:38].
Steven Becher Exec Director of Insurance Agents of ND testified in support of amendments 21.8047.01002 [14:39].
Kent Blickensderfer testified in opposition [14:43].

Senator Vedaa moved a DO PASS on Amendment 21.8047.01002 [15:01]
Senator Kreun seconded the motion [15:01].

[15:01]

Senators	Vote
Senator Jerry Klein	Y
Senator Doug Larsen	Y
Senator Randy A. Burckhard	Y
Senator Curt Kreun	Y
Senator Richard Marcellais	Y
Senator Shawn Vedaa	Y

Motion passed: 6-0-0

Senator Vedaa moved a DO PASS AS AMENDED [15:02].
Senator Larsen seconded the motion [15:03].

[15:03]

Senators	Vote
Senator Jerry Klein	Y
Senator Doug Larsen	Y
Senator Randy A. Burckhard	Y
Senator Curt Kreun	Y
Senator Richard Marcellais	Y
Senator Shawn Vedaa	Y

Motion passed: 6-0-0

Senator Kreun will carry the bill [15:03].
Chair Klein closed the meeting at 3:04 p.m.
Isabella Grotberg, Committee Clerk

Adopted by the Industry, Business and Labor Committee

February 2, 2021

PROPOSED AMENDMENTS TO SENATE BILL NO. 2075

Page 1, line 1, after "A BILL" replace the remainder of the bill with "for an Act to create and enact chapter 26.1-02.2 of the North Dakota Century Code, relating to insurance data and security; and to provide for a legislative management study.

BE IT ENACTED BY THE LEGISLATIVE ASSEMBLY OF NORTH DAKOTA:

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

26.1-02.2-01 Definitions.

As used in this chapter:

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

2. "Commissioner" means the insurance commissioner.

3. "Consumer" means an individual, including an applicant, policyholder, insured, beneficiary, claimant, and certificate holder, who is a resident of this state and whose nonpublic information is in a licensee's possession, custody, or control.

4. "Cybersecurity event" means an event resulting in unauthorized access to, disruption, or misuse of, an information system or nonpublic information stored on the information system. The term does not include:

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

   b. An event the licensee has determined that the nonpublic information accessed by an unauthorized person has not been used or released and has been returned or destroyed.

5. "Department" means the insurance department.

6. "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.

7. "Information security program" means the administrative, technical, and physical safeguards a licensee uses to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle nonpublic information.

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

9. "Licensee" means any person licensed, authorized to operate, registered, or required to be licensed, authorized, or registered pursuant to the insurance laws of this state. The term does not include a purchasing group or a risk retention group chartered and licensed in another state or a licensee that is acting as an assuming insurer that is domiciled in another state or jurisdiction.

10. "Multi-factor authentication" means authentication through verification of at least two of the following types of authentication factors:

    a. Knowledge factors, including a password;

    b. Possession factors, including a token or text message on a mobile phone; or

    c. Inherence factors, including a biometric characteristic.

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

    a. Any information concerning a consumer which can be used to identify the consumer because of name, number, personal mark, or other identifier in combination with any one or more 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) Any security code, access code, or password that would permit access to a consumer's financial account; or

        (5) Biometric records.

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

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

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

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

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

13. "Publicly available information" means any information 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 to the general public which are required to be made by federal, state, or local law. A licensee has a reasonable basis to believe that information is lawfully made available to the general public if the licensee has taken steps to determine:

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

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

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

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

26.1-02.2-02. Exclusive regulation.

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

26.1-02.2-03. Information security program.

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

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

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

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

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

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

3. The licensee shall:

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

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

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

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

(1) Employee training and management;

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

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

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

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

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

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

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

(2) Identify and manage the data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes in accordance with the business' relative importance to business objectives and the organization's risk strategy;

(3) Restrict physical access to nonpublic information only to an authorized individual;

(4) Protect by encryption or other appropriate means, all nonpublic information while being transmitted over an external network and all nonpublic information stored on a laptop computer or other portable computing or storage device or media;

(5) Adopt secure development practices for in-house developed applications utilized by the licensee;

(6) Modify the information system in accordance with the licensee's information security program;

(7) Utilize effective controls, which may include multi-factor authentication procedures for employees accessing nonpublic information;

(8) Regularly test and monitor systems and procedures to detect actual and attempted attacks on, or intrusions into, information systems;

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

(10) Implement measures to protect against destruction, loss, or damage of nonpublic information due to environmental hazards, including fire and water damage or other catastrophes or technological failures; and

(11) Develop, implement, and maintain procedures for the secure disposal of nonpublic information in any format.

c. Include cybersecurity risks in the licensee's enterprise risk management process.

d. Stay informed regarding emerging threats or vulnerabilities and use reasonable security measures if sharing information relative to the character of the sharing and the type of information shared; and

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

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

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

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

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

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

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

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

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

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

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

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

(2) The goals of the incident response plan;

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

(4) External and internal communications and information sharing;

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

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

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

10. Annually, an insurer domiciled in this state shall submit to the commissioner, a written statement by April fifteenth, certifying the insurer is in compliance with the requirements set forth in this section. An insurer shall maintain for examination by the department all records, schedules, and data supporting this certificate for a period of five 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 the areas, systems, or processes. The documentation must be available for inspection by the commissioner.

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

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

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

   a. Determine whether a cybersecurity event has occurred;

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

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

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

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

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

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

1. A licensee shall notify the commissioner as promptly as possible, but no 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 if:

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

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

(1) A cybersecurity event impacting the licensee for 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

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

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

a. The date of the cybersecurity event;

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

c. How the cybersecurity event was discovered;

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

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

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

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

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

i. The total number of 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 the estimate with a subsequent report to the commissioner pursuant to this section;

j. 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;

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

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

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

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

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

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

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

5. If a cybersecurity event involving nonpublic information that is used by a licensee that is acting as an assuming insurer or in the possession, custody, or control of a licensee that is acting as an assuming insurer and that does not have a direct contractual relationship with the affected consumers, the assuming insurer shall notify the insurer's affected ceding insurers and the commissioner of the insurer's state of domicile within three business days of making the determination that a cybersecurity event has occurred.

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

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

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

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

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

26.1-02.2-06. Power of commissioner.

1. The commissioner may examine and investigate the affairs of any licensee to determine whether the licensee has been or is engaged in any conduct in violation of this chapter. This power is in addition to the powers the commissioner has under chapter 26.1-03. Any investigation or examination must be conducted pursuant to chapter 26.1-03.

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

26.1-02.2-07. Confidentiality.

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

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

3. In order to assist in the performance of the commissioner's duties the commissioner:

a. May share documents, materials, or other information, including the confidential and privileged documents, materials, or information subject to subsection 1, with other state, federal, and international regulatory agencies, with the national association of insurance commissioners, and with state, federal, and international law enforcement authorities, provided the recipient agrees in writing to maintain the confidentiality and privileged status of the document, material, or other information;

b. May receive documents, materials, or information, including otherwise confidential and privileged documents, materials, or information, from the national association of insurance commissioners, and from regulatory and law enforcement officials of other foreign or domestic jurisdictions, and shall maintain as confidential or privileged any document, material, or information received with notice or the understanding that it is confidential or privileged under the laws of the jurisdiction that is the source of the document, material, or information;

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

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

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

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

26.1-02.2-08. Exceptions.

1. The following exceptions apply to this chapter:

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

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

c. After July 31, 2023, a licensee with fewer than twenty-five employees, including independent contractors and employees of affiliated companies having access to nonpublic information used by the

licensee or in the licensee's possession, custody, or control is exempt from section 26.1-02.2-03.

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

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

26.1-02.2-09. Penalties.

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

26.1-02.2-10. Rules and regulations.

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

26.1-02.2-11. Implementation dates.

A licensee shall implement:

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

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

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

Renumber accordingly

REPORT OF STANDING COMMITTEE

SB 2075: Industry, Business and Labor Committee (Sen. Klein, Chairman) recommends **AMENDMENTS AS FOLLOWS** and when so amended, recommends **DO PASS** (6 YEAS, 0 NAYS, 0 ABSENT AND NOT VOTING). SB 2075 was placed on the Sixth order on the calendar.

Page 1, line 1, after "A BILL" replace the remainder of the bill with "for an Act to create and enact chapter 26.1-02.2 of the North Dakota Century Code, relating to insurance data and security; and to provide for a legislative management study.

BE IT ENACTED BY THE LEGISLATIVE ASSEMBLY OF NORTH DAKOTA:

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

26.1-02.2-01 Definitions.

As used in this chapter:

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

2. "Commissioner" means the insurance commissioner.

3. "Consumer" means an individual, including an applicant, policyholder, insured, beneficiary, claimant, and certificate holder, who is a resident of this state and whose nonpublic information is in a licensee's possession, custody, or control.

4. "Cybersecurity event" means an event resulting in unauthorized access to, disruption, or misuse of, an information system or nonpublic information stored on the information system. The term does not include:

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

   b. An event the licensee has determined that the nonpublic information accessed by an unauthorized person has not been used or released and has been returned or destroyed.

5. "Department" means the insurance department.

6. "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.

7. "Information security program" means the administrative, technical, and physical safeguards a licensee uses to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle nonpublic information.

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

9. "Licensee" means any person licensed, authorized to operate, registered, or required to be licensed, authorized, or registered pursuant to the insurance laws of this state. The term does not include a purchasing group or a risk retention group chartered and licensed in another state or a licensee that is acting as an assuming insurer that is domiciled in another state or jurisdiction.

10. "Multi-factor authentication" means authentication through verification of at least two of the following types of authentication factors:

    a. Knowledge factors, including a password;

    b. Possession factors, including a token or text message on a mobile phone; or

    c. Inherence factors, including a biometric characteristic.

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

    a. Any information concerning a consumer which can be used to identify the consumer because of name, number, personal mark, or other identifier in combination with any one or more 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) Any security code, access code, or password that would permit access to a consumer's financial account; or

        (5) Biometric records.

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

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

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

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

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

13. "Publicly available information" means any information 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 to the general public which are required to be made by federal, state, or local law. A licensee has a reasonable basis to believe that information is lawfully made available to the general public if the licensee has taken steps to determine:

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

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

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

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

26.1-02.2-02. Exclusive regulation.

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

26.1-02.2-03. Information security program.

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

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

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

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

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

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

3. The licensee shall:

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

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

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

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

(1) Employee training and management;

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

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

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

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

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

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

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

(2) Identify and manage the data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes in accordance with the business' relative importance to business objectives and the organization's risk strategy;

(3) Restrict physical access to nonpublic information only to an authorized individual;

(4) Protect by encryption or other appropriate means, all nonpublic information while being transmitted over an external network and all nonpublic information stored on a laptop computer or other portable computing or storage device or media;

(5) Adopt secure development practices for in-house developed applications utilized by the licensee;

(6) Modify the information system in accordance with the licensee's information security program;

(7) Utilize effective controls, which may include multi-factor authentication procedures for employees accessing nonpublic information;

(8) Regularly test and monitor systems and procedures to detect actual and attempted attacks on, or intrusions into, information systems;

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

(10) Implement measures to protect against destruction, loss, or damage of nonpublic information due to environmental hazards, including fire and water damage or other catastrophes or technological failures; and

(11) Develop, implement, and maintain procedures for the secure disposal of nonpublic information in any format.

c. Include cybersecurity risks in the licensee's enterprise risk management process.

d. Stay informed regarding emerging threats or vulnerabilities and use reasonable security measures if sharing information relative to the character of the sharing and the type of information shared; and

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

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

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

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

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

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

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

6. A licensee shall exercise due diligence in selecting its third-party service provider; and a licensee shall require a third-party service provider to implement appropriate administrative, technical, and physical measures

to protect and secure the information systems and nonpublic information accessible to, or held by, the third-party service provider.

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

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

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

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

   (2) The goals of the incident response plan;

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

   (4) External and internal communications and information sharing;

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

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

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

10. Annually, an insurer domiciled in this state shall submit to the commissioner, a written statement by April fifteenth, certifying the insurer is in compliance with the requirements set forth in this section. An insurer shall maintain for examination by the department all records, schedules, and data supporting this certificate for a period of five 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 the areas, systems, or processes. The documentation must be available for inspection by the commissioner.

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

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

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

a. Determine whether a cybersecurity event has occurred;

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

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

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

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

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

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

1. A licensee shall notify the commissioner as promptly as possible, but no 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 if:

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

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

      (1) A cybersecurity event impacting the licensee for 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

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

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

   a. The date of the cybersecurity event;

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

c. How the cybersecurity event was discovered;

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

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

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

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

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

i. The total number of 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 the estimate with a subsequent report to the commissioner pursuant to this section;

j. 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;

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

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

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

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

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

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

b. Nothing in this chapter prevents or abrogates an agreement between a licensee and another licensee, a third-party service provider, or any other party to fulfill any of the investigation requirements

imposed under section 26.1-02.2-04 or notice requirements imposed under subsection 1.

5. If a cybersecurity event involving nonpublic information that is used by a licensee that is acting as an assuming insurer or in the possession, custody, or control of a licensee that is acting as an assuming insurer and that does not have a direct contractual relationship with the affected consumers, the assuming insurer shall notify the insurer's affected ceding insurers and the commissioner of the insurer's state of domicile within three business days of making the determination that a cybersecurity event has occurred.

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

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

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

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

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

26.1-02.2-06. Power of commissioner.

1. The commissioner may examine and investigate the affairs of any licensee to determine whether the licensee has been or is engaged in any conduct in violation of this chapter. This power is in addition to the powers the commissioner has under chapter 26.1-03. Any investigation or examination must be conducted pursuant to chapter 26.1-03.

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

26.1-02.2-07. Confidentiality.

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

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

3. In order to assist in the performance of the commissioner's duties the commissioner:

   a. May share documents, materials, or other information, including the confidential and privileged documents, materials, or information subject to subsection 1, with other state, federal, and international regulatory agencies, with the national association of insurance commissioners, and with state, federal, and international law enforcement authorities, provided the recipient agrees in writing to maintain the confidentiality and privileged status of the document, material, or other information;

   b. May receive documents, materials, or information, including otherwise confidential and privileged documents, materials, or information, from the national association of insurance commissioners, and from regulatory and law enforcement officials of other foreign or domestic jurisdictions, and shall maintain as confidential or privileged any document, material, or information received with notice or the understanding that it is confidential or privileged under the laws of the jurisdiction that is the source of the document, material, or information;

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

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

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

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

26.1-02.2-08. Exceptions.

1. The following exceptions apply to this chapter:

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

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

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

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

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

26.1-02.2-09. Penalties.

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

26.1-02.2-10. Rules and regulations.

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

26.1-02.2-11. Implementation dates.

A licensee shall implement:

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

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

SECTION 2. LEGISLATIVE MANAGEMENT STUDY - CYBER VULNERABILITIES OF ENTITIES LICENSED BY THE INSURANCE DEPARTMENT. During the 2021-22 interim, the legislative management shall consider, with the assistance of the insurance department, studying the North Dakota laws and practice of insurers making property and casualty insurance policies and related information available to insureds by electronic means; the feasibility and desirability of prohibiting insurers from restricting the conditions in which insureds may access such information, including through software and agents of their choosing; and the extent to which insurers conducting business in this state have sought to limit access to policies and related information made available to insureds, whether such restrictions restrain competition in the marketplace, balance with an

analysis of the impact of such access on potential cyber breaches, and loss of trade secret or proprietary information resulting from third-party usage and software applications, and how the two competing considerations can be safely and fairly reconciled. The legislative management shall report its findings and recommendations, together with any legislation required to implement the recommendations, to the sixty-eighth legislative assembly."

Renumber accordingly

2021 SENATE STANDING COMMITTEE MINUTES

Industry, Business and Labor Committee
Fort Union Room, State Capitol

SB 2075
2/9/2021

relating to insurance data and security

Chair Klein opened the meeting at 10:08 a.m. All members were present. Senators Klein, Larsen, Burckhard, Vedaa, Kreun, and Marcellais.

Discussion Topics:

- Amendment issue on floor

Senator Larsen moved to reconsider committee action [10:08].
Senator Kreun seconded the motion [10:08].

Voice vote: motion passed [10:09].

Senator Larsen moved to adopt Amendment 21.8047.02001 [10:10].
Senator Kreun seconded the motion [10:10].

[10:10]

Senators	Vote
Senator Jerry Klein	Y
Senator Doug Larsen	Y
Senator Randy A. Burckhard	Y
Senator Curt Kreun	Y
Senator Richard Marcellais	Y
Senator Shawn Vedaa	Y

Motion passed: 6-0-0

Senator Kreun moved a DO PASS AS AMENDED [10:10].
Senator Larsen seconded the motion [10:10].

[10:10]

Senators	Vote
Senator Jerry Klein	Y
Senator Doug Larsen	Y
Senator Randy A. Burckhard	Y
Senator Curt Kreun	Y
Senator Richard Marcellais	Y
Senator Shawn Vedaa	Y

Motion passed: 6-0-0
Senator Kreun will carry the bill [10:10].

Chair Klein ended the hearing at 10:10 a.m.

Isabella Grotberg, Committee Clerk

CJ 2/9 1 of 1

21.8047.02001
Title.03000

Prepared by the Legislative Council staff for
Senator Klein
February 8, 2021

PROPOSED AMENDMENTS TO ENGROSSED SENATE BILL NO. 2075

Page 6, line 22, after "board" insert "at a minimum"

Page 8, line 19, after the underscored comma insert "at a minimum"

Page 11, line 18, remove "6."

Page 11, line 22, replace "7." with "6."

Page 11, line 27, remove "8."

Page 12, line 1, replace "9." with "7."

Page 12, line 4, replace "10." with "8."

Page 13, line 11, after "commissioners" insert ", its affiliates or subsidiaries"

Page 13, line 17, after "commissioners" insert ", its affiliates or subsidiaries"

Page 14, line 18, after "d." insert "A licensee that is subject to and governed by the privacy, security, and breach notification rules issued by the United States department of health and human services, title 45, Code of Federal Regulations, parts 160 and 164, established pursuant to the federal Health Insurance Portability and Accountability Act of 1996 [Pub. L. 104-191], and the federal Health Information Technology for Economic and Clinical Health Act [Pub. L. 111-5], and which maintains nonpublic information concerning a consumer in the same manner as protected health information is deemed to comply with the requirements of this chapter except for the commissioner notification requirements under subsections 1 and 2 of section 26.1-02.2-05.

e."

Renumber accordingly

REPORT OF STANDING COMMITTEE

SB 2075, as engrossed: Industry, Business and Labor Committee (Sen. Klein, Chairman) recommends **AMENDMENTS AS FOLLOWS** and when so amended, recommends **DO PASS** (6 YEAS, 0 NAYS, 0 ABSENT AND NOT VOTING). Engrossed SB 2075 was placed on the Sixth order on the calendar.

Page 6, line 22, after "board" insert "at a minimum"

Page 8, line 19, after the underscored comma insert "at a minimum"

Page 11, line 18, remove "6."

Page 11, line 22, replace "7." with "6."

Page 11, line 27, remove "8."

Page 12, line 1, replace "9." with "7."

Page 12, line 4, replace "10." with "8."

Page 13, line 11, after "commissioners" insert ", its affiliates or subsidiaries"

Page 13, line 17, after "commissioners" insert ", its affiliates or subsidiaries"

Page 14, line 18, after "d." insert "A licensee that is subject to and governed by the privacy, security, and breach notification rules issued by the United States department of health and human services, title 45, Code of Federal Regulations, parts 160 and 164, established pursuant to the federal Health Insurance Portability and Accountability Act of 1996 [Pub. L. 104-191], and the federal Health Information Technology for Economic and Clinical Health Act [Pub. L. 111-5], and which maintains nonpublic information concerning a consumer in the same manner as protected health information is deemed to comply with the requirements of this chapter except for the commissioner notification requirements under subsections 1 and 2 of section 26.1-02.2-05.

e."

Renumber accordingly

2021 HOUSE INDUSTRY, BUSINESS AND LABOR

SB 2075

2021 HOUSE STANDING COMMITTEE MINUTES

Industry, Business and Labor Committee
Room JW327C, State Capitol

SB 2075
3/9/2021

Insurance data & security & provide a legislative management study.

(2:18) Chairman Lefor called the hearing to order.

Representatives	Attendance	Representatives	Attendance
Chairman Lefor	P	Rep Ostlie	P
Vice Chairman Keiser	P	Rep D Ruby	A
Rep Hagert	P	Rep Schauer	P
Rep Kasper	P	Rep Stemen	P
Rep Louser	P	Rep Thomas	P
Rep Nehring	P	Rep Adams	P
Rep O'Brien	P	Rep P Anderson	P

Discussion Topics:

- Insurance Data Cybersecurity Law

Jon Godfread~ND Insurance Commissioner. Attachment # 7958.

Bruce Ferguson~American Council of Life Insurers-Senior Vice President. Attachment #8111.

Chairman Lefor closes the hearing.

Rep Stemen moved a Do Pass.

Rep P Anderson second.

Representatives	Vote
Chairman Lefor	Y
Vice Chairman Keiser	A
Rep Hagert	Y
Rep Jim Kasper	Y
Rep Scott Louser	Y
Rep Nehring	Y
Rep O'Brien	Y
Rep Ostlie	Y
Rep Ruby	A
Rep Schauer	Y
Rep Stemen	Y
Rep Thomas	Y
Rep Adams	Y
Rep P Anderson	Y

Vote roll call taken Motion carried 12-0-2 & Rep O'Brien is the carrier.

(2:58) End time.

Ellen LeTang, Committee Clerk

REPORT OF STANDING COMMITTEE

SB 2075, as reengrossed: Industry, Business and Labor Committee (Rep. Lefor, Chairman) recommends **DO PASS** (12 YEAS, 0 NAYS, 2 ABSENT AND NOT VOTING). Reengrossed SB 2075 was placed on the Fourteenth order on the calendar.

Engrossed Senate Bill No. 2075

Presented by: **Jon Godfread**
Insurance Commissioner
North Dakota Insurance Department

Before: **House Industry Business and Labor Committee**
Representative Mike Lefor, Chairman

Date: **March 9th, 2021**

Chairman Lefor and members of the House Industry Business and Labor Committee. For the record, I am Jon Godfread, North Dakota Insurance Commissioner. I appear before you in support of Engrossed Senate Bill 2075. As Senate Bill 2075 was introduced, it dealt with third party access to insurance information. The discussion centered on an attempt to help consumers and agents shop the complex world of insurance products and allow them to compare products without the threat of insurance companies restricting consumers access to their data.

During that initial hearing, the industry brought forward several concerns regarding cybersecurity and the potential harm our proposed legislation could cause or potentially expose them to. We heard their concerns, and prior to passage of Engrossed SB 2075 we worked diligently with the industry to work on a proposed solution to the cybersecurity concerns that were raised by the industry.

We shared those same concerns, we share the same desire to protect consumer data, to safe guard against data breeches, and make sure we are doing our part as a state to provide a reasonable framework of regulation to help provide those protections to the industry and our consumers. To that end, we proposed a hog house to SB 2075 and that is the bill that passed the Senate and the bill you have before you today. Engrossed Senate Bill 2075 would implement the National Association of Insurance Commissioners (NAIC) Insurance Data Security Model Law.

In recent years, there have been several major data breaches involving large insurers that have exposed and compromised the sensitive personal information of millions of insurance consumers. As a result, state insurance regulators made reevaluating the regulations around cybersecurity and consumer data protection as a key priority. In early 2016 the NAIC began the process of drafting the Insurance Data Security Model Law.

Following almost two years of extensive deliberations and input from state insurance regulators, consumer representatives, and the insurance industry, the NAIC model was adopted in October of 2017. Adoption of the model is critical for us to have the tools necessary to protect sensitive consumer information. The U.S. Treasury Department has urged quick action and adoption by the states. The Treasury Department also further recommended that if adoption and implementation of the model by the states does not result in mostly uniform data security regulations within 5 years, then Congress needs to act by passing legislation setting forth uniform requirements for insurer data security. With the results of the last election and the

current make up of congress, the deadline has become more evident and more important for states to pay attention to.

When we proposed our agency legislation for this coming session, we did not anticipate the change in the makeup of Congress and planned on bringing this model to the legislature during the 2023 Legislative Session. The interest and concerns proposed in the original hearing of Senate Bill 2075, coupled with the finalized elections results and the seating of a new congress, is why we are here asking this body to adopt the Insurance Data Security Model Law.

I think we can all agree that state-based regulation is preferred, and that is why we worked diligently with all of the stakeholders to ensure we can propose a law that is agreeable and workable by all parties. In proposing Engrossed SB 2075, we reviewed the language passed by the 11 states that have already enacted this legislation, the 3 states that currently have it before their legislative bodies, and worked with trade associations from across the industry. The version you have before you is essentially a combination of all the good work that has been accomplished across the country and brings in the best changes that have been proposed and accepted in other states, while maintaining the overall structure to retain uniformity and hopefully prevent federal action in this space.

The Insurance Data Cybersecurity Law contains three main requirements:

1. Requires licensees to develop, implement, and maintain an information security program.
    a. The information security program is intended to scale with the size and complexity of the organization based on the licensee's own risk assessment.
    b. The model is principles-based, meaning that specific kinds or types of information security measures are not required. Instead, it is left to the licensee to determine what security measures best fit their needs.
    c. Licensees who have less than $10 million in assets, less than $5 million in revenue, or fewer than 50 employees (for the first 2 years and then 25 thereafter) are exempt from this requirement.
    d. There is also an exemption for licensees that meet the federal Health Information Portability and Accountability Act (HIPPA) data security standards for all non-public information.
2. Requires licensees to investigate possible cybersecurity events and notify the Insurance Commissioner if a cybersecurity event occurs.
    a. The required notification includes the information that was exposed, the number of consumers affected, and the efforts made to address the breach.
    b. The information provided is held confidentially.
3. Requires notice to affected consumers when a cybersecurity event occurs.

As I mentioned before, this model has been adopted in eleven states – Alabama, Connecticut, Delaware, Indiana, Louisiana, Michigan, Mississippi, New Hampshire, Ohio, South Carolina, and Virginia; and is currently before the legislative bodies in Maine, Rhode Island and Wisconsin.

I believe this is critically important given the recent outcomes and the priorities that may be coming from the federal government. It is important to preserve state authority in this area and to protect North Dakota consumers while maintaining a strong, competitive insurance industry.

I have also included a section by section breakdown of the amendment and would be happy to walk through that if you would find that helpful.

Breakdown of SB 2075 Proposed Amendment:

Pg 1 – Pg3 lns 1-23 -- Section 1: Definitions – these definitions are modeled after definitions from other areas of our code.

Pg 3 ln 24-27 -- Exclusive Regulation

26.1-02.2-02 – This would provide the Insurance Department with the exclusive regulation of data security and investigations of cybersecurity events, within the insurance industry. There are currently no conflicts with North Dakota law, however there is another bill, HB 1314, that was passed by this chamber that has to do with notification. As you can see, this area continues to develop and this section would help us avoid either duplicative regulations or regulations that would not apply to the insurance industry.

Pg 3 ln 28-31 – Pg 8 ln 1-13 -- Information Security Program

26.1-02.2-03 - This section requires a licensee to develop, implement, and maintain a comprehensive written security program based on a licensee's self-risk assessment. This security program should contain administrative, technical, and physical safeguards for the protection of nonpublic information in the control of a licensee.

Subsection 2 breaks down the technical aspects of which the security program shall be designed to do. Such as protect the confidentiality of nonpublic information, protect against any threats, protect from any unauthorized use, and reevaluate that as needed.

Subsection 3 establishes standard safeguards of the security program. Such as designation of an employee to oversee the security program, identify any internal or external threats, assess the likelihood of these threats, assess the procedures and policies in place (such as employee training) and maintain an ongoing assessment of these safeguards no less than annually.

Subsection 4 breaks down what measures should be implemented based on the self-assessment risk of a licensee. These measures begin on page 5, line 14 and go through page 6, line 11. Again, I want to stress the measures that may be implemented will be unique and customizable base on the licensee's self-assessment:

Subsection 5 lays out criteria that should be taken if the licensee has a board of directors.

Subsection 6 lays out criteria if the licensee is working with a third party. And requires a license to implement appropriate administrative, technical, and physical measures on the third party.

Subsection 7 requires a licensee to monitor, evaluate and adjust the information security program as appropriate. These changes may be required due to internal external threats or the licensee's changing business arrangements such as a merger or acquisition.

Subsection 8 indicates how information security program shall respond to a cyber security event and what areas this incident response plan shall address.

Subsection 9 details the seven criteria that a licensee's incident response plan must address.

Subsection 10 requires domiciliary licensees shall submit a written statement every April to the commissioner certifying their compliance with the requirements of this section. We worked with the stakeholders to implement changes from the proposed model that are both reasonable and flexible to the industry and the department while maintaining the true nature of the regulation.

While we have lessened the burden for licensees around testing and developing new applications, that doesn't mean once a system is in place companies can ignore it. Ongoing monitoring is required, but we have worked with stakeholders to lessen the burden from the NAIC model law.

Pg 8 ln 14-31 – Pg 9 ln 1-3 -- Investigation of a Cybersecurity Event

26.1-02.2-04 - This sets out criteria of how a licensee should investigate a cyber security event

Pg 9 ln 4-30 – Pg 12 ln 1-13 -- Notification of a Cyber Event

26.1-02.2-05 – This sets out criteria of who needs to be notified when there is a Cyber event.

Subsection 1 and 2 lays out criteria for when and how to notify the commissioner's office.

Subsection 3 falls back to what is already in place under chapter 51-30 in terms of consumer notification for breaches of personal data. This subsection also adds on that if a consumer is notified the commissioner must be as well

Subsection 4 explains the requirements for when a third party maintains the information system and how notifications need to be handled.

Subsection 5 and 6 detail how a licensee shall notify ceding companies, whether the licensee or a third-party is in control of the non-public information.; while subsection 7 states that the assuming insurer does not have notice obligations.

Subsection 8 details how notification should be handled between a company and a producer. We have changed the notification to the Commissioner from the NAIC model law to only include a cyber event in which nonpublic information has been breached. Furthermore, we require that the breach have a material harm to the consumer.

We have also changed the notification to third parties, to once again only be required if there is a material harm to the consumer or to the third parties.

We have also changed the notification to producers to allow companies to notify a consumer and producer of a cyber security event at the same time rather than a producer first.

Pg 12 ln 14 – 22 -- Powers of the Commissioner

26.1-02.2-06 - This section gives the power to the Commissioner to examine a licensee if necessary and take appropriate steps in case of a cyber breach. This is an addition to the Commissioner's authority already established under 26.1-03

Pg 12 ln 23 - 31 – Pg 14 ln 1-4 Confidentiality

26.1-02.2-07 - This section sets out what information can be held confidential during an investigation of a cyber breach by the Commissioner's Office.

Pg 14 ln 5 – 31 – Pg 15 ln 1-2 -- Exemptions

26.1-02.2-08 – This section, as I already stated, exempts certain licensees from implementing a security program, the idea of this law is not to become over burdensome on smaller licensees such as an agent who has one employee. That is to say, if a small agency had to implement a security program the cost of implementing that program would almost cause that small agent to be run out of business therefore we have added exemptions for cases such as this.

We also realize it may take some time for a licensee to implement a sophisticated security program. Therefore, we have called for a phased in approach to this model. Our law phases in the requirements over the course of two years. Initially, licensees with fewer than 50 employees are exempt from the security program burden. And after those two years that exemption drops to licensees with 25 or fewer employees. We have also exempted out licensees with less than $5million in gross revenue or less than $10million in year-end assets.

There is also a reporting requirement exemption for a licensee which is subject to HIPAA. HIPAA requires a more stringent cybersecurity program, implementation, and monitoring. Therefore, a licensee subject to HIPAA is exempt from this law, other than notifying the commissioner if there is a cyber breach.

Pg 15 ln 3 – 5 – Penalties

Pg 15 ln 6 – 8 – Rules and Regulations

Pg 15 ln 9 – 13 – Delayed Implementation of the Information Security Program

This allows for the implementation of this law to take effect on August 1st, 2022, essentially giving the companies operating in this state the time necessary to develop programs in response this legislation. We believe this is a reasonable request from the industry as we are all still responding to and coming off of the global health pandemic, a delayed implementation date does make some sense in this instance.

This would also delay the implementation of the requirement of companies to hold third party service providers to this standard for an additional year, effective August 1st, of 2023. We also think this is a reasonable request as these agreements take time to enter in to and place a new responsibility on companies. Essentially this gives companies the opportunity to ensure their house is in order, before fixing the third-party agreements.

Section 2 of the bill Pg 15 Ln 14 – 28 Study Language

This studies the original intent of the bill and allows the Insurance Department to study North Dakota laws and practices of insurers related to making information available to insureds by electronic means; the feasibility and desirability of prohibiting insurers from restricting the conditions in which insureds may access that information.

We believe this study is important to help gain better understanding of the issues that surround new entrants to the market, how they are interacting with consumer data and are there players within the industry that are restricting access in an anti-competitive way, while maintaining critical cybersecurity protections for our consumers. This would be important to do with the assistance of a legislative interim committee as it would likely result in potential policy changes, which may be complex in nature.

This study request would address some of the concerns raised by the original intent of the bill as to actions that have been taken against authorized third-party providers. This study would be conducted with the Insurance Department and Legislative Management.

I understand that this is a lot, but I hope we can express to you that much of the leg work has been done in working with the various stakeholders. We are certainly open to further comments, but we believe we have this bill and proposed law in a situation where all parties are amenable to the changes and certainly understand our intentions and the importance of this legislation.

I know there are others who are seeking to testify on this issue, so I would pause for questions, but I also want to ensure everyone else gets an opportunity to address the committee. Thank you.

8111

TESTIMONY OF THE AMERICAN COUNCIL OF LIFE INSURERS

Before the House Industry, Business and Labor Committee

March 9, 2021

Senate Bill 2075 – An Act Relating to Insurance Data and Security

Chairman Lefor and members of the House Industry, Business and Labor Committee, I am writing on behalf of the American Council of Life Insurers (ACLI) to express our support for the Senate-passed amendments to Senate Bill 2075.

ACLI is the leading trade association driving public policy and advocacy on behalf of the life insurance industry and its consumers. Ninety million American families rely on the life insurance industry for financial protection and retirement security. ACLI members have robust data security programs and processes in place to protect the security of their customers' personal information and the systems on which the information is stored.

Our Position

ACLI supports the Senate-passed amendments to SB 2075, as they reflect substantial improvements to the NAIC Insurance Data Security Model Law on which the bill is based. Specifically, these amendments establish standards that (1) are flexible enough to reflect the risk profile of individual insurers; (2) are the exclusive standards to which insurers must comply (page 3, lines 24-27); and (3) require insurers to give notice to the Commissioner and consumers only when the cybersecurity event is reasonably likely to cause material harm (page 9, lines 4-20). We appreciate Commissioner Godfread's willingness to work with multiple stakeholders to make these amendments workable for insurers doing business in the Peace Garden state.

Background

ACLI's Board of Directors has approved the following principles relating to data security laws expressly applicable to life insurance companies and other insurance licensees:

- Data security standards should be uniform from state to state and constitute the exclusive security standards in any individual state to the greatest extent possible. This will ensure level consumer protection across the country and avoid subjecting companies and other insurance licensees to different and conflicting standards in different states or any individual state.

- Data security standards should not be prescriptive. Instead, such standards should be flexible, risk-based and subject to the risk assessment of each company or other insurance licensee based on its particular risk profile. This will enable companies and other insurance licensees

American Council of Life Insurers
101 Constitution Avenue, NW, Washington, DC 20001-2133
www.acli.com

to effectively protect the security of their customers' personal information and the systems on which the information is stored.

- Any requirements to notify state insurance commissioners or other government agencies of data security or cybersecurity events should apply only to events reasonably likely to cause material harm to a company or other insurance licensee or to consumers whose sensitive personal information is reasonably believed to have been involved in the event. To the extent possible, these requirements should not conflict with consumer notification requirements that may be imposed under other laws.

Chairman Lefor and members of the Committee, I appreciate the opportunity you have given us to provide our comments on Senate Bill 2075 and stand ready to answer any questions you may have.

Respectfully submitted,

J. Bruce Ferguson
Senior Vice President, State Relations
American Council of Life Insurers
101 Constitution Avenue NW
Washington, DC 20001
bruceferguson@acli.com
202.624.2385
301.980.4820 mobile