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.