NORTH DAKOTA
Insurance Department

TESTIMONY

Matt Fischer, Division Director, Company Licensing & Examinations
Senate Industry and Business Committee
January 22, 2025

Good morning, Chairman Barta and members of the Committee. My name is Matt Fischer, and I am the Division Director of Company Licensing & Examinations for the North Dakota Insurance Department. I appear before you today in support Senate Bill No. 2088.

This bill amends the existing Insurance Data Security law. This law was first passed during the 67th Legislative Session as Senate Bill 2075. The law is based the National Association of Insurance Commissioners ("NAIC") model law which was drafted back in 2016. The purpose of this law is to require licensees, which includes both insurance producers and insurance companies, to report to the Insurance Commissioner any cybersecurity events the licensee or its vendors experience. With this bill we are hoping to address some emerging cyber issues and to align our statute more closely with the original model language as various deviations were made when this law was first passed. As we have seen over the four years since its passage, some issues were unintendedly created by these deviations.

Section one would strike out an exclusion from the definition of a cybersecurity event. Under the current law, if a licensee determines that nonpublic information was accessed but it was either not used or released and it was returned or deleted, this would not be considered a reportable cybersecurity event. We know following the Change Healthcare ("Change") data breach last year, that Change paid the requested ransom to ensure that its data would be deleted, however, the hackers did not delete the data after receiving the ransom, instead the data was sold on the dark web to another ransomware group. By leaving the law unchanged, this language allows a licensee to not report a cybersecurity event to the Department if they believe that the same individual or group who just hacked their systems, can also be trusted to completely delete or return all the licensee's breached policyholder data. The Department feels licensees cannot trust hackers.

In addition, the Department has worked on an amendment to the definition of what qualifies as a cybersecurity event. This amendment was drafted in conjunction with our largest domestic health insurer. There was concern with the original draft of this section that any kind of event would need to be reported. That is not the goal of this bill. The goal of this amendment was to ensure that cybersecurity events in which a consumer's data was potentially comprised would be reported to our Department.

Section two includes a few changes. One revision changes the reporting period of an event to 72 hours from 3 business days. This change aligns with the original model and will allow the Department to be made aware of a cybersecurity event sooner so that if follow up or

action is necessary, additional time is not wasted. The second change is an overstrike to remove language regarding materiality. Materiality is a term that is not defined within the current law or the model, but it is often used by the Department and licensees to describe items or events relating to financial solvency. Our concern with this language in the context of this law is that, to a billion-dollar company, the unauthorized release of one policyholder's sensitive, confidential information is clearly immaterial from a financial perspective, but to that individual this is often a material, life altering event. To fulfill the Department's mission of meeting the needs of North Dakota's insurance consumers, we feel it is appropriate to modify this language so that all cybersecurity events of domestic licensees get reported to the Department.

Section three is an overstrike from the confidentiality section of the law. The law currently gives the Department the authority to investigate or examine a licensee which has experienced a cybersecurity event. If an examination is conducted it must be done in accordance with our general examination authority within N.D.C.C. § 26.1-03. Under that statute a written report of examination must be issued. The language that is being overstricken could allow a licensee to prevent the release of an examination report. We do not feel this is appropriate as consumers of the licensee need to know if a breach has occurred and how the licensee has responded.

Section four is removing certain licensee exemptions and clarifying what sections of the law apply to small licensees. Under the law as it is currently written, all licensees are required to report a cybersecurity event to the Department. One piece of the law is that all licensees are required to have an Information Security Program. During the 67th Legislative Session it was decided that an Information Security Program could be burdensome to small licensees and therefore exemptions were added to alleviate that concern. In our view, completely exempting small licensees is not appropriate as it means consumers doing business with those licensees may not have the same protections of their data as consumers of larger licensees. The changes we are requesting still exempts those small licensees from creating and maintaining a full Information Security Program but instead, it requires them to have a program that is commensurate with their size and complexity. The last change made in section four is related to a licensee which is subject to the Health Insurance Portability and Accountability Act of 1996 "(HIPAA"). When the law was first passed, licensees subject to HIPAA only needed to comply with the reporting requirements of this law. The Department is therefore, not permitted to investigate, examine, or issue an examination report if a cybersecurity event were to occur with a licensee subject to HIPAA.

Finally, section five repeals the staggered implementation dates of the exemptions in the bill as passed in 2021.

I respectfully request a "do pass" recommendation from the committee on Senate Bill 2088 and I am happy to take any questions.