

2025 SENATE INDUSTRY AND BUSINESS

SB 2088

2025 SENATE STANDING COMMITTEE MINUTES

Industry and Business Committee Fort Union Room, State Capitol

SB 2088
1/22/2025

A bill relating to data security requirements for insurance producers; and relating to implementation dates for certain data security requirements for insurance producers.

9:00 a.m. Chairman Barta called the meeting to order.

Members present: Chairman Barta, Vice-Chairman Boehm, Senator Klein, Senator Kessel, Senator Enget

Discussion Topics:

- National Association of Insurance Commissioners (NAIC)
- Unreleased, returned, or deleted data.
- Distrust in hackers
- Domestic health insurers
- Reporting period
- Definition of materiality

9:01 a.m. Matt Fischer, Division Director of Company Licensing and Examinations for the ND Insurance Department, testified in favor and submitted testimony #30631.

9:23 a.m. Dennis Pathroff, lobbyist representing APCIA, testified in opposition and submitted testimony #30608.

9:30 a.m. Megan Hruby, Blue Cross Blue Shield, testified neutrally and answered committee questions.

9:32 a.m. Chairman Barta closed the hearing.

Audrey Oswald, Committee Clerk



January 21, 2025

RE: SB 2088 – North Dakota Data Security

Thank you for this opportunity to provide comments on North Dakota Senate Bill 2088. The American Property Casualty Insurance Association (APCIA)¹, the American Council of Life Insurers (ACLI)², and the National Association of Mutual Insurance Companies (NAMIC)³ support robust consumer protection and the safeguarding of sensitive personal information. We appreciate the Insurance Department's robust engagement with stakeholders as we have worked towards solutions that balance operational feasibility and consumer protections. However, we still have significant concerns about the proposed amendments to North Dakota's data security law, as these changes could impose considerable challenges on insurers while providing limited additional benefit to consumers.

1. Revisions to Notice Provisions

The existing law appropriately limits notification requirements to cybersecurity events that are reasonably likely to cause material harm to insurance licensees or consumers whose sensitive personal information is affected. This standard strikes a crucial balance between meaningful oversight and operational efficiency, ensuring attention is focused on incidents that truly matter.

In contrast, the proposed amendment, which mandates notifications for all cybersecurity events—even those unlikely to cause harm—would create unnecessary administrative burdens and divert resources from addressing genuine threats to consumer protection and cybersecurity. Many instances of unauthorized access are not malicious and pose no risk of harm to consumers. For example, a claims file might be sent to the wrong plaintiff's lawyer, or an employee could inadvertently include sensitive information in an internal email. Such occurrences do not warrant

¹ APCIA is the primary national trade association for home, auto, and business insurers. APCIA promotes and protects the viability of private competition for the benefit of consumers and insurers, with a legacy dating back 150 years. APCIA represents the broadest cross-section of home, auto, and business insurers of any national trade association.

² ACLI is the leading trade association driving public policy and advocacy on behalf of the life insurance industry. 90 million American families rely on the life insurance industry for financial protection and retirement security. ACLI's member companies are dedicated to protecting consumers' financial wellbeing through life insurance, annuities, retirement plans, long-term care insurance, disability income insurance, reinsurance, and dental, vision and other supplemental benefits. ACLI's 275 member companies represent 93 percent of industry assets in the United States.

³ NAMIC represents nearly 1,500 member companies, including six of the top 10 property/casualty insurers in the United States. NAMIC member companies collectively write more than \$391 billion in annual premiums and represent significant portions of the homeowners, automobile, and business insurance markets, including \$546 million in written premium in the state of North Dakota.

notification, and regulatory departments would neither need nor want to be inundated with these reports.

Equally concerning is the potential ripple effect: requiring notification of insignificant events to North Dakota could trigger notice obligations in other states, amplifying the burden without enhancing consumer protection.

Notably, most states that have enacted the NAIC Insurance Data Security Model Act have adopted similar language, ensuring notification provisions target only events with a meaningful likelihood of harm. Retaining the current standard not only safeguards consumers but also fosters uniformity across jurisdictions, creating a consistent, efficient framework that benefits both insurers and consumers.

2. Notification Timeline

The proposed change from “three business days” to “seventy-two hours” for notification of a cybersecurity event fails to account for weekends and holidays, when key personnel may not be available. This rigid timeline would create significant challenges for insurers, particularly in complex cases where initial assessments take time. A “three business days” standard is more practical and provides sufficient time for insurers to investigate and provide accurate, meaningful reports to regulators without compromising consumer protection. This timeline would also align with regulator schedules, which similarly accommodate weekends and holidays when such reports are unlikely to be reviewed.

3. Removal of Written Consent for Public Disclosure

We also have concerns about the amendment removing the requirement for licensees' prior written consent before public disclosure of sensitive information. While we understand the Department's intention to align this change with statutory requirements for transparency, it raises significant confidentiality concerns. Stakeholders have been assured that sensitive information will not be disclosed unnecessarily, but removing the consent requirement introduces risks to insurers and their consumers without a clear consumer benefit.

Recommendations

1. Retain the existing language found in ND §26.1-02.2-05. Notification of a cybersecurity event: *“...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.”*
2. Retain existing references to “three business days” rather than amending the language to “seventy-two hours.”

3. Retain the existing language found in ND §26.1-02.2-07. Confidentiality: “...*The commissioner may not otherwise make the documents, materials, or other information public without the prior written consent of the licensee.*”

Conclusion

APCIA, ACLI, and NAMIC all believe in protecting consumers and ensuring strong data security practices. However, the proposed amendments would burden insurers with requirements that provide limited additional consumer protection. We urge the North Dakota legislature to reconsider these amendments and maintain the balance between regulatory oversight and operational feasibility that the current law achieves.

By preserving a practical, focused approach to data security, North Dakota can ensure robust consumer protection while supporting an insurance industry that effectively serves its policyholders.

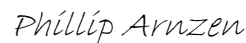
Sincerely,



Brooke Kelley
AVP. State Government Relations
APCIA



Alex Young
Regional Director – State Relations
ACLI



Phillip Arnzen
Regional Vice President- Midwest
NAMIC



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 it 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.

2025 SENATE STANDING COMMITTEE MINUTES

Industry and Business Committee Fort Union Room, State Capitol

SB 2088
1/28/2025

A bill relating to data security requirements for insurance producers; and relating to implementation dates for certain data security requirements for insurance producers.

9:44 a.m. Chairman Barta opened the hearing on SB 2088.

Members present: Chairman Barta, Vice-Chairman Boehm, Senator Enget, Senator Klein, Senator Kessel

Discussion Topics:

- Insurance Department and the American Property Casualty Insurance Association (APCIA)
- Notification of a cybersecurity event
- Attorney General reference
- Normal operations of licensees
- Model language deviation

9:47 a.m. Senator Klein moved to adopt amendment LC# 25.8122.01001.

9:47 a.m. Senator Kessel seconded the motion.

Senators	Vote
Senator Jeff Barta	Y
Senator Keith Boehm	Y
Senator Mark Enget	Y
Senator Greg Kessel	Y
Senator Jerry Klein	Y

Motion passed 5-0-0.

9:48 a.m. Senator Kessel moved a Do Pass As Amended.

9:48 a.m. Senator Klein seconded the motion.

Senators	Vote
Senator Jeff Barta	Y
Senator Keith Boehm	Y
Senator Mark Enget	Y
Senator Greg Kessel	Y
Senator Jerry Klein	Y

Motion passed 5-0-0.

Senator Boehm will carry the bill.

Senate Industry and Business Committee
SB 2088
01/28/25
Page 2

9:50 a.m. Chairman Barta closed the hearing.

Audrey Oswald, Committee Clerk

January 28, 2025

Sixty-ninth
Legislative Assembly
of North Dakota

PROPOSED AMENDMENTS TO

SENATE BILL NO. 2088

Introduced by

Industry and Business Committee

(At the request of the Insurance Commissioner)

JB 1-28-25
1 of 7

1 A BILL for an Act to amend and reenact subsection 4 of section 26.1-02.2-01, sections
2 26.1-02.2-05 and 26.1-02.2-07, and subsection 1 of section 26.1-02.2-08 of the North Dakota
3 Century Code, relating to data security requirements for insurance producers; and to repeal
4 section 26.1-02.2-11 of the North Dakota Century Code, relating to implementation dates for
5 certain data security requirements for insurance producers.

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

7 **SECTION 1. AMENDMENT.** Subsection 4 of section 26.1-02.2-01 of the North Dakota
8 Century Code is amended and reenacted as follows:

- 9 4. "Cybersecurity event" means an event resulting in unauthorized access to, disruption,
10 or misuse of, an information system or nonpublic information stored on the information
11 system. The term does not include:
- 12 a. ~~The~~the unauthorized acquisition of encrypted nonpublic information if the
 - 13 encryption, process, or key is not also acquired, released, or used without
 - 14 authorization; ~~or~~
 - 15 b. ~~An event the licensee has determined that the nonpublic information accessed by~~
 - 16 ~~an unauthorized person has not been used or released and has been returned or~~
 - 17 ~~destroyed.~~

18 **SECTION 2. AMENDMENT.** Section 26.1-02.2-05 of the North Dakota Century Code is
19 amended and reenacted as follows:

DM 2087

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~~ seventy-two hours 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~~ triggers notification to a consumer residing in the state in accordance with chapter 51-30 or has a 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;

- 1 e. The identity of the source of the cybersecurity event;
- 2 f. Whether the licensee has filed a police report or has notified any regulatory,
3 government, or law enforcement agencies and, if so, when the notification was
4 provided;
- 5 g. Description of the specific types of information acquired without authorization.
6 Specific types of information means particular data elements, including medical
7 information, financial information, or any other information allowing identification
8 of the consumer;
- 9 h. The period during which the information system was compromised by the
10 cybersecurity event;
- 11 i. The total number of consumers in this state affected by the cybersecurity event.
12 The licensee shall provide the best estimate in the initial report to the
13 commissioner and update the estimate with a subsequent report to the
14 commissioner pursuant to this section;
- 15 j. The results of any internal review identifying a lapse in either automated controls
16 or internal procedures, or confirming that all automated controls or internal
17 procedures were followed;
- 18 k. Description of efforts being undertaken to remediate the situation that permitted
19 the cybersecurity event to occur;
- 20 l. A copy of the licensee's privacy policy and a statement outlining the steps the
21 licensee will take to investigate and notify consumers affected by the
22 cybersecurity event; and
- 23 m. Name of a contact person that is both familiar with the cybersecurity event and
24 authorized to act for the licensee.
- 25 3. The licensee shall comply with chapter 51-30, as applicable, and provide a copy of the
26 notice sent to consumers to the commissioner, when a licensee is required to notify
27 the commissioner under subsection 1.
- 28 4. In the case of a cybersecurity event in a system maintained by a third-party service
29 provider, of which the licensee has become aware, the licensee shall treat the event in
30 accordance with subsection 1 unless the third-party service provider provides the
31 notice required under chapter 26.1-02.2 to the commissioner.

JB 4007

- 1 a. The computation of licensee's deadlines under this subsection begin on the day
- 2 after the third-party service provider notifies the licensee of the cybersecurity
- 3 event or the licensee otherwise has actual knowledge of the cybersecurity event,
- 4 whichever is sooner.
- 5 b. Nothing in this chapter prevents or abrogates an agreement between a licensee
- 6 and another licensee, a third-party service provider, or any other party to fulfill
- 7 any of the investigation requirements imposed under section 26.1-02.2-04 or
- 8 notice requirements imposed under subsection 1.
- 9 5. If a cybersecurity event involving nonpublic information that is used by a licensee that
- 10 is acting as an assuming insurer or in the possession, custody, or control of a licensee
- 11 that is acting as an assuming insurer and that does not have a direct contractual
- 12 relationship with the affected consumers, the assuming insurer shall notify the
- 13 insurer's affected ceding insurers and the commissioner of the insurer's state of
- 14 domicile within ~~three business days~~seventy-two hours of making the determination
- 15 that a cybersecurity event has occurred. The ceding insurer that has a direct
- 16 contractual relationship with affected consumers shall fulfill the consumer notification
- 17 requirements imposed under chapter 51-30 and any other notification requirements
- 18 relating to a cybersecurity event imposed under subsection 1.
- 19 6. If a cybersecurity event involving nonpublic information that is in the possession,
- 20 custody, or control of a third-party service provider of a licensee that is an assuming
- 21 insurer, the assuming insurer shall notify the insurer's affected ceding insurers and the
- 22 commissioner of the insurer's state of domicile within ~~three business days~~seventy-two
- 23 hours of receiving notice from its third-party service provider that a cybersecurity event
- 24 has occurred. The ceding insurers that have a direct contractual relationship with
- 25 affected consumers shall fulfill the consumer notification requirements imposed under
- 26 chapter 51-30 and any other notification requirements relating to a cybersecurity event
- 27 imposed under subsection 1.
- 28 7. Any licensee acting as assuming insurer does not have any other notice obligations
- 29 relating to a cybersecurity event or other data breach under this section or any other
- 30 law of this state.

Amg 5007

8. 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.

SECTION 3. AMENDMENT. Section 26.1-02.2-07 of the North Dakota Century Code is amended and reenacted as follows:

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 under this chapter, the commissioner:
 - a. May share documents, materials, or other information, including the confidential and privileged documents, materials, or information subject to subsection 1, with

Am 6007

- 1 other state, federal, and international regulatory agencies, with the national
2 association of insurance commissioners, its affiliates or subsidiaries, and with
3 state, federal, and international law enforcement authorities, provided the
4 recipient agrees in writing to maintain the confidentiality and privileged status of
5 the document, material, or other information;
- 6 b. May receive documents, materials, or information, including otherwise
7 confidential and privileged documents, materials, or information, from the national
8 association of insurance commissioners, its affiliates or subsidiaries, and from
9 regulatory and law enforcement officials of other foreign or domestic jurisdictions,
10 and shall maintain as confidential or privileged any document, material, or
11 information received with notice or the understanding that it is confidential or
12 privileged under the laws of the jurisdiction that is the source of the document,
13 material, or information;
- 14 c. May share documents, materials, or other information subject to this section, with
15 a third-party consultant or vendor provided the consultant agrees in writing to
16 maintain the confidentiality and privileged status of the document, material, or
17 other information; and
- 18 d. May enter agreements governing sharing and use of information consistent with
19 this subsection.
- 20 4. A waiver of any applicable privilege or claim of confidentiality in the documents,
21 materials, or information does not occur as a result of disclosure to the commissioner
22 under this section or as a result of sharing as authorized in subsection 3.
- 23 5. Documents, materials, or other information in the possession or control of the national
24 association of insurance commissioners or a third-party consultant or vendor pursuant
25 to this chapter are confidential, not subject to chapter 44-04, not subject to subpoena,
26 and not subject to discovery or admissible in evidence in any private civil action.

27 **SECTION 4. AMENDMENT.** Subsection 1 of section 26.1-02.2-08 of the North Dakota
28 Century Code is amended and reenacted as follows:

- 29 1. The following exceptions apply to this chapter:

John 7 of 7

- 1 a. A licensee with less than five million dollars in gross revenue or less than
2 ten million dollars in year-end assets is exempt from subsections 2 through 10 of
3 section 26.1-02.2-03.
- 4 ~~b. During the period beginning on August 1, 2021, and ending on July 31, 2023, a~~
5 ~~licensee with fewer than fifty employees, including independent contractors and~~
6 ~~employees of affiliated companies having access to nonpublic information used~~
7 ~~by the licensee or in the licensee's possession, custody, or control, is exempt~~
8 ~~from section 26.1-02.2-03.~~
- 9 ~~c. After July 31, 2023, a licensee with fewer than twenty-five employees, including~~
10 ~~independent contractors and employees of affiliated companies having access to~~
11 ~~nonpublic information used by the licensee or in the licensee's possession,~~
12 ~~custody, or control is exempt from section 26.1-02.2-03.~~
- 13 ~~d.b.~~ A licensee that is subject to and, governed by, and compliant with the privacy,
14 security, and breach notification rules issued by the United States department of
15 health and human services, title 45, Code of Federal Regulations, parts 160
16 and 164, established pursuant to the federal Health Insurance Portability and
17 Accountability Act of 1996 [Pub. L. 104-191], and the federal Health Information
18 Technology for Economic and Clinical Health Act [Pub. L. 111-5], and which
19 maintains nonpublic information concerning a consumer in the same manner as
20 protected health information is deemed to comply with the requirements of this
21 chapter ~~except for the commissioner notification requirements under~~
22 ~~subsections 1 and 2 of section 26.1-02.2-05~~section 26.1-02.2-03.
- 23 ~~e.c.~~ An employee, agent, representative, or designee of a licensee, that also is a
24 licensee, is exempt from section 26.1-02.2-03 and is not required to develop an
25 information security program to the extent the employee, agent, representative,
26 or designee is covered by the information security program of the other licensee.

27 **SECTION 5. REPEAL.** Section 26.1-02.2-11 of the North Dakota Century Code is repealed.

**REPORT OF STANDING COMMITTEE
SB 2088**

Industry and Business Committee (Sen. Barta, Chairman) recommends **AMENDMENTS** ([25.8122.01001](#)) and when so amended, recommends **DO PASS** (5 YEAS, 0 NAYS, 0 ABSENT AND NOT VOTING). SB 2088 was placed on the Sixth order on the calendar. This bill does not affect workforce development.

2025 HOUSE INDUSTRY, BUSINESS AND LABOR

SB 2088

2025 HOUSE STANDING COMMITTEE MINUTES

Industry, Business and Labor Committee Room JW327C, State Capitol

SB 2088
3/17/2025

A BILL for an Act to amend and reenact subsection 4 of section 26.1-02.2-01, sections 26.1-02.2-05 and 26.1-02.2-07, and subsection 1 of section 26.1-02.2-08 of the North Dakota Century Code, relating to data security requirements for insurance producers; and to repeal section 26.1-02.2-11 of the North Dakota Century Code, relating to implementation dates for certain data security requirements for insurance producers.

11:01 a. m. Chairman Warrey opened the meeting.

Members Present: Chairman Warrey, Vice Chairman Ostlie, Vice Chairman Johnson, Representatives Bahl, C. Brown, T. Brown, Finley-DeVile, Grindberg, Kasper, Koppelman, D. Ruby, Schatz, Schauer, Vollmer

Discussion Topics:

- National Association of Insurance Commissioners (NAIC) Model law
- SB 2075 67th Legislative Session
- Reporting cybersecurity events
- Close loopholes
- Producer prospective

11:01 a.m. Matt Fischer, Division Director, Company Licensing & Examinations, ND Insurance Department, testified in favor and submitted testimony #42209.

11:19 a.m. Megan Hruby, Blue Cross and Blue Shield of ND, testified in favor.

11:26 a.m. Representative Schauer moved Do Pass.

11:26 a.m. Representative Bahl seconded the motion.

Representatives	Vote
Representative Jonathan Warrey	Y
Representative Mitch Ostlie	Y
Representative Jorin Johnson	Y
Representative Landon Bahl	Y
Representative Collette Brown	Y
Representative Timothy Brown	Y
Representative Lisa Finley-DeVile	Y
Representative Karen Grindberg	Y
Representative Jim Kasper	N
Representative Ben Koppelman	Y
Representative Dan Ruby	Y
Representative Mike Schatz	Y

Representative Austin Schauer	Y
Representative Daniel R. Vollmer	Y

Motion passed 13-1-0.

11:28 a.m. Representative Warrey will carry the bill.

Additional Written Testimony:

Brooke Kelley, American Property Casualty Insurance Association (APCIA), American Council of Life Insurers (ACLI), and National Association of Mutual Insurance Companies (NAMIC), submitted testimony in opposition #41665.

11:28 a.m. Chairman Warrey closed the meeting.

Diane Lillis, Committee Clerk

**REPORT OF STANDING COMMITTEE
ENGROSSED SB 2088 ([25.8122.02000](#))**

Industry, Business and Labor Committee (Rep. Warrey, Chairman) recommends **DO PASS** (13 YEAS, 1 NAY, 0 ABSENT OR EXCUSED AND NOT VOTING). SB 2088 was placed on the Fourteenth order on the calendar.



March 17, 2025

RE: SB 2088 – North Dakota Data Security

Thank you for this opportunity to provide comments on North Dakota Senate Bill 2088. The American Property Casualty Insurance Association (APCIA)¹, the American Council of Life Insurers (ACLI)², and the National Association of Mutual Insurance Companies (NAMIC)³ are committed to strong consumer protections and the safeguarding of sensitive personal information. We appreciate the Insurance Department's robust engagement with stakeholders in pursuing solutions that balance consumer protections with operational feasibility.

However, we have significant concerns about the proposed amendments to North Dakota's data security law and must oppose this bill. These changes would impose substantial challenges on insurers while offering limited additional benefits to consumers.

1. Definition of Cybersecurity Event

Our members oppose the proposed amendment to the definition of "cybersecurity event" and respectfully request that it remain unchanged in the existing law. Altering this definition could lead to unintended consequences, potentially triggering new or inconsistent technical requirements that create compliance challenges without improving consumer protection. Additionally, maintaining the current definition aligns North Dakota's law with other states that have enacted the NAIC Insurance Data Security Model Law, promoting regulatory uniformity and reducing unnecessary burdens on insurers operating in multiple jurisdictions.

2. Revisions to Notice Provisions

¹ APCIA is the primary national trade association for home, auto, and business insurers. APCIA promotes and protects the viability of private competition for the benefit of consumers and insurers, with a legacy dating back 150 years. APCIA represents the broadest cross-section of home, auto, and business insurers of any national trade association.

² ACLI is the leading trade association driving public policy and advocacy on behalf of the life insurance industry. 90 million American families rely on the life insurance industry for financial protection and retirement security. ACLI's member companies are dedicated to protecting consumers' financial wellbeing through life insurance, annuities, retirement plans, long-term care insurance, disability income insurance, reinsurance, and dental, vision and other supplemental benefits. ACLI's 275 member companies represent 93 percent of industry assets in the United States.

³ NAMIC represents nearly 1,500 member companies, including six of the top 10 property/casualty insurers in the United States. NAMIC member companies collectively write more than \$391 billion in annual premiums and represent significant portions of the homeowners, automobile, and business insurance markets, including \$546 million in written premium in the state of North Dakota.

The existing law appropriately limits notification requirements to cybersecurity events that are reasonably likely to cause material harm to insurance licensees or consumers whose sensitive personal information is affected. This standard strikes a crucial balance between meaningful oversight and operational efficiency, ensuring attention is focused on incidents that truly matter.

In contrast, the proposed amendment would create unnecessary administrative burdens and divert resources from addressing genuine threats to consumer protection and cybersecurity. Many instances of unauthorized access are not malicious and pose no risk of harm to consumers. For example, a claims file might be sent to the wrong plaintiff's lawyer, or an employee could inadvertently include sensitive information in an internal email. Such occurrences do not warrant notification, and regulatory departments would neither need nor want to be inundated with these reports.

Equally concerning is the potential ripple effect: requiring notification of insignificant events to North Dakota could trigger notice obligations in other states, amplifying the burden without enhancing consumer protection.

Notably, most states that have enacted the NAIC Insurance Data Security Model Act have adopted similar language, ensuring notification provisions target only events with a meaningful likelihood of harm. Retaining the current standard not only safeguards consumers but also fosters uniformity across jurisdictions, creating a consistent, efficient framework that benefits both insurers and consumers.

3. Removal of Written Consent for Public Disclosure

We also oppose removing the requirement for licensees' prior written consent before public disclosure of sensitive information. While we understand the Department's intention to align this change with statutory requirements for transparency, this change introduces risks without clear consumer benefits.

The Department has stated that confidential documents will still be protected and that examination reports will be shared only after review by the company. However, the absence of a written consent requirement removes a critical safeguard that ensures insurers maintain control over the release of potentially sensitive information. While an opportunity to review the report before publication is valuable, it does not provide the same level of protection as requiring affirmative consent. Even minor inaccuracies or misinterpretations in a public report could have reputational and operational consequences for insurers, especially when cybersecurity-related findings are involved.

Furthermore, IT security concerns are fundamentally different from traditional financial examination findings. Public disclosure of issues—without prior consent—could expose vulnerabilities that bad actors might exploit. Removing consent for publication may inadvertently undermine cybersecurity rather than strengthen oversight.

Conclusion

APCIA, ACLI, and NAMIC all believe in protecting consumers and ensuring strong data security practices. However, the proposed amendments would burden insurers with requirements that provide limited additional consumer protection. We urge the North Dakota legislature to oppose Senate Bill 2088 to maintain the balance between regulatory oversight and operational feasibility that the current law achieves.

By preserving a practical, focused approach to data security, North Dakota can ensure robust consumer protection while supporting an insurance industry that effectively serves its policyholders.

Sincerely,



Brooke Kelley
AVP. State Government Relations
APCIA



Alex Young
Regional Director – State Relations
ACLI



Phillip Arnzen
Regional Vice President- Midwest
NAMIC



TESTIMONY

Matt Fischer, Division Director, Company Licensing & Examinations

House Industry, Business and Labor Committee

March 17, 2025

Good morning, Chairman Warrey 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 unintentionally 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.

Section two includes 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. While this bill was working its way through the Senate a few amendments were made to what you see now. The triggering event language as now proposed is tied to N.D.C.C. § 51-30 which requires notice to a consumer if unencrypted personal information

is acquired by an unauthorized person. This in turn would require the licensee to make a report to our Department if even one consumer where to potentially be harmed.

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.

Section five repeals the staggered implementation dates of the exemptions in the bill as passed in 2021.

For context, during the four years since the passage of this statute, we have seen far fewer reports than would be expected. We have received only 60 reports, of which 21 were associated with the MOVEit breach and only one related to Change. In past 12 months we have only received 12 reports and only 2 since October 2024. In our view, this lack of reporting stems from the unintended issues created by the deviations from the NAIC Model that were made when this law was first passed. At the end of the day, this statute requires licensees to simply report a cybersecurity event to our Department. Based on the number of reports we have received, the average time it takes licensees to complete this form is around 15 minutes. We believe that the changes we are proposing in this bill impose minimal burden on licensees.

To fulfill the Department's mission of serving the needs of North Dakota's insurance consumers, we believe Senate Bill 2088 strengthens our role as a consumer protection agency.

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

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.