21.0198.03002

Sixty-seventh
Legislative Assembly
of North Dakota

HOUSE BILL NO. 1314

Introduced by

Representatives Mock, Bosch, Dockter, Louser, Roers Jones, Toman, Vigesaa, Weisz

Senators Davison, Piepkorn, Vedaa

A BILL for an Act to create and enact a new chapter to title 54 of the North Dakota Century Code, relating to cybersecurity incident reporting requirements.

BE IT ENACTED BY THE LEGISLATIVE ASSEMBLY OF NORTH DAKOTA:

SECTION 1. A new chapter to title 54 of the North Dakota Century Code is created and enacted as follows:

Definitions.

As used in this chapter, unless the context otherwise requires:

1. "Breach" means unauthorized access or acquisition of computerized data that has not been secured by encryption or other methods or technology that renders electronic files, media, or databases unreadable or unusable. Good faith acquisitions of personal information by an employee or agent of the employee is not a breach of security of the system if the personal information is not used or subject to further unauthorized disclosure.
2. "Criminal justice information" means private or sensitive information collected by federal, state, or local law enforcement including the following:
   a. Fingerprints or other biometric information;
   b. Criminal background and investigation information; and
   c. Personal information.
3. "Denial of service attack" means an attack against a computer system designed to make the system inaccessible to users.
4. "Department" means the information technology department.
5. "Entity" means an executive branch state agency or a political subdivision within the state.

6. "Financial information" means banking, credit, or other account information that, if accessed without being authorized, may result in potential harm to an individual and includes:
   a. Account numbers or codes;
   b. Credit card expiration dates;
   c. Credit card security codes;
   d. Bank account statements; and
   e. Records of financial transactions.
7. "Health insurance information" means an individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify an individual.
8. "Identity theft or identity fraud" means all types of crime in which an individual wrongfully obtains and uses another individual's personal data in a way that involves fraud or deception, most commonly for economic gain.
9. "Malware" means software or firmware intended to perform an unauthorized process that will have adverse effect on the confidentiality, integrity, or availability of an information system and includes a virus, worm, trojan horse, spyware, adware, or other code-based system that infects hosts.
10. "Medical information" means an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.
11. "Personal information" means an individual's first name or first initial and last name in combination with the following when names and data are not encrypted, but does not include information available to the public from federal, state, or local government records:
    a. The individual's social security number;
    b. The operator's license number assigned to an individual under section 39-06-14;
    c. A nondriver photo identification card number assigned to the individual under section 39-06-03.1;
    d. The individual's financial institution account number, credit card number, or debit card number in combination with required security codes, access codes, or passwords that permit access to an individual's financial accounts;

e. The individual's date of birth;

f. The maiden name of the individual's mother;

g. Medical information;

h. Health insurance information;

i. An identification number assigned to the individual by the individual's employer in combination with security codes, access codes, or passwords; or

j. The individual's digitized or other electronic signature.

12. "Ransom" means a payment for services or goods to a malicious agent to:

a. Decrypt data on a computer system;

b. Retrieve lost or stolen data; or

c. Prevent the disclosure and dissemination of information.

13. "Regulated information" means information and information technology resource protection requirements established by the federal government and regulating organizations.

14. "Regulating organizations" means organizations that issue laws, regulations, policies, guidelines, and standards, including the:

a. Federal bureau of investigation;

b. Internal revenue service;

c. Social security administration;

d. Federal deposit insurance corporation;

e. United States department of health and human services;

f. Centers for Medicare and Medicaid services; and

g. Payment card industry security standards council.

15. "Significant damage" means:

a. A degradation in or loss of mission capability to an extent and duration that the entity is not able to perform one or more of its primary functions;

b. Damages of ten thousand dollars or more to entity assets as estimated by the entity;

c. A financial loss of ten thousand dollars or more as estimated by the entity; or

d. Harm to individuals involving loss of life or serious life-threatening injuries.

Immediate disclosure to the department.

An entity shall disclose to the department an identified or suspected cybersecurity incident that affects the confidentiality, integrity, or availability of information systems, data, or services. Disclosure must be made in the most expedient time possible and without unreasonable delay. Cybersecurity incidents required to be reported to the department include:

1. Suspected breaches;
2. Malware ~~affecting more than ten thousand dollars worth of devices or services~~incidents that cause significant damage;
3. Denial of service attacks that affect the availability of services;
4. Demands for ransom related to a cybersecurity incident or unauthorized disclosure of digital records;
5. Identify theft or identity fraud services hosted by entity information technology systems;
6. Incidents that require response and remediation efforts that will cost more than ten thousand dollars in equipment, software, and labor; and
7. Other incidents the entity deems worthy of communication to the department.

Ongoing disclosure to the department during a cybersecurity incident.

Until a cybersecurity incident is resolved, an entity shall disclose clarifying details regarding a cybersecurity incident to the department, including:

1. The number of potentially exposed records;
2. The type of records potentially exposed, including health insurance information, medical information, criminal justice information, regulated information, financial information, and personal information;
3. Efforts the entity is undertaking to mitigate and remediate the damage of the incident to the entity and other affected entities; and
4. The expected impact of the incident, including:
   a. The disruption of the entity services;
   b. The effect on customers and employees that experienced data or service losses;
   c. The effect on entities receiving wide area network services from the department; and

d. Other concerns that could potentially disrupt or degrade the confidentiality, integrity, or availability of information systems, data, or services that may affect the state.

Disclosure to the department - Legislative and judicial branches.

The legislative and judicial branches may disclose to the department cybersecurity incidents that affect the confidentiality, integrity, or availability of information systems, data, or services.

Method of disclosure of cybersecurity incidents.

The department shall establish and make known methods an entity must use to securely disclose cybersecurity incidents to the department.

Statewide cybersecurity incident response.

The department, to the extent possible, shall provide consultation services and other resources to assist entities and the legislative and judicial branches in responding to and remediating cybersecurity incidents.

Disclosure to the legislative management.

The department shall report to the legislative management all disclosed cybersecurity incidents as required by this chapter, including the status of the cybersecurity incident and any response or remediation to mitigate the cybersecurity incident. The department shall ensure all reports of disclosed cybersecurity incidents are communicated in a manner that protects victims of cybersecurity incidents, prevents unauthorized disclosure of cybersecurity plans and strategies, and adheres to federal and state laws regarding protection of cybersecurity information.