Publications
June 01, 2014
SECURITY BREACH NOTIFICATION CHART - North Dakota

N.D. Cent. Code § 51-30-01 ***et seq.***

S.B. 2251 (signed into law April 22, 2005)

Effective June 1, 2005

H.B. 1435 (signed into law April 18, 2013)

S.B. 2214 (signed into law April 13, 2015)

Effective August 1, 2015

Application. Any Entity that conducts business in ND and that owns or licenses computerized data that includes PI.

Security Breach Definition. Unauthorized acquisition of computerized data when access to PI has not been secured by encryption or by any other method or technology that renders the electronic files, media, or databases unreadable or unusable.

- Good-faith acquisition of PI by an employee or agent of the Entity is not a breach of the security of the system if the PI is not used or subject to further unauthorized disclosure.

Notification Obligation. Any Entity to which the statute applies shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of ND whose unencrypted PI was, or is reasonably believed to have been, acquired by an unauthorized person.

Attorney General Notification. Any person that experiences a breach of the security system shall disclose to the Attorney General by mail or email any breach of the security system that exceeds 250 individuals.

Third-Party Data Notification. Any person that maintains computerized data that includes PI that the person does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following the discovery if the PI was, or is reasonably believed to have been, acquired by an unauthorized person.

Timing of Notification. In the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and to restore the integrity of the data system.

Personal Information Definition. An individual's first name or first initial and last name in combination with any of the following data elements, when the name and the data elements are not encrypted:

- Social Security number;
- The operator's license number assigned to an individual by the Department of Transportation;
- A non-driver color photo identification card number assigned to the individual by the Department of Transportation;
- An account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial accounts;

- The individual's date of birth;
- The maiden name of the individual's mother;
- Medical information;
- Health insurance information;
- An identification number assigned to the individual by the individual's employer in combination with any required security code, access code, or password; or
- The individual's digitized or other electronic signature.

PI does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Notice Required. Notice may be provided by one of the following methods:

- Written notice; or
- Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 (E-Sign Act).

Substitute Notice Available. If the Entity demonstrates that the cost of providing notice would exceed $250,000, the affected class of subject individuals to be notified exceeds 500,000, or the Entity does not have sufficient contact information. Substitute notice shall consist of all of the following:

- Email notice when the Entity has email addresses for the subject persons;
- Conspicuous posting of the notice on the Entity's website, if the Entity maintains one; and
- Notification to major statewide media.

Exception: Own Notification Policy. An Entity that maintains its own notification procedures as part of an information security policy for the treatment of PI and is otherwise consistent with the timing requirements of this chapter is deemed to be in compliance with the notification requirements of this chapter if the Entity notifies subject individuals in accordance with its policies in the event of a breach of security of the system.

Exception: Compliance with Other Laws.

- **Interagency Guidance.** A financial institution, trust company, or credit union that is subject to, examined for, and in compliance with the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice is deemed to be in compliance with this chapter.
- **HIPAA.** A covered entity, business associate, or subcontractor that is subject to the breach notification requirements of title 45 of the Code of Federal Regulations, part 164, subpart D, is considered to be in compliance with this chapter.

Other Key Provisions:

- **Delay for Law Enforcement.** The notification required by this chapter may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The required notification must be made after the law enforcement agency determines that the notification will not compromise the investigation.
- Attorney General Enforcement.