Publications
June 01, 2014
SECURITY BREACH NOTIFICATION CHART - Nebraska

Neb. Rev. Stat. § 87-801 ***et seq.***

L.B. 876 (signed into law April 10, 2006)

Effective July 14, 2006

L.B. 835 (signed into law April 13, 2016)

Effective July 20, 2016

Application. An individual, government agency, or any other legal entity, whether for profit or not for profit (collectively, Entity), that conducts business in NE and that owns or licenses computerized data that includes PI about a resident of NE.

Security Breach Definition. An unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of PI maintained by an Entity.

- Good-faith acquisition of PI by an employee or agent of an Entity for the purposes 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.
- Acquisition of PI pursuant to a search warrant, subpoena, or other court order or pursuant to a subpoena or order of a state agency is not a breach of the security of the system.

Notification Obligation. Any Entity to which the statute applies shall, when it determines that the use of information about a NE resident for an unauthorized purpose has occurred or is reasonably likely to occur, give notice to the affected NE resident.

- Notification is not required if after a good-faith, reasonable, and prompt investigation the Entity determines that it is unlikely that PI has been or will be used for an unauthorized purpose.

Attorney General Notification. If notice of a security breach to NE residents is required, the Entity shall also, not later than the time when notice is provided to the NE resident, provide notice of the breach of security of the system to the Attorney General.

Third-Party Data Notification. An Entity that maintains computerized data that includes PI that the Entity does not own or license shall give notice to and cooperate with the owner or licensee of the information of any breach of the security of the system when it becomes aware of a breach if use of PI about a NE resident for an unauthorized purpose occurred or is reasonably likely to occur. Cooperation includes, but is not limited to, sharing with the owner or licensee information relevant to the breach, not including information proprietary to the Entity.

Timing of Notification. Notice shall be made as soon as possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system.

Personal Information Definition.

(a) A NE resident's first name or first initial and last name in combination with any one or more of the following data elements that relate to the resident if either the name or the data elements are not encrypted, redacted, or otherwise altered by any method or technology in such a manner that the name or data elements are unreadable:

- Social Security number;
- Driver's license number or state identification card number;
- 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 a resident's financial account;
- Unique electronic ID number or routing code, in combination with any required security code, access code, or password; or
- Unique biometric data, such as a fingerprint, voice print, or retina or iris image, or other unique physical representation; or

(b) A username or email address, in combination with a password or security question and answer, that would permit access to an online account.

Data shall not be considered encrypted if the confidential process or key was or is reasonably believed to have been acquired as a result of the breach of the security of the system.

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;
- Telephonic 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 will exceed $75,000, that the affected class of NE residents to be notified exceeds 100,000 residents, or that the Entity does not have sufficient contact information to provide notice. Substitute notice requires all of the following:

- Email notice, if the Entity has email addresses for the members of the affected class of NE residents;
- Conspicuous posting of the notice on the Entity's website, if it maintains one; and
- Notice to major statewide media.

Substitute Notice Exception. If the Entity has 10 employees or fewer and demonstrates that the cost of providing notice will exceed $10,000. Substitute notice requires all of the following:

- Email notice, if the Entity has email addresses for the members of the affected class of NE residents;
- Notification by a paid advertisement in a local newspaper that is distributed in the geographic area in which the Entity is located, which advertisement shall be of sufficient size that it covers at least one-quarter of a page in the newspaper and shall be published in the newspaper at least once a week for 3 consecutive weeks;
- Conspicuous posting of the notice on the Entity's website, if it maintains one; and
- Notification to major media outlets in the geographic area in which the Entity is located.

Exception: Own Notification Policy. An Entity that maintains its own notice procedures which are part of an information security policy for the treatment of PI and which are otherwise consistent with the timing

requirements of the statute, is deemed to be in compliance with the notice requirements of the statute if the Entity notifies affected NE residents and Attorney General in accordance with its notice procedures in the event of a breach of the security of the system.

Exception: Compliance with Other Laws.

- **Primary Regulator.** An Entity that is regulated by state or federal law and that maintains procedures for a breach of the security of the system pursuant to the laws, rules, regulations, guidance, or guidelines established by its primary or functional state or federal regulator is deemed to be in compliance with the notice requirements of the statute if the Entity notifies affected NE residents and Attorney General in accordance with the maintained procedures in the event of a breach of the security of the system.

Other Key Provisions:

- **Delay for Law Enforcement.** Notice may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation. Notice shall be made in good faith, without unreasonable delay, and as soon as possible after the law enforcement agency determines that notification will no longer impede the investigation.
- **Attorney General Enforcement.** The Attorney General may issue subpoenas and seek and recover direct economic damages for each affected NE resident injured by a violation of the statute.
- Waiver Not Permitted.