Publications
June 01, 2014
SECURITY BREACH NOTIFICATION CHART - Idaho

Idaho Code § 28-51-104 ***et seq.***

S.B. 1374 (signed into law March 30, 2006, Chapter 258)

Effective July 1, 2006

H.B. 566 (signed into law March 31, 2010)

Effective July 1, 2010

Application. Any agency, individual or commercial entity (collectively, Entity) that conducts business in ID and that owns or licenses computerized data that includes PI about a resident of ID.

Security Breach Definition. An illegal acquisition of unencrypted computerized data that materially compromises the security, confidentiality, or integrity of PI for one or more persons maintained by 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, provided that the PI is not used or subject to further unauthorized disclosure.

Notification Obligation. An Entity to which the statute applies shall give notice as soon as possible to the affected ID resident.

- Notification is not required if after a good-faith, reasonable, and prompt investigation the Entity determines that the PI has not been and will not be misused.

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 immediately following discovery of the breach, if misuse of PI about an ID resident occurred or is reasonably likely to occur. Cooperation includes sharing with the owner or licensee information relevant to the breach.

Timing of Notification. Notice must be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach, to identify the individuals affected, and to restore the reasonable integrity of the computerized data system.

Personal Information Definition. An ID 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, when either the name or the data elements are not encrypted:

- Social Security number;
- Driver's license number or state identification card number; or
- Account number or credit card number in combination with any required security code, access code, or password that would permit access to a resident's financial account.

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

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

- Written notice to the most recent address the Entity has in its records;
- 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 required to provide notice demonstrates that the cost of providing notice would exceed $25,000, or that the number of ID residents to be notified exceeds 50,000, or that the Entity does not have sufficient contact information to provide notice. Substitute notice consists of all of the following:

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

Exception: Own Notification Policy. Any Entity that maintains its own notice procedures as part of an information security policy for the treatment of PI, and whose procedures are otherwise consistent with the timing requirements of the statute is deemed to be in compliance with the notice requirements if the Entity notifies affected ID residents in accordance with its policies in the event of a breach of the security of the system.

Exception: Compliance with Other Laws.

- **Primary Regulator.** Notification pursuant to laws, rules, regulations, guidance, or guidelines established by an Entity's primary or functional state regulator is sufficient for compliance.

Penalties. Any Entity that intentionally fails to give notice in accordance with the statute shall be subject to a fine of not more than $25,000 per 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 required by the statute must be made as soon as possible after the law enforcement agency determines that notification will no longer impede the investigation.
- **Primary State Regulator Enforcement.** Authorizes primary state regulator to bring a civil action against an Entity that it believes to have violated the statute by failing to give notice to enforce compliance with the statute and enjoin the Entity from further violation.