Publications
June 01, 2014
SECURITY BREACH NOTIFICATION CHART - Montana

Mont. Code § 2-6-1501 *et seq*, 30-14-1701 *et seq.*, 33-19-321

H.B. 732 (signed into law April 28, 2005, Chapter 518)

Effective March 1, 2006

H.B. 74 (signed into law Feb. 27, 2015)

Effective October 1, 2015

S.B. 50 (signed into law April 24, 2023)

Effective October 1, 2023

Application. Any person or business that conducts business in MT, or state agency (collectively, Entity) that owns or licenses computerized data that includes PI.

Security Breach Definition. Any unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of PI maintained by the Entity and causes or is reasonably believed to cause loss or injury to a MT resident.

- Good-faith acquisition of PI by an employee or agent of the Entity for the purpose of the Entity is not a breach of the security of the data system, provided that the PI is not used or subject to further unauthorized disclosure.

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

Notification of Consumer Reporting Agencies. If a business notifies an individual of a breach and suggests, indicates, or implies that the individual may obtain a credit report, the business must coordinate with the credit reporting agency as to the timing, content and distribution of notice to the individual (but this may not unreasonably delay disclosure of the breach).

Attorney General/Insurance Commissioner Notification. Any Entity that is required to issue a notification shall simultaneously submit an electronic copy of the notification and a statement providing the date and method of distribution of the notification to the Attorney General's Consumer Protection office.

Insurance entities and support organizations must submit the above information to the Montana Insurance Commissioner (Mont. Code § 33-19-321).

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

Timing of Notification. Disclosure is to be made without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

Personal Information Definition.

An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

- Social Security number;
- Driver's license number, state identification card number, or tribal identification card number;
- Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account;
- Medical record information as defined in § 33-19-104 (PI that (a) relates to an individual's physical or mental condition, medical history, medical claims history, or medical treatment; and (b) is obtained from a medical professional or medical care institution, from the individual, or from the individual's spouse, parent, or legal guardian);
- Taxpayer identification number; or
- An identity protection personal identification number issued by the U.S. Internal Revenue Service.

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 would exceed $250,000, or that the affected class of subject persons to be notified exceeds 500,000, or the Entity does not have sufficient contact information. Substitute notice shall consist of email notice when the Entity has email addresses for the subject persons and one of the following:

- Conspicuous posting of the notice on the Entity's website, if the Entity maintains one; or
- Notification to applicable local or 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 that does not unreasonably delay notice is considered to be in compliance with the notification requirements of the statute if the Entity notifies subject persons in accordance with its policies in the event of a breach of security of the data system.

Other Key Provisions:

- **Delay for Law Enforcement.** Notice may be delayed if a law enforcement agency determines that it will impede a criminal investigation and requests a delay in notification. The notification must be made after the law enforcement agency determines that it will not compromise the investigation.