Publications
June 01, 2014

SECURITY BREACH NOTIFICATION CHART - Colorado

Colo. Rev. Stat. § 6-1-716

H.B. 1119 (signed into law April 24, 2006)

Effective September 1, 2006

H.B. 18-1128 (signed into law on May 29, 2018)

Effective September 1, 2018

Application. Any individual or commercial entity (collectively, Entity) that conducts business in CO and that owns, licenses, or maintains computerized data that includes PI.

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 for a purpose unrelated to the lawful operation of the business or is not subject to further unauthorized disclosure.

Notification Obligation. An Entity that owns or licenses the affected PI shall, when it becomes aware of a breach of the security of the system, give notice as soon as possible to the affected CO resident.

- Notification is not required if after a good-faith, prompt, and reasonable investigation, the Entity determines that misuse of PI about a CO resident has not occurred and is not likely to occur.

Attorney General Notification. If notice is provided to more than 500 CO residents, the Entity must provide notice to the Attorney General not later than 30 days after the date of determination that the breach occurred.

Notification to Consumer Reporting Agencies. If an Entity is required to notify more than 1,000 CO residents, the Entity shall also notify, without unreasonable delay, all nationwide consumer reporting agencies of the anticipated date of the notification and the approximate number who are to be notified. This paragraph shall not apply to a person who is subject to Title V of the Gramm-Leach-Bliley Act.

Third-Party Data Notification. If an Entity maintains computerized data that includes PI that the Entity does not own or license, the Entity 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 a breach, if misuse of PI about a CO resident occurred or is likely to occur. Cooperation includes sharing with the owner or licensee information relevant to the breach, except that such cooperation shall not be deemed to require the disclosure of confidential business information or trade secrets.

Timing of Notification. Notice shall be made in the most expedient time possible and without unreasonable delay, but not later than 30 days after the date of determination that the breach occurred, 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 CO 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 the data elements are not encrypted, redacted, or secured by any other method rendering the name or the element unreadable or unusable:

- Social Security number;
- Student, military, or passport ID number;
- Driver's license number or other identification card number;
- Medical information;
- Health insurance identification number; or
- Biometric data;

(b) Username or email address, in combination with a password or security question that would permit access to an online account; or

(c) 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 that 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 postal address listed in the Entity's records;
- Telephonic notice; or
- Electronic notice, if a primary means of communication by the Entity with a CO resident is by electronic means or the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 (E-Sign Act).

For incidents that involve login credentials of an email account furnished by the Entity, notice may not be given to that email address, but may be given by clear and conspicuous notice delivered to the resident online when connected to the account from an IP address or online location from which the Entity knows the resident customarily accesses the account.

The notice must include:

- The date, estimated date, or estimated date range of the breach;
- Type of PI subject to the unauthorized acquisition;
- Information the resident can use to contact the Entity to inquire about the security breach;
- The toll-free telephone numbers, addresses, and websites of the major credit reporting agencies and the Federal Trade Commission; and
- A statement that the resident can obtain information from the Federal Trade Commission and the credit reporting agencies about fraud alerts and security freezes.

For a breach of online account credentials, *in addition to* the information above, the notice must direct the consumer to promptly change his or her password or question and answer, or to take other steps appropriate to protect the online account with the covered Entity and all other online accounts for which the person whose PI has been breached uses the same username or email address and password or security question or answer.

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

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

Exception: Own Notification Policy. Any Entity that maintains its own notification 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 shall be deemed to be in compliance with the notice requirements of the statute if the Entity notifies affected CO customers 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.
- **Gramm-Leach-Bliley Act.** The provisions of this statute shall not apply to any Entity who is subject to Title V of the Gramm-Leach-Bliley Act.

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 and the law enforcement agency has notified the Entity that conducts business in CO not to send notice required by the statute.
- **Attorney General Enforcement.** The Attorney General may seek direct damages and injunctive relief.