

## 6-1-716. Notification of security breach.

(1) **Definitions.** As used in this section, unless the context otherwise requires:

(a) "Breach of the security of the system" means the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by an individual or a commercial entity. Good faith acquisition of personal information by an employee or agent of an individual or commercial entity for the purposes of the individual or commercial entity is not a breach of the security of the system if the personal information is not used for or is not subject to further unauthorized disclosure.

(b) "Commercial entity" means any private legal entity, whether for-profit or not-for-profit.

(c) "Notice" means:

(I) Written notice to the postal address listed in the records of the individual or commercial entity;

(II) Telephonic notice;

(III) Electronic notice, if a primary means of communication by the individual or commercial entity with a Colorado 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. sec. 7001 et seq.; or

(IV) Substitute notice, if the individual or the commercial entity required to provide notice demonstrates that the cost of providing notice will exceed two hundred fifty thousand dollars, the affected class of persons to be notified exceeds two hundred fifty thousand Colorado residents, or the individual or the commercial entity does not have sufficient contact information to provide notice. Substitute notice consists of all of the following:

(A) E-mail notice if the individual or the commercial entity has e-mail addresses for the members of the affected class of Colorado residents;

(B) Conspicuous posting of the notice on the web site page of the individual or the commercial entity if the individual or the commercial entity maintains one; and

(C) Notification to major statewide media.

(d) (I) "Personal information" means a Colorado 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:

(A) Social security number;

(B) Driver's license number or identification card number;

(C) Account number or credit 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.

(II) "Personal information" 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.

(2) **Disclosure of breach.** (a) An individual or a commercial entity that conducts business in Colorado and that owns or licenses computerized data that includes personal information about a resident of Colorado shall, when it becomes aware of a breach of the security of the system, conduct in good faith a prompt investigation to determine the likelihood that personal information has been or will be misused. The individual or the commercial entity shall give notice as soon as possible to the affected Colorado resident unless the investigation determines that the misuse of information about a Colorado resident has not occurred and is not reasonably likely to occur. Notice shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system.

(b) An individual or a commercial entity that maintains computerized data that includes personal information that the individual or the commercial 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 a breach, if misuse of personal information about a Colorado 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.

(c) Notice required by this section 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 individual or commercial entity that conducts business in Colorado not to send notice required by this section. Notice required by this section 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 and has notified the individual or commercial entity that conducts business in Colorado that it is appropriate to send the notice required by this section.

(d) If an individual or commercial entity is required to notify more than one thousand Colorado residents of a breach of the security of the system pursuant to this section, the individual or commercial entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by 15 U.S.C. sec. 1618a (p), of the anticipated date of the notification to the residents and the approximate number of residents who are to be notified. Nothing in this paragraph (d) shall be construed to require the individual or commercial entity to provide to the consumer reporting agency the names or other personal information of breach notice recipients. This paragraph (d) shall not apply to a person who is subject to title V of the federal "Gramm-Leach-Bliley Act", 15 U.S.C. sec. 6801 et seq.

(3) **Procedures deemed in compliance with notice requirements.** (a) Under this section, an individual or a commercial entity that maintains its own notification procedures as part of an information security policy for the treatment of personal information and whose procedures are otherwise consistent with the timing requirements of this section shall be deemed to be in compliance with the notice requirements of this section if the individual or the commercial entity notifies affected Colorado customers in accordance with its policies in the event of a breach of security of the system.

(b) An individual or a commercial 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, guidances, or guidelines established by its primary or functional state or federal regulator is deemed to be in compliance with this section.

(4) **Violations.** The attorney general may bring an action in law or equity to address violations of this section and for other relief that may be appropriate to ensure compliance with this section or to recover direct economic damages resulting from a violation, or both. The provisions of this section are not exclusive and do not relieve an individual or a commercial entity subject to this section from compliance with all other

applicable provisions of law.

**Source: L. 2006:** Entire section added, p. 536, § 1, effective September 1.