C.R.S. 6-1-716

Statutes current through Chapter 52 of the 2024 Regular Session, effective as of April 4, 2024. The 2024 legislative changes are not final until compared and reconciled to the 2024 work product of the Colorado Office of Legislative Services later in 2024.

6-1-716. Notification of security breach.

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

(a) "Biometric data" means unique biometric data generated from measurements or analysis of human body characteristics for the purpose of authenticating the individual when he or she accesses an online account.

(b) "Covered entity" means a person, as defined in section 6-1-102 (6), that maintains, owns, or licenses personal information in the course of the person's business, vocation, or occupation. "Covered entity" does not include a person acting as a third-party service provider as defined in subsection (1)(i) of this section.

(c) "Determination that a security breach occurred" means the point in time at which there is sufficient evidence to conclude that a security breach has taken place.

(d) "Encrypted" means rendered unusable, unreadable, or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security.

(e) "Medical information" means any information about a consumer's medical or mental health treatment or diagnosis by a health-care professional.

(f) "Notice" means:

(I) Written notice to the postal address listed in the records of the covered entity;

(II) Telephonic notice;

(III) Electronic notice, if a primary means of communication by the covered 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 the federal "Electronic Signatures in Global and National Commerce Act", 15 U.S.C. sec. 7001 et seq.; or

(IV) Substitute notice, if the covered 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 covered entity does not have sufficient contact information to provide notice. Substitute notice consists of all of the following:

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

(B) Conspicuous posting of the notice on the website page of the covered entity if the covered entity maintains one; and

(C) Notification to major statewide media.

(g)

(I)

(A) "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: Social security number; student, military, or passport identification number; driver's license number or identification card number; medical information; health insurance identification number; or biometric data;

(B) A Colorado resident's username or e-mail address, in combination with a password or security questions and answers, that would permit access to an online account; or

(C) A Colorado resident's account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to that 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.

(h) "Security breach" means the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a covered entity. Good faith acquisition of personal information by an employee or agent of a covered entity for the covered entity's business purposes is not a security breach if the personal information is not used for a purpose unrelated to the lawful operation of the business or is not subject to further unauthorized disclosure.

(i) "Third-party service provider" means an entity that has been contracted to maintain, store, or process personal information on behalf of a covered entity.

(2) Disclosure of breach.

(a) A covered entity that maintains, owns, or licenses computerized data that includes personal information about a resident of Colorado shall, when it becomes aware that a security breach may have occurred, conduct in good faith a prompt investigation to determine the likelihood that personal information has been or will be misused. The covered entity shall give notice to the affected Colorado residents unless the investigation determines that the misuse of information about a Colorado resident has not occurred and is not reasonably likely to occur. Notice must be made in the most expedient time possible and without unreasonable delay, but not later than thirty days after the date of determination that a security breach occurred,

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.

(a.2) In the case of a breach of personal information, notice required by this subsection (2) to affected Colorado residents must include, but need not be limited to, the following information:

(I) The date, estimated date, or estimated date range of the security breach;

(II) A description of the personal information that was acquired or reasonably believed to have been acquired as part of the security breach;

(III) Information that the resident can use to contact the covered entity to inquire about the security breach;

(IV) The toll-free numbers, addresses, and websites for consumer reporting agencies;

(V) The toll-free number, address, and website for the federal trade commission; and

(VI) A statement that the resident can obtain information from the federal trade commission and the credit reporting agencies about fraud alerts and security freezes.

(a.3) If an investigation by the covered entity pursuant to subsection (2)(a) of this section determines that the type of personal information described in subsection (1)(g)(I)(B) of this section has been misused or is reasonably likely to be misused, then the covered entity shall, in addition to the notice otherwise required by subsection (2)(a.2) of this section and in the most expedient time possible and without unreasonable delay, but not later than thirty days after the date of determination that a security breach occurred, 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:

(I) Direct the person whose personal information has been breached to promptly change his or her password and security question or answer, as applicable, 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 personal information has been breached uses the same username or e-mail address and password or security question or answer.

(II) For log-in credentials of an e-mail account furnished by the covered entity, the covered entity shall not comply with this section by providing the security breach notification to that e-mail address, but may instead comply with this section by providing notice through other methods, as defined in subsection (1)(f) of this section, or by clear and conspicuous notice delivered to the resident online when the resident is connected to the online account from an internet protocol address or online location from which the covered entity knows the resident customarily accesses the account.

(a.4) The breach of encrypted or otherwise secured personal information must be disclosed in accordance with this section if the confidential process, encryption key, or other means to decipher the secured information was also acquired in the security breach or was reasonably believed to have been acquired.

(a.5)A covered entity that is required to provide notice to affected Colorado residents pursuant to this subsection (2) is prohibited from charging the cost of providing such notice to such residents.

(a.6) Nothing in this subsection (2) prohibits the notice described in this subsection (2) from containing additional information, including any information that may be required by state or federal law.

(b) If a covered entity uses a third-party service provider to maintain computerized data that includes personal information, then the third-party service provider shall give notice to and cooperate with the covered entity in the event of a security breach that compromises such computerized data, including notifying the covered entity of any security breach in the most expedient time possible, and without unreasonable delay following discovery of a security breach, if misuse of personal information about a Colorado resident occurred or is likely to occur. Cooperation includes sharing with the covered entity information relevant to the security breach; except that such cooperation does not 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 covered entity that conducts business in Colorado not to send notice required by this section. Notice required by this section must be made in good faith, in the most expedient time possible and without unreasonable delay, but not later than thirty days after the law enforcement agency determines that notification will no longer impede the investigation and has notified the covered entity that conducts business in Colorado that it is appropriate to send the notice required by this section.

(d) If a covered entity is required to notify more than one thousand Colorado residents of a security breach pursuant to this section, the covered entity shall also notify, in the most expedient time possible and without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by the federal "Fair Credit Reporting Act", 15 U.S.C. sec. 1681a (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 subsection (2)(d) requires the covered entity to provide to the consumer reporting agency the names or other personal information of security breach notice recipients. This subsection (2)(d) does not apply to a covered entity who is subject to Title V of the federal "Gramm-Leach-Bliley Act", 15 U.S.C. sec. 6801 et seq.

(e) A waiver of these notification rights or responsibilities is void as against public policy.

(f)

(I) The covered entity that must notify Colorado residents of a data breach pursuant to this section shall provide notice of any security breach to the Colorado attorney general in the most expedient time possible and without unreasonable delay, but not later than thirty days after the date of determination that a security breach occurred, if the security breach is reasonably believed to have affected five hundred Colorado residents or more, unless the investigation determines that the misuse of information about a Colorado resident has not occurred and is not likely to occur.

(II) The Colorado attorney general shall designate a person or persons as a point of contact for functions set forth in this subsection (2)(f) and shall make the contact information for that person or those persons public on the attorney general's website and by any other appropriate means.

(g) The breach of encrypted or otherwise secured personal information must be disclosed in accordance with this section if the confidential process, encryption key, or other means to decipher the secured information was also acquired or was reasonably believed to have been acquired in the security breach.

(3) Procedures deemed in compliance with notice requirements.

(a) Pursuant to this section, a covered 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 is in compliance with the notice requirements of this section if the covered entity notifies affected Colorado residents in accordance with its policies in the event of a security breach; except that notice to the attorney general is still required pursuant to subsection (2)(f) of this section.

(b) A covered entity that is regulated by state or federal law and that maintains procedures for a security breach pursuant to the laws, rules, regulations, guidances, or guidelines established by its state or federal regulator is in compliance with this section; except that notice to the attorney general is still required pursuant to subsection (2)(f) of this section. In the case of a conflict between the time period for notice to individuals that is required pursuant to this subsection (3) and the applicable state or federal law or regulation, the law or regulation with the shortest time frame for notice to the individual controls.

(4) Violations. The attorney general may bring an action in law or equity to address violations of this section, section 6-1-713, or section 6-1-713.5, 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 a covered entity subject to this section from compliance with all other applicable provisions of law.

(5) Attorney general criminal authority. Upon receipt of notice pursuant to subsection (2) of this section, and with either a request from the governor to prosecute a particular case or with the approval of the district attorney with jurisdiction to prosecute cases in the judicial district where a case could be brought, the attorney general has the authority to prosecute any criminal violations of section 18-5.5-102.

History

Source: L. 2006: Entire section added, p. 536, § 1, effective September 1. **L. 2010:**(2)(d) amended,(HB 10-1422), ch. 419, p. 2064, § 9, effective August 11. **L. 2018:**(1) R&RE, (2), (3), and (4) amended, and (5) added,(HB 18-1128), ch. 266, p. 1634, § 3, effective September 1.

Colorado Revised Statutes Annotated
Copyright © 2024 All rights reserved.

End of Document