

California Civil Code

Division 3 – Obligations

Part 4 – Obligations Arising from Particular Transactions

Title 1.8 – Personal Data

Chapter 1 – Information Practices Act of 1977

Article 7 – Accounting of Disclosures

§ 1798.29

(a) Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(e) For purposes of this section, "personal information" means 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:

- (1) Social security number.
- (2) Driver's license number or California Identification Card number.
- (3) Account number, 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.

(f) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(g) For purposes of this section, "notice" may be provided by one of the following methods:

- (1) Written notice.
- (2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.
- (3) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars (\$250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information. Substitute notice shall consist of all of the following:

- (A) E-mail notice when the person or business has an e-mail address for the subject persons.
- (B) Conspicuous posting of the notice on the Web site page of the person or business, if the person or business maintains one.
- (C) Notification to major statewide media.

(h) Notwithstanding subdivision (g), a person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part, shall be deemed to be in compliance with the notification requirements of this section if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system.

California Civil Code

Division 3 – Obligations

Part 4 – Obligations Arising from Particular Transactions

Title 1.81 – Customer Records

§ 1798.80. The following definitions apply to this title:

(a) "Business" means a sole proprietorship, partnership, corporation, association, or other group, however organized and whether or not organized to operate at a profit, including financial institution organized, chartered, or holding a license or authorization certificate under the law of this state, any other state, the United States, or of any other country, or the parent or the subsidiary of a financial institution. The term includes an entity that destroys records.

(b) "Records" means any material, regardless of the physical form, on which information is recorded or preserved by any means, including in written or spoken words, graphically depicted, printed, or electromagnetically transmitted. "Records" does not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, such as name, address, or telephone number.

(c) "Customer" means an individual who provides personal information to a business for the purpose of purchasing or leasing a product or obtaining a service from the business.

(d) "Individual" means a natural person.

(e) "Personal information" means any information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, his or her name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information.

§ 1798.81. A business shall take all reasonable steps to destroy, or arrange for the destruction of a customer's records within its custody or control containing personal information which is no longer to be retained by the business by (1) shredding, (2) erasing, or (3) otherwise modifying the personal information in those records to make it unreadable or undecipherable through any means.

1798.81.5.

(a) It is the intent of the Legislature to ensure that personal information about California residents is protected. To that end, the purpose of this section is to encourage businesses that own or license personal information about Californians to provide reasonable security for that information. For the purpose of this section, the phrase "owns or licenses" is intended to include, but is not limited to, personal information that a business retains as part of the business' internal customer account or for the purpose of using that information in transactions with the person to whom the information relates.

(b) A business that owns or licenses personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.

(c) A business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party shall require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.

(d) For purposes of this section, the following terms have the following meanings:

(1) "Personal information" means an individual's first name or first initial and his or her 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 or redacted:

- (A) Social security number.
- (B) Driver's license number or California identification card number.
- (C) Account number, 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.
- (D) Medical information.

(2) "Medical information" means any individually identifiable information, in electronic or physical form, regarding the individual's medical history or medical treatment or diagnosis by a health care professional.

(3) "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(e) The provisions of this section do not apply to any of the following:

(1) A provider of health care, health care service plan, or contractor regulated by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1).

(2) A financial institution as defined in Section 4052 of the Financial Code and subject to the California Financial Information Privacy Act (Division 1.2 (commencing with Section 4050) of the Financial Code.

(3) A covered entity governed by the medical privacy and security rules issued by the federal Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Availability Act of 1996 (HIPAA).

(4) An entity that obtains information under an agreement pursuant to Article 3 (commencing with Section 1800) of Chapter 1 of Division 2 of the Vehicle Code and is subject to the confidentiality requirements of the Vehicle Code.

(5) A business that is regulated by state or federal law providing greater protection to personal information than that provided by this section in regard to the subjects addressed by this section. Compliance with that state or federal law shall be deemed compliance with this section with regard to those subjects. This paragraph does not relieve a business from a duty to comply with any other

requirements of other state and federal law regarding the protection and privacy of personal information.

§ 1798.82.

(a) Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(e) For purposes of this section, "personal information" means 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:

- (1) Social security number.
- (2) Driver's license number or California Identification Card number.
- (3) Account number, 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.

(f) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(g) For purposes of this section, "notice" may be provided by one of the following methods:

- (1) Written notice.
- (2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.
- (3) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars (\$250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information. Substitute notice shall consist of all of the following:

- (A) E-mail notice when the person or business has an e-mail address for the subject persons.
- (B) Conspicuous posting of the notice on the Web site page of the person or business, if the person or business maintains one.
- (C) Notification to major statewide media.

(h) Notwithstanding subdivision (g), a person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part, shall be deemed to be in compliance with the notification requirements of this section if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system.

§ 1798.84

(a) Any waiver of a provision of this title is contrary to public policy and is void and unenforceable.

(b) Any customer injured by a violation of this title may institute a civil action to recover damages.

(c) In addition, for a willful, intentional, or reckless violation of Section 1798.83, a customer may recover a civil penalty not to exceed three thousand dollars (\$3,000) per violation; otherwise, the customer may recover a civil penalty of up to five hundred dollars (\$500) per violation for a violation of Section 1798.83.

(d) Unless the violation is willful, intentional, or reckless, a business that is alleged to have not provided all the information required by subdivision (a) of Section 1798.83, to have provided inaccurate information, failed to provide any of the information required by subdivision (a) of Section 1798.83, or failed to provide information in the time period

required by subdivision (b) of Section 1798.83, may assert as a complete defense in any action in law or equity that it thereafter provided regarding the information that was alleged to be untimely, all the information, or accurate information, to all customers who were provided incomplete or inaccurate information, respectively, within 90 days of the date the business knew that it had failed to provide the information, timely information, all the information, or the accurate information, respectively.

(e) Any business that violates, proposes to violate, or has violated this title may be enjoined.

(f) A prevailing plaintiff in any action commenced under Section 1798.83 shall also be entitled to recover his or her reasonable attorney's fees and costs.

(g) The rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under law.