



Home	Bill Information	California Law	Publications	Other Resources	My Subscriptions	My Favorites
------	------------------	----------------	--------------	-----------------	------------------	--------------

Code:  Section:

[Up^](#) [Add To My Favorites](#)

**CIVIL CODE - CIV**

**DIVISION 3. OBLIGATIONS [1427 - 3273.69]** ( *Heading of Division 3 amended by Stats. 1988, Ch. 160, Sec. 14. )*

**PART 4. OBLIGATIONS ARISING FROM PARTICULAR TRANSACTIONS [1738 - 3273.69]** ( *Part 4 enacted 1872. )*

**TITLE 1.81. CUSTOMER RECORDS [1798.80 - 1798.84]** ( *Title 1.81 added by Stats. 2000, Ch. 1039, Sec. 1. )*

**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 a 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 disposes of 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, medical information, or health insurance information. "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(Amended by Stats. 2009, Ch. 134, Sec. 1. (AB 1094) Effective January 1, 2010.)

**1798.81.** A business shall take all reasonable steps to dispose, or arrange for the disposal, of customer records within its custody or control containing personal information when the records are no longer to be retained by the business by (a) shredding, (b) erasing, or (c) otherwise modifying the personal information in those records to make it unreadable or undecipherable through any means.

(Amended by Stats. 2009, Ch. 134, Sec. 2. (AB 1094) Effective January 1, 2010.)

**1798.81.5.** (a) (1) 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, license, or maintain personal information about Californians to provide reasonable security for that information.

(2) For the purpose of this section, the terms "own" and "license" include 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. The term "maintain" includes personal information that a business maintains but does not own or license.

(b) A business that owns, licenses, or maintains 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 that is not subject to subdivision (b) 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 either of the following:

(A) An individual's first name or first initial and the individual's 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:

(i) Social security number.

(ii) Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual.

(iii) 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.

(iv) Medical information.

(v) Health insurance information.

(vi) Unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes.

(vii) Genetic data.

(B) A username or email address in combination with a password or security question and answer that would permit access to an online account.

(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) "Health insurance information" means an individual's insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

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

(5) "Genetic data" means any data, regardless of its format, that results from the analysis of a biological sample of an individual, or from another source enabling equivalent information to be obtained, and concerns genetic material. Genetic material includes, but is not limited to, deoxyribonucleic acids (DNA), ribonucleic acids (RNA), genes, chromosomes, alleles, genomes, alterations or modifications to DNA or RNA, single nucleotide polymorphisms (SNPs), uninterpreted data that results from analysis of the biological sample or other source, and any information extrapolated, derived, or inferred therefrom.

(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 1.4 (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.

**1798.81.6.** (a) A consumer credit reporting agency, as defined in 15 U.S.C. Sec. 1681a(p), that owns, licenses, or maintains personal information about a California resident, or a third party that maintains personal information about a California resident on behalf of a consumer credit reporting agency, that knows, or reasonably should know, that a computer system it owns, operates, or maintains, and for which it controls the security protocols, is subject to a security vulnerability that poses a significant risk, as defined in subdivision (c), to the security of computerized data that contains personal information, as defined in subdivision (h) of Section 1798.82, shall do all of the following:

(1) If a consumer credit reporting agency knows or reasonably should know that a software update is available to address the vulnerability as described in subdivision (a), the agency shall begin the necessary testing, planning, and assessment of its systems for implementation of that software update in the most expedient time possible and without unreasonable delay, in keeping with industry best practices, but in any case no later than three business days after becoming aware, or after the point at which it reasonably should have become aware, of the vulnerability and the available software update. The software update shall be completed in the most expedient time possible and without unreasonable delay, in keeping with industry best practices, but in any case no later than 90 days after becoming aware, or after the point at which it reasonably should have become aware, of the vulnerability and the available software update.

(2) Until the software update described in paragraph (1) is complete, the consumer credit reporting agency shall, in keeping with industry best practices, employ reasonable compensating controls to reduce the risk of a breach caused by computer system vulnerability as described in subdivision (a).

(b) Notwithstanding whether a software update is available, the consumer credit reporting agency, in keeping with industry best practices, shall do all of the following:

(1) Identify, prioritize, and address the highest risk security vulnerabilities most quickly in order to reduce the likelihood that the vulnerabilities that pose the greatest security risk will be exploited.

(2) Test and evaluate the impact of compensating controls and software updates and how they affect the vulnerability of the system to threats to the security of computerized data.

(3) Require, by contract, that the third party implement and maintain appropriate security measures for personal information. Contracting with a third party to maintain personal information about California residents shall not relieve the consumer credit agency of the requirements of this section.

(c) As used in this section, "significant risk" means a vulnerability score, calculated using a standard measurement system that is accepted as a best practice for the industry, to determine that the risk could reasonably result in a breach of the security of the system, as defined in subdivision (g) of Section 1798.82, of personal information, as defined in subdivision (h) of Section 1798.82.

(d) As used in this section, "compensating controls" means controls that the agency reasonably believes will prevent the computer system vulnerability as described in subdivision (a) from being exploited while the software update is being tested, assessed, and a plan for implementation is being developed, and have been adequately tested and confirmed to sufficiently offset the risk of breach caused by computer system vulnerability as described in subdivision (a).

(e) Nothing in this section shall reduce the responsibilities and obligations of a consumer credit reporting agency or third party under this title, including, but not limited to, Section 1798.81.5.

(f) The Attorney General has exclusive authority to enforce this section.

*(Added by Stats. 2018, Ch. 532, Sec. 1. (AB 1859) Effective January 1, 2019.)*

**1798.82.** (a) A person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California (1) whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person, or, (2) whose encrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the encryption key or security credential was, or is reasonably believed to have been, acquired by an unauthorized person and the person or business that owns or licenses the encrypted information has a reasonable belief that the encryption key or security credential could render that personal information readable or usable. 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) A 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 the 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 promptly after the law enforcement agency determines that it will not compromise the investigation.

(d) A person or business that is required to issue a security breach notification pursuant to this section shall meet all of the following requirements:

(1) The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described in paragraph (2) under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.

(A) The format of the notice shall be designed to call attention to the nature and significance of the information it contains.

(B) The title and headings in the notice shall be clearly and conspicuously displayed.

(C) The text of the notice and any other notice provided pursuant to this section shall be no smaller than 10-point type.

(D) For a written notice described in paragraph (1) of subdivision (j), use of the model security breach notification form prescribed below or use of the headings described in this paragraph with the information described in paragraph (2), written in plain language, shall be deemed to be in compliance with this subdivision.

[NAME OF INSTITUTION / LOGO] _____ Date: [insert date]	
NOTICE OF DATA BREACH	
What Happened?	
What Information Was Involved?	
What We Are Doing.	
What You Can Do.	
Other Important Information. [insert other important information]	

For More Information.	Call [telephone number] or go to [internet website]
-----------------------	---

(E) For an electronic notice described in paragraph (2) of subdivision (j), use of the headings described in this paragraph with the information described in paragraph (2), written in plain language, shall be deemed to be in compliance with this subdivision.

(2) The security breach notification described in paragraph (1) shall include, at a minimum, the following information:

(A) The name and contact information of the reporting person or business subject to this section.

(B) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

(C) If the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred. The notification shall also include the date of the notice.

(D) Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.

(E) A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

(F) The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number.

(G) If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed personal information defined in subparagraphs (A) and (B) of paragraph (1) of subdivision (h).

(3) At the discretion of the person or business, the security breach notification may also include any of the following:

(A) Information about what the person or business has done to protect individuals whose information has been breached.

(B) Advice on steps that people whose information has been breached may take to protect themselves.

(C) In breaches involving biometric data, instructions on how to notify other entities that used the same type of biometric data as an authenticator to no longer rely on data for authentication purposes.

(e) A covered entity under the federal Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. Sec. 1320d et seq.) will be deemed to have complied with the notice requirements in subdivision (d) if it has complied completely with Section 13402(f) of the federal Health Information Technology for Economic and Clinical Health Act (Public Law 111-5). However, nothing in this subdivision shall be construed to exempt a covered entity from any other provision of this section.

(f) A person or business that is required to issue a security breach notification pursuant to this section to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. A single sample copy of a security breach notification shall not be deemed to be within Article 1 (commencing with Section 7923.600) of Chapter 1 of Part 5 of Division 10 of Title 1 of the Government Code.

(g) 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.

(h) For purposes of this section, "personal information" means either of the following:

(1) 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:

(A) Social security number.

(B) Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual.

(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 an individual's financial account.

(D) Medical information.

(E) Health insurance information.

(F) Unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes.

(G) Information or data collected through the use or operation of an automated license plate recognition system, as defined in Section 1798.90.5.

(H) Genetic data.

(2) A username or email address, in combination with a password or security question and answer that would permit access to an online account.

(i) (1) 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.

(2) For purposes of this section, "medical information" means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

(3) For purposes of this section, "health insurance information" means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

(4) For purposes of this section, "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.

(5) "Genetic data" means any data, regardless of its format, that results from the analysis of a biological sample of an individual, or from another source enabling equivalent information to be obtained, and concerns genetic material. Genetic material includes, but is not limited to, deoxyribonucleic acids (DNA), ribonucleic acids (RNA), genes, chromosomes, alleles, genomes, alterations or modifications to DNA or RNA, single nucleotide polymorphisms (SNPs), uninterpreted data that results from analysis of the biological sample or other source, and any information extrapolated, derived, or inferred therefrom.

(j) 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) Email notice when the person or business has an email address for the subject persons.

(B) Conspicuous posting, for a minimum of 30 days, of the notice on the internet website page of the person or business, if the person or business maintains one. For purposes of this subparagraph, conspicuous posting on the person's or business's

internet website means providing a link to the notice on the home page or first significant page after entering the internet website that is in larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size, or set off from the surrounding text of the same size by symbols or other marks that call attention to the link.

(C) Notification to major statewide media.

(4) In the case of a breach of the security of the system involving personal information defined in paragraph (2) of subdivision (h) for an online account, and no other personal information defined in paragraph (1) of subdivision (h), the person or business may comply with this section by providing the security breach notification in electronic or other form that directs the person whose personal information has been breached promptly to change the person's password and security question or answer, as applicable, or to take other steps appropriate to protect the online account with the person or business and all other online accounts for which the person whose personal information has been breached uses the same username or email address and password or security question or answer.

(5) In the case of a breach of the security of the system involving personal information defined in paragraph (2) of subdivision (h) for login credentials of an email account furnished by the person or business, the person or business shall not comply with this section by providing the security breach notification to that email address, but may, instead, comply with this section by providing notice by another method described in this subdivision 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 person or business knows the resident customarily accesses the account.

(k) For purposes of this section, "encryption key" and "security credential" mean the confidential key or process designed to render data usable, readable, and decipherable.

(l) Notwithstanding subdivision (j), 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.

*(Amended by Stats. 2022, Ch. 28, Sec. 23. (SB 1380) Effective January 1, 2023.)*

**1798.83.** (a) Except as otherwise provided in subdivision (d), if a business has an established business relationship with a customer and has within the immediately preceding calendar year disclosed personal information that corresponds to any of the categories of personal information set forth in paragraph (6) of subdivision (e) to third parties, and if the business knows or reasonably should know that the third parties used the personal information for the third parties' direct marketing purposes, that business shall, after the receipt of a written or electronic mail request, or, if the business chooses to receive requests by toll-free telephone or facsimile numbers, a telephone or facsimile request from the customer, provide all of the following information to the customer free of charge:

(1) In writing or by electronic mail, a list of the categories set forth in paragraph (6) of subdivision (e) that correspond to the personal information disclosed by the business to third parties for the third parties' direct marketing purposes during the immediately preceding calendar year.

(2) In writing or by electronic mail, the names and addresses of all of the third parties that received personal information from the business for the third parties' direct marketing purposes during the preceding calendar year and, if the nature of the third parties' business cannot reasonably be determined from the third parties' name, examples of the products or services marketed, if known to the business, sufficient to give the customer a reasonable indication of the nature of the third parties' business.

(b) (1) A business required to comply with this section shall designate a mailing address, electronic mail address, or, if the business chooses to receive requests by telephone or facsimile, a toll-free telephone or facsimile number, to which customers may deliver requests pursuant to subdivision (a). A business required to comply with this section shall, at its election, do at least one of the following:

(A) Notify all agents and managers who directly supervise employees who regularly have contact with customers of the designated addresses or numbers or the means to obtain those addresses or numbers and instruct those employees that customers who inquire about the business's privacy practices or the business's compliance with this section shall be informed of the designated addresses or numbers or the means to obtain the addresses or numbers.

(B) Add to the home page of its Web site a link either to a page titled "Your Privacy Rights" or add the words "Your Privacy Rights" to the home page's link to the business's privacy policy. If the business elects to add the words "Your Privacy Rights" to the link to the business's privacy policy, the words "Your Privacy Rights" shall be in the same style and size as the link to the business's privacy policy. If the business does not display a link to its privacy policy on the home page of its Web site, or does not have a privacy policy, the words "Your Privacy Rights" shall be written in larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size, or set off from the surrounding text of the same size by

symbols or other marks that call attention to the language. The first page of the link shall describe a customer's rights pursuant to this section and shall provide the designated mailing address, e-mail address, as required, or toll-free telephone number or facsimile number, as appropriate. If the business elects to add the words "Your California Privacy Rights" to the home page's link to the business's privacy policy in a manner that complies with this subdivision, and the first page of the link describes a customer's rights pursuant to this section, and provides the designated mailing address, electronic mailing address, as required, or toll-free telephone or facsimile number, as appropriate, the business need not respond to requests that are not received at one of the designated addresses or numbers.

(C) Make the designated addresses or numbers, or means to obtain the designated addresses or numbers, readily available upon request of a customer at every place of business in California where the business or its agents regularly have contact with customers.

The response to a request pursuant to this section received at one of the designated addresses or numbers shall be provided within 30 days. Requests received by the business at other than one of the designated addresses or numbers shall be provided within a reasonable period, in light of the circumstances related to how the request was received, but not to exceed 150 days from the date received.

(2) A business that is required to comply with this section and Section 6803 of Title 15 of the United States Code may comply with this section by providing the customer the disclosure required by Section 6803 of Title 15 of the United States Code, but only if the disclosure also complies with this section.

(3) A business that is required to comply with this section is not obligated to provide information associated with specific individuals and may provide the information required by this section in standardized format.

(c) (1) A business that is required to comply with this section is not obligated to do so in response to a request from a customer more than once during the course of any calendar year. A business with fewer than 20 full-time or part-time employees is exempt from the requirements of this section.

(2) If a business that is required to comply with this section adopts and discloses to the public, in its privacy policy, a policy of not disclosing personal information of customers to third parties for the third parties' direct marketing purposes unless the customer first affirmatively agrees to that disclosure, or of not disclosing the personal information of customers to third parties for the third parties' direct marketing purposes if the customer has exercised an option that prevents that information from being disclosed to third parties for those purposes, as long as the business maintains and discloses the policies, the business may comply with subdivision (a) by notifying the customer of his or her right to prevent disclosure of personal information, and providing the customer with a cost-free means to exercise that right.

(d) The following are among the disclosures not deemed to be disclosures of personal information by a business for a third party's direct marketing purposes for purposes of this section:

(1) Disclosures between a business and a third party pursuant to contracts or arrangements pertaining to any of the following:

(A) The processing, storage, management, or organization of personal information, or the performance of services on behalf of the business during which personal information is disclosed, if the third party that processes, stores, manages, or organizes the personal information does not use the information for a third party's direct marketing purposes and does not disclose the information to additional third parties for their direct marketing purposes.

(B) Marketing products or services to customers with whom the business has an established business relationship where, as a part of the marketing, the business does not disclose personal information to third parties for the third parties' direct marketing purposes.

(C) Maintaining or servicing accounts, including credit accounts and disclosures pertaining to the denial of applications for credit or the status of applications for credit and processing bills or insurance claims for payment.

(D) Public record information relating to the right, title, or interest in real property or information relating to property characteristics, as defined in Section 408.3 of the Revenue and Taxation Code, obtained from a governmental agency or entity or from a multiple listing service, as defined in Section 1087, and not provided directly by the customer to a business in the course of an established business relationship.

(E) Jointly offering a product or service pursuant to a written agreement with the third party that receives the personal information, provided that all of the following requirements are met:

(i) The product or service offered is a product or service of, and is provided by, at least one of the businesses that is a party to the written agreement.



(ii) The product or service is jointly offered, endorsed, or sponsored by, and clearly and conspicuously identifies for the customer, the businesses that disclose and receive the disclosed personal information.

(iii) The written agreement provides that the third party that receives the personal information is required to maintain the confidentiality of the information and is prohibited from disclosing or using the information other than to carry out the joint offering or servicing of a product or service that is the subject of the written agreement.

(2) Disclosures to or from a consumer reporting agency of a customer's payment history or other information pertaining to transactions or experiences between the business and a customer if that information is to be reported in, or used to generate, a consumer report as defined in subdivision (d) of Section 1681a of Title 15 of the United States Code, and use of that information is limited by the federal Fair Credit Reporting Act (15 U.S.C. Sec. 1681 et seq.).

(3) Disclosures of personal information by a business to a third party financial institution solely for the purpose of the business obtaining payment for a transaction in which the customer paid the business for goods or services with a check, credit card, charge card, or debit card, if the customer seeks the information required by subdivision (a) from the business obtaining payment, whether or not the business obtaining payment knows or reasonably should know that the third party financial institution has used the personal information for its direct marketing purposes.

(4) Disclosures of personal information between a licensed agent and its principal, if the personal information disclosed is necessary to complete, effectuate, administer, or enforce transactions between the principal and the agent, whether or not the licensed agent or principal also uses the personal information for direct marketing purposes, if that personal information is used by each of them solely to market products and services directly to customers with whom both have established business relationships as a result of the principal and agent relationship.

(5) Disclosures of personal information between a financial institution and a business that has a private label credit card, affinity card, retail installment contract, or cobranded card program with the financial institution, if the personal information disclosed is necessary for the financial institution to maintain or service accounts on behalf of the business with which it has a private label credit card, affinity card, retail installment contract, or cobranded card program, or to complete, effectuate, administer, or enforce customer transactions or transactions between the institution and the business, whether or not the institution or the business also uses the personal information for direct marketing purposes, if that personal information is used solely to market products and services directly to customers with whom both the business and the financial institution have established business relationships as a result of the private label credit card, affinity card, retail installment contract, or cobranded card program.

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

(1) "Customer" means an individual who is a resident of California who provides personal information to a business during the creation of, or throughout the duration of, an established business relationship if the business relationship is primarily for personal, family, or household purposes.

(2) "Direct marketing purposes" means the use of personal information to solicit or induce a purchase, rental, lease, or exchange of products, goods, property, or services directly to individuals by means of the mail, telephone, or electronic mail for their personal, family, or household purposes. The sale, rental, exchange, or lease of personal information for consideration to businesses is a direct marketing purpose of the business that sells, rents, exchanges, or obtains consideration for the personal information. "Direct marketing purposes" does not include the use of personal information (A) by bona fide tax exempt charitable or religious organizations to solicit charitable contributions, (B) to raise funds from and communicate with individuals regarding politics and government, (C) by a third party when the third party receives personal information solely as a consequence of having obtained for consideration permanent ownership of accounts that might contain personal information, or (D) by a third party when the third party receives personal information solely as a consequence of a single transaction where, as a part of the transaction, personal information had to be disclosed in order to effectuate the transaction.

(3) "Disclose" means to disclose, release, transfer, disseminate, or otherwise communicate orally, in writing, or by electronic or any other means to any third party.

(4) "Employees who regularly have contact with customers" means employees whose contact with customers is not incidental to their primary employment duties, and whose duties do not predominantly involve ensuring the safety or health of the business's customers. It includes, but is not limited to, employees whose primary employment duties are as cashier, clerk, customer service, sales, or promotion. It does not, by way of example, include employees whose primary employment duties consist of food or beverage preparation or service, maintenance and repair of the business's facilities or equipment, direct involvement in the operation of a motor vehicle, aircraft, watercraft, amusement ride, heavy machinery or similar equipment, security, or participation in a theatrical, literary, musical, artistic, or athletic performance or contest.

(5) "Established business relationship" means a relationship formed by a voluntary, two-way communication between a business and a customer, with or without an exchange of consideration, for the purpose of purchasing, renting, or leasing real or personal

property, or any interest therein, or obtaining a product or service from the business, if the relationship is ongoing and has not been expressly terminated by the business or the customer, or if the relationship is not ongoing, but is solely established by the purchase, rental, or lease of real or personal property from a business, or the purchase of a product or service, and no more than 18 months have elapsed from the date of the purchase, rental, or lease.

(6) (A) The categories of personal information required to be disclosed pursuant to paragraph (1) of subdivision (a) are all of the following:

- (i) Name and address.
- (ii) Electronic mail address.
- (iii) Age or date of birth.
- (iv) Names of children.
- (v) Electronic mail or other addresses of children.
- (vi) Number of children.
- (vii) The age or gender of children.
- (viii) Height.
- (ix) Weight.
- (x) Race.
- (xi) Religion.
- (xii) Occupation.
- (xiii) Telephone number.
- (xiv) Education.
- (xv) Political party affiliation.
- (xvi) Medical condition.
- (xvii) Drugs, therapies, or medical products or equipment used.
- (xviii) The kind of product the customer purchased, leased, or rented.
- (xix) Real property purchased, leased, or rented.
- (xx) The kind of service provided.
- (xxi) Social security number.
- (xxii) Bank account number.
- (xxiii) Credit card number.
- (xxiv) Debit card number.
- (xxv) Bank or investment account, debit card, or credit card balance.
- (xxvi) Payment history.
- (xxvii) Information pertaining to the customer's creditworthiness, assets, income, or liabilities.

(B) If a list, description, or grouping of customer names or addresses is derived using any of these categories, and is disclosed to a third party for direct marketing purposes in a manner that permits the third party to identify, determine, or extrapolate any other personal information from which the list was derived, and that personal information when it was disclosed identified, described, or was associated with an individual, the categories set forth in this subdivision that correspond to the personal information used to derive the list, description, or grouping shall be considered personal information for purposes of this section.

(7) "Personal information" as used in this section means any information that when it was disclosed identified, described, or was able to be associated with an individual and includes all of the following:

- (A) An individual's name and address.
- (B) Electronic mail address.
- (C) Age or date of birth.
- (D) Names of children.
- (E) Electronic mail or other addresses of children.
- (F) Number of children.
- (G) The age or gender of children.
- (H) Height.
- (I) Weight.
- (J) Race.
- (K) Religion.
- (L) Occupation.
- (M) Telephone number.
- (N) Education.
- (O) Political party affiliation.
- (P) Medical condition.
- (Q) Drugs, therapies, or medical products or equipment used.
- (R) The kind of product the customer purchased, leased, or rented.
- (S) Real property purchased, leased, or rented.
- (T) The kind of service provided.
- (U) Social security number.
- (V) Bank account number.
- (W) Credit card number.
- (X) Debit card number.
- (Y) Bank or investment account, debit card, or credit card balance.
- (Z) Payment history.

(AA) Information pertaining to creditworthiness, assets, income, or liabilities.

(8) "Third party" or "third parties" means one or more of the following:

- (A) A business that is a separate legal entity from the business that has an established business relationship with a customer.
- (B) A business that has access to a database that is shared among businesses, if the business is authorized to use the database for direct marketing purposes, unless the use of the database is exempt from being considered a disclosure for direct marketing purposes pursuant to subdivision (d).
- (C) A business not affiliated by a common ownership or common corporate control with the business required to comply with subdivision (a).

(f) (1) Disclosures of personal information for direct marketing purposes between affiliated third parties that share the same brand name are exempt from the requirements of paragraph (1) of subdivision (a) unless the personal information disclosed corresponds to

one of the following categories, in which case the customer shall be informed of those categories listed in this subdivision that correspond to the categories of personal information disclosed for direct marketing purposes and the third party recipients of personal information disclosed for direct marketing purposes pursuant to paragraph (2) of subdivision (a):

- (A) Number of children.
- (B) The age or gender of children.
- (C) Electronic mail or other addresses of children.
- (D) Height.
- (E) Weight.
- (F) Race.
- (G) Religion.
- (H) Telephone number.
- (I) Medical condition.
- (J) Drugs, therapies, or medical products or equipment used.
- (K) Social security number.
- (L) Bank account number.
- (M) Credit card number.
- (N) Debit card number.
- (O) Bank or investment account, debit card, or credit card balance.

(2) If a list, description, or grouping of customer names or addresses is derived using any of these categories, and is disclosed to a third party or third parties sharing the same brand name for direct marketing purposes in a manner that permits the third party to identify, determine, or extrapolate the personal information from which the list was derived, and that personal information when it was disclosed identified, described, or was associated with an individual, any other personal information that corresponds to the categories set forth in this subdivision used to derive the list, description, or grouping shall be considered personal information for purposes of this section.

(3) If a business discloses personal information for direct marketing purposes to affiliated third parties that share the same brand name, the business that discloses personal information for direct marketing purposes between affiliated third parties that share the same brand name may comply with the requirements of paragraph (2) of subdivision (a) by providing the overall number of affiliated companies that share the same brand name.

(g) The provisions of this section are severable. If any provision of this section or its application is held invalid, that invalidity shall not affect other provisions or applications that can be given effect without the invalid provision or application.

(h) This section does not apply to a financial institution that is subject to the California Financial Information Privacy Act (Division 1.2 (commencing with Section 4050) of the Financial Code) if the financial institution is in compliance with Sections 4052, 4052.5, 4053, 4053.5, and 4054.6 of the Financial Code, as those sections read when they were chaptered on August 28, 2003, and as subsequently amended by the Legislature or by initiative.

(i) This section shall become operative on January 1, 2005.

*(Amended by Stats. 2005, Ch. 22, Sec. 16. Effective January 1, 2006.)*

**1798.83.5.** (a) The purpose of this section is to ensure that information obtained on an Internet Web site regarding an individual's age will not be used in furtherance of employment or age discrimination.

(b) A commercial online entertainment employment service provider that enters into a contractual agreement to provide employment services to an individual for a subscription payment shall not, upon request by the subscriber, do either of the following:

- (1) Publish or make public the subscriber's date of birth or age information in an online profile of the subscriber.
- (2) Share the subscriber's date of birth or age information with any Internet Web sites for the purpose of publication.

(c) A commercial online entertainment employment service provider subject to subdivision (b) shall, within five days, remove from public view in an online profile of the subscriber the subscriber's date of birth and age information on any companion Internet Web sites under its control upon specific request by the subscriber naming the Internet Web sites. A commercial online entertainment employment service provider that permits members of the public to upload or modify Internet content on its own Internet Web site or any Internet Web site under its control without prior review by that provider shall not be deemed in violation of this section unless first requested by the subscriber to remove age information.

(d) For purposes of this section, the following definitions apply:

(1) "Commercial online entertainment employment service provider" means a person or business that owns, licenses, or otherwise possesses computerized information, including, but not limited to, age and date of birth information, about individuals employed in the entertainment industry, including television, films, and video games, and that makes the information available to the public or potential employers.

(2) "Payment" means a fee in exchange for advertisements, or any other form of compensation or benefit.

(3) "Provide employment services" means post resumes, photographs, or other information about a subscriber when one of the purposes is to provide individually identifiable information about the subscriber to a prospective employer.

(4) "Subscriber" means a natural person who enters into a contractual agreement with a commercial online entertainment employment service provider to receive employment services in return for a subscription payment.

*(Added by Stats. 2016, Ch. 555, Sec. 1. (AB 1687) Effective January 1, 2017.)*

**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) (1) A cause of action shall not lie against a business for disposing of abandoned records containing personal information by shredding, erasing, or otherwise modifying the personal information in the records to make it unreadable or undecipherable through any means.

(2) The Legislature finds and declares that when records containing personal information are abandoned by a business, they often end up in the possession of a storage company or commercial landlord. It is the intent of the Legislature in paragraph (1) to create a safe harbor for such a record custodian who properly disposes of the records in accordance with paragraph (1).

(g) 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.

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

*(Amended by Stats. 2009, Ch. 134, Sec. 3. (AB 1094) Effective January 1, 2010.)*