An act to repeal and add Section 1798.83 to the Civil Code, relating to privacy.

LEGISLATIVE COUNSEL’S DIGEST

AB 1291, as introduced, Lowenthal. Privacy: disclosure of a customer’s personal information.

(1) Existing law requires a business to ensure the privacy of a customer’s personal information, as defined, contained in records by destroying, or arranging for the destruction of, the records, as specified. Any customer injured by a business’ violation of these provisions is entitled to recover damages, obtain injunctive relief, or seek other remedies.

This bill would repeal and reorganize certain provisions of existing law.

(2) Existing law also requires a business that collects customer information for marketing purposes and that discloses a customer’s personal information to a 3rd party for direct marketing purposes, to provide the customer with whom it had a business relationship, as defined, within 30 days after the customer’s request, as specified, in writing or by e-mail, the names and addresses of the recipients of that information and specified details regarding the information disclosed, except as specified. Existing law requires a business subject to these provisions to provide an address, electronic address, or toll-free telephone or facsimile number that a customer may use to deliver requests for copies of his or her personal information.
This bill would instead require any business that has a customer’s personal information, as defined, to provide at no charge, within 30 days of the customer’s specified request, a copy of that information to the customer as well as the names and contact information for all 3rd parties with which the business has shared the information during the previous 12 months, regardless of any business relationship with the customer. This bill would require that a business subject to these provisions choose one of several specified options to provide the customer with a designated address for use in making a request for copies of information under these provisions.

(3) Existing law also requires a business that is required to comply with these provisions to provide information to customers regarding its privacy policy and to provide a designated means of preventing disclosure of personal information.

This bill would require a business that is required to comply with these provisions to provide specified notice to the customer of its privacy policies.

(4) Existing law provides that a customer who sustains injury as a result of a violation of these provisions is entitled to specified remedies, including civil penalties.

This bill would also provide that a violation of these provisions is deemed to constitute an injury to the customer for purposes of seeking remedies available under law.


The people of the State of California do enact as follows:

SECTION 1. Section 1798.83 of the Civil Code is repealed.

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.

(e) (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
does 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.
“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.

SEC. 2. Section 1798.83 is added to the Civil Code, to read:

1798.83. (a) (1) A business that has a customer’s personal information shall make available to the customer free of charge access to, or copies of, all of the customer’s personal information held by the business.

(2) A business that has a customer’s personal information and discloses that personal information to a third party shall make the following information available to the customer free of charge:

(A) All personal information that was disclosed, including the categories set forth in paragraph (1) of subdivision (e).

(B) The names and contact information of all of the third parties that received personal information from the business, including the third party’s designated request address or addresses if available.

(b) A business required to comply with subdivision (a) shall make the required information available by one or more of the following means:
(1) By providing a designated request address and, upon receipt of a request under this section to the designated request address, providing the customer within 30 days the required information for all disclosures occurring in the prior 12 months, provided that:

(A) If the business has an online privacy policy, that policy includes a description of a customer’s rights pursuant to this section accompanied by one or more designated request addresses. A business with multiple online privacy policies must include a description in the policy of each product or service that collects personal information that may be disclosed to a third party.

(B) The business ensures that all persons responsible for handling customer inquiries about the business’ privacy practices or the business’ compliance with this section are informed of all designated request addresses.

(C) The business provides information pertaining to the specific customer if that information is reasonably available to the business, and provides information in standardized format if information pertaining to the specific customer is not reasonably available.

(2) For information required to be provided by paragraph (2) of subdivision (a), by providing the customer with notice including the required information prior to or immediately following a disclosure.

(3) 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.

(c) A business is not obligated to provide more than one notice under paragraph (2) of subdivision (b) to the same customer in a 12-month period about the disclosure of the same personal information to the same third party and is not obligated under paragraph (1) of subdivision (b) to respond to a request by the same customer more than once within a given 12-month period.

(d) A violation of this section by a business subject to these provisions is deemed to constitute an injury to a customer.

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

1. “Categories of personal information” includes, but is not limited to, the following:

   (A) Identity information including, but not limited to, real name, alias, nickname, and user name.
(B) Address information, including, but not limited to, postal address or e-mail.
(C) Telephone number.
(D) Account name.
(E) Social security number or other government-issued identification number, including, but not limited to, social security number, driver’s license number, identification card number, and passport number.
(F) Birthdate or age.
(G) Physical characteristic information, including, but not limited to, height and weight.
(H) Sexual information, including, but not limited to, sexual orientation, sex, gender status, gender identity, and gender expression.
(I) Race or ethnicity.
(J) Religious affiliation or activity.
(K) Political affiliation or activity.
(L) Professional or employment-related information.
(M) Educational information.
(N) Medical information, including, but not limited to, medical conditions or drugs, therapies, mental health, or medical products or equipment used.
(O) Financial information, including, but not limited to, credit, debit, or account numbers, account balances, payment history, or information related to assets, liabilities, or general creditworthiness.
(P) Commercial information, including, but not limited to, records of property, products or services provided, obtained, or considered, or other purchasing or consuming histories or tendencies.
(Q) Location information.
(R) Internet or mobile activity information, including, but not limited to, Internet Protocol addresses or information concerning the access or use of any Internet or mobile-based site or service.
(S) Content, including text, photographs, audio or video recordings, or other material generated by or provided by the customer.
(T) Any of the above categories of information as they pertain to the children of the customer.
(2) (A) “Customer” means an individual who is a resident of California who provides personal information to a business, with
or without an exchange of consideration, in the course of purchasing, viewing, accessing, renting, leasing, or otherwise using real or personal property, or any interest therein, or obtaining a product or service from the business including advertising or any other content.

(B) An individual is also the customer of a business if that business obtained the personal information of that individual from any other business.

(3) “Designated request address” means a mailing address, e-mail address, Web page, toll-free telephone number, or other applicable contact information, whereby customers may request or obtain the information required to be provided under subdivision (a).

(4) (A) “Disclose” means to disclose, release, share, transfer, disseminate, make available, or otherwise communicate orally, in writing, or by electronic or any other means to any third party as defined in this section.

(B) “Disclose” does not include:

(i) Disclosure of personal information by a business to a third party pursuant to a written contract authorizing the third party to utilize the personal information to perform services on behalf of the business, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, or similar services, but only if (I) the contract prohibits the third party from using the personal information for any reason other than performing the specified service(s) on behalf of the business and from disclosing any such personal information to additional third parties and (II) the business effectively enforces these prohibitions.

(ii) Disclosure of personal information by a business to a third party based on a good-faith belief that disclosure is required to comply with applicable law, regulation, legal process, or court order.

(iii) Disclosure of personal information by a business to a third party that is reasonably necessary to address fraud, security, or technical issues; to protect the disclosing business’s rights or property; or to protect customers or the public from illegal activities as required or permitted by law.
(iv) Disclosure of personal information by a business to a third party that is otherwise lawfully available to the general public, provided that the business did not direct the third party to the personal information.

(5) “Personal information” means:
(A) Any information that identifies or references a particular individual or electronic device, including, but not limited to, a real name, alias, postal address, telephone number, electronic mail address, Internet Protocol address, account name, social security number, driver’s license number, passport number, or any other identifier intended or able to be uniquely associated with a particular individual or device.
(B) Any information that relates to or describes an individual, including, but not limited to, any information specifically listed in subdivision (e) of Section 1798.80 of the Civil Code, and including inferences or conclusions drawn from other information, if such information is disclosed in connection with any identifying or referencing information as defined in subparagraph (A) above.

(6) “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 disclosed personal information.
(B) A business that does not share common ownership or common corporate control with the business that has disclosed personal information.
(C) A business that does not share a brand name or common branding with the business that has disclosed personal information such that the affiliate relationship is clear to the customer.

(f) 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.