

AMENDED IN SENATE JULY 1, 2014
AMENDED IN SENATE JUNE 5, 2014
AMENDED IN ASSEMBLY MAY 8, 2014
AMENDED IN ASSEMBLY APRIL 24, 2014
AMENDED IN ASSEMBLY MARCH 28, 2014
CALIFORNIA LEGISLATURE—2013–14 REGULAR SESSION

ASSEMBLY BILL

No. 1710

Introduced by Assembly Members Dickinson and Wieckowski

February 13, 2014

An act to amend Sections 1798.81.5, 1798.82, and 1798.85 of the Civil Code, relating to personal information privacy.

LEGISLATIVE COUNSEL'S DIGEST

AB 1710, as amended, Dickinson. Personal information: privacy.

Existing law requires a person or business conducting business in California that owns or licenses computerized data that includes personal information, as defined, to disclose, as specified, a breach of the security of the system or data following discovery or notification of the security breach to any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. *Existing law also requires a person or business that maintains computerized data that includes personal information that the person or business does not own to notify the owner or licensee of the information of any breach of the security of the data immediately following discovery as specified. Existing law requires a person or business required to issue a security breach notification pursuant to*

these provisions to meet various requirements, including that the security breach notification provide specified information.

~~This bill would instead require a person or business conducting business in California that owns or licenses computerized data that contains personal information to disclose, as specified, a breach of the security of the system or data following discovery or notification of the security breach to any California resident whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person unless the data was encrypted, as specified. If require, if 500 or more persons are affected by the breach, that a person or business that maintains computerized data that includes personal information notify those persons of the breach of the security when a credit or debit card number was, or is reasonably believed to have been, acquired by an unauthorized person at the same time that the notice is given to the owner or licensee, as specified. The bill would authorize the owner or licensee of computerized data that includes personal information and a person or business that maintains computerized data that includes personal information to agree, pursuant to a written contractual agreement, to make the owner or licensee responsible for carrying out the notice requirement described above. With respect to the information required to be included in the notification, the bill would require, if the person or business providing the notification was the source of the breach, the bill would require the that person or business to offer to provide appropriate identity theft prevention and mitigation services, if any, to the affected person at no cost for not less than 24 12 months if the breach exposed or may have exposed specified personal information. The bill would also require a person or business that maintains but does not own the data to notify the persons affected at the same time that notice is given to the owner or licensee, as specified.~~

Existing law requires a business that owns or licenses personal information about a California resident to 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.

This bill would expand these provisions to businesses that own, license, or maintain personal information about a California resident, as specified.

Existing law prohibits a person or entity, with specified exceptions, from publicly posting or displaying an individual's social security number or doing certain other acts that might compromise the security

of an individual’s social security number, unless otherwise required by federal or state law.

This bill would also, except as specified, prohibit the sale, advertisement for sale, or offer to sell of an individual’s social security number.

Vote: majority. Appropriation: no. Fiscal committee: no. State-mandated local program: no.

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

1 SECTION 1. Section 1798.81.5 of the Civil Code is amended
2 to read:

3 1798.81.5. (a) (1) It is the intent of the Legislature to ensure
4 that personal information about California residents is protected.
5 To that end, the purpose of this section is to encourage businesses
6 that own, license, or maintain personal information about
7 Californians to provide reasonable security for that information.

8 (2) For the purpose of this section, the terms “own” and
9 “license” include personal information that a business retains as
10 part of the business’ internal customer account or for the purpose
11 of using that information in transactions with the person to whom
12 the information relates. The term “maintain” includes personal
13 information that a business maintains but does not own or license.

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

20 (c) A business that discloses personal information about a
21 California resident pursuant to a contract with a nonaffiliated third
22 party that is not subject to subdivision (b) shall require by contract
23 that the third party implement and maintain reasonable security
24 procedures and practices appropriate to the nature of the
25 information, to protect the personal information from unauthorized
26 access, destruction, use, modification, or disclosure.

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

29 (1) “Personal information” means an individual’s first name or
30 first initial and his or her last name in combination with any one

1 or more of the following data elements, when either the name or
2 the data elements are not encrypted or redacted:

3 (A) Social security number.

4 (B) Driver's license number or California identification card
5 number.

6 (C) Account number, credit or debit card number, in
7 combination with any required security code, access code, or
8 password that would permit access to an individual's financial
9 account.

10 (D) Medical information.

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

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

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

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

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

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

32 (4) An entity that obtains information under an agreement
33 pursuant to Article 3 (commencing with Section 1800) of Chapter
34 1 of Division 2 of the Vehicle Code and is subject to the
35 confidentiality requirements of the Vehicle Code.

36 (5) A business that is regulated by state or federal law providing
37 greater protection to personal information than that provided by
38 this section in regard to the subjects addressed by this section.
39 Compliance with that state or federal law shall be deemed
40 compliance with this section with regard to those subjects. This

1 paragraph does not relieve a business from a duty to comply with
2 any other requirements of other state and federal law regarding
3 the protection and privacy of personal information.

4 SEC. 2. Section 1798.82 of the Civil Code is amended to read:

5 1798.82. (a) A person or business that conducts business in
6 California, and that owns or licenses computerized data that
7 includes personal information, shall disclose a breach of the
8 security of the system following discovery or notification of the
9 breach in the security of the data to a resident of California whose
10 *unencrypted* personal information was, or is reasonably believed
11 to have been, acquired by an unauthorized person unless the data
12 ~~was encrypted in conformance with the Advanced Encryption~~
13 ~~Standard of the National Institute of Standards and Technology,~~
14 ~~Federal Information Processing Standards Publication 197, as~~
15 ~~amended from time to time.~~ *person*. The disclosure shall be made
16 in the most expedient time possible and without unreasonable
17 delay, consistent with the legitimate needs of law enforcement, as
18 provided in subdivision (c), or any measures necessary to determine
19 the scope of the breach and restore the reasonable integrity of the
20 data system.

21 (b) (1) A person or business that maintains computerized data
22 that includes personal information that the person or business does
23 not own shall notify the owner or licensee of the information of
24 the breach of the security of the data immediately following
25 discovery, if the personal information was, or is reasonably
26 believed to have been, acquired by an unauthorized person.

27 (2) ~~In addition to notifying the owner or licensee of the data,~~
28 ~~the person or business that maintains the data shall notify persons~~
29 ~~affected by the breach~~ *Except as provided in paragraph (3), if 500*
30 *or more subject persons are affected, a person or business that*
31 *maintains computerized data that includes personal information*
32 *shall notify those subject persons of the breach of the security*
33 *when a credit or debit card number was, or is reasonably believed*
34 *to have been, acquired by an unauthorized person* at the same time
35 that *the* notice is given to the owner or licensee by United States
36 mail if the person or business has a mailing address for the subject
37 persons or email notice if the person or business has an email
38 address for the subject persons. If the subject persons cannot be
39 notified by mail or email, the person or business shall provide
40 notice by the following methods:

1 (A) Conspicuous posting of the notice on the Internet Web site
2 page of the person or business, if the person or business maintains
3 an Internet Web site page, for at least 30 days.

4 (B) Notification to major statewide media.

5 (3) *Notwithstanding paragraph (2), the owner or licensee of*
6 *computerized data that includes personal information and a person*
7 *or business that maintains computerized data that includes*
8 *personal information may agree, based on a written contractual*
9 *agreement, to make the owner or licensee responsible for the*
10 *requirement in paragraph (2).*

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

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

19 (1) The security breach notification shall be written in plain
20 language.

21 (2) The security breach notification shall include, at a minimum,
22 the following information:

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

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

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

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

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

38 (F) The toll-free telephone numbers and addresses of the major
39 credit reporting agencies if the breach exposed a social security

1 number or a driver's license or California identification card
2 number.

3 (G) If the person or business providing the notification was the
4 source of the breach, an offer to provide appropriate identity theft
5 prevention and mitigation services, if any, shall be provided at no
6 cost to the affected person for not less than ~~24~~ 12 months, along
7 with all information necessary to take advantage of the offer to
8 any person whose information was or may have been breached if
9 the breach exposed or may have exposed personal information
10 defined in subparagraphs (A) and (B) of paragraph (1) of
11 subdivision (h).

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

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

16 (B) Advice on steps that the person whose information has been
17 breached may take to protect himself or herself.

18 (4) In the case of a breach of the security of the system involving
19 personal information defined in paragraph (2) of subdivision (h)
20 for an online account, and no other personal information defined
21 in paragraph (1) of subdivision (h), the person or business may
22 comply with this section by providing the security breach
23 notification in electronic or other form that directs the person whose
24 personal information has been breached promptly to change his
25 or her password and security question or answer, as applicable, or
26 to take other steps appropriate to protect the online account with
27 the person or business and all other online accounts for which the
28 person whose personal information has been breached uses the
29 same user name or email address and password or security question
30 or answer.

31 (5) In the case of a breach of the security of the system involving
32 personal information defined in paragraph (2) of subdivision (h)
33 for login credentials of an email account furnished by the person
34 or business, the person or business shall not comply with this
35 section by providing the security breach notification to that email
36 address, but may, instead, comply with this section by providing
37 notice by another method described in subdivision (j) or by clear
38 and conspicuous notice delivered to the resident online when the
39 resident is connected to the online account from an Internet

1 Protocol address or online location from which the person or
2 business knows the resident customarily accesses the account.

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

11 (f) A person or business that is required to issue a security breach
12 notification pursuant to this section to more than 500 California
13 residents as a result of a single breach of the security system shall
14 electronically submit a single sample copy of that security breach
15 notification, excluding any personally identifiable information, to
16 the Attorney General. A single sample copy of a security breach
17 notification shall not be deemed to be within subdivision (f) of
18 Section 6254 of the Government Code.

19 (g) For purposes of this section, “breach of the security of the
20 system” means unauthorized acquisition of computerized data that
21 compromises the security, confidentiality, or integrity of personal
22 information maintained by the person or business. Good faith
23 acquisition of personal information by an employee or agent of
24 the person or business for the purposes of the person or business
25 is not a breach of the security of the system, provided that the
26 personal information is not used or subject to further unauthorized
27 disclosure.

28 (h) For purposes of this section, “personal information” means
29 either of the following:

30 (1) An individual’s first name or first initial and last name in
31 combination with any one or more of the following data elements,
32 when either the name or the data elements are not ~~encrypted in~~
33 ~~conformance with the Advanced Encryption Standard of the~~
34 ~~National Institute of Standards and Technology, Federal~~
35 ~~Information Processing Standards Publication 197, as amended~~
36 ~~from time to time:~~ *encrypted:*

- 37 (A) Social security number.
- 38 (B) Driver’s license number or California identification card
- 39 number.

1 (C) Account number, credit or debit card number, in
2 combination with any required security code, access code, or
3 password that would permit access to an individual’s financial
4 account.

5 (D) Medical information.

6 (E) Health insurance information.

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

10 (i) (1) For purposes of this section, “personal information” does
11 not include publicly available information that is lawfully made
12 available to the general public from federal, state, or local
13 government records.

14 (2) For purposes of this section, “medical information” means
15 any information regarding an individual’s medical history, mental
16 or physical condition, or medical treatment or diagnosis by a health
17 care professional.

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

23 (j) For purposes of this section, “notice” may be provided by
24 one of the following methods:

25 (1) Written notice.

26 (2) Electronic notice, if the notice provided is consistent with
27 the provisions regarding electronic records and signatures set forth
28 in Section 7001 of Title 15 of the United States Code.

29 (3) Substitute notice, if the person or business demonstrates that
30 the cost of providing notice would exceed two hundred fifty
31 thousand dollars (\$250,000), or that the affected class of subject
32 persons to be notified exceeds 500,000, or the person or business
33 does not have sufficient contact information. Substitute notice
34 shall consist of all of the following:

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

37 (B) Conspicuous posting of the notice on the Internet Web site
38 page of the person or business, if the person or business maintains
39 one.

40 (C) Notification to major statewide media.

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

9 SEC. 3. Section 1798.85 of the Civil Code is amended to read:

10 1798.85. (a) Except as provided in this section, a person or
11 entity may not do any of the following:

12 (1) Publicly post or publicly display in any manner an
13 individual's social security number. "Publicly post" or "publicly
14 display" means to intentionally communicate or otherwise make
15 available to the general public.

16 (2) Print an individual's social security number on any card
17 required for the individual to access products or services provided
18 by the person or entity.

19 (3) Require an individual to transmit his or her social security
20 number over the Internet, unless the connection is secure or the
21 social security number is encrypted.

22 (4) Require an individual to use his or her social security number
23 to access an Internet Web site, unless a password or unique
24 personal identification number or other authentication device is
25 also required to access the Internet Web site.

26 (5) Print an individual's social security number on any materials
27 that are mailed to the individual, unless state or federal law requires
28 the social security number to be on the document to be mailed.
29 Notwithstanding this paragraph, social security numbers may be
30 included in applications and forms sent by mail, including
31 documents sent as part of an application or enrollment process, or
32 to establish, amend or terminate an account, contract or policy, or
33 to confirm the accuracy of the social security number. A social
34 security number that is permitted to be mailed under this section
35 may not be printed, in whole or in part, on a postcard or other
36 mailer not requiring an envelope, or visible on the envelope or
37 without the envelope having been opened.

38 (6) Sell, advertise for sale, or offer to sell an individual's social
39 security number. For purposes of this paragraph, the following
40 apply:

1 (A) “Sell” shall not include the release of an individual’s social
2 security number if the release of the social security number is
3 incidental to a larger transaction and is necessary to identify the
4 individual in order to accomplish a legitimate business purpose.

5 (B) The release of a social security number for the purpose of
6 marketing is not a legitimate business purpose.

7 (C) “Sell” shall not include the release of an individual’s social
8 security number for a purpose specifically authorized or specifically
9 allowed by federal or state law.

10 (b) This section does not prevent the collection, use, or release
11 of a social security number as required by state or federal law or
12 the use of a social security number for internal verification or
13 administrative purposes.

14 (c) This section does not prevent an adult state correctional
15 facility, an adult city jail, or an adult county jail from releasing an
16 inmate’s social security number, with the inmate’s consent and
17 upon request by the county veterans service officer or the United
18 States Department of Veterans Affairs, for the purposes of
19 determining the inmate’s status as a military veteran and his or her
20 eligibility for federal, state, or local veterans’ benefits or services.

21 (d) This section does not apply to documents that are recorded
22 or required to be open to the public pursuant to Chapter 3.5
23 (commencing with Section 6250), Chapter 14 (commencing with
24 Section 7150) or Chapter 14.5 (commencing with Section 7220)
25 of Division 7 of Title 1 of, Article 9 (commencing with Section
26 11120) of Chapter 1 of Part 1 of Division 3 of Title 2 of, or Chapter
27 9 (commencing with Section 54950) of Part 1 of Division 2 of
28 Title 5 of, the Government Code. This section does not apply to
29 records that are required by statute, case law, or California Rule
30 of Court, to be made available to the public by entities provided
31 for in Article VI of the California Constitution.

32 (e) (1) In the case of a health care service plan, a provider of
33 health care, an insurer or a pharmacy benefits manager, a contractor
34 as defined in Section 56.05, or the provision by any person or
35 entity of administrative or other services relative to health care or
36 insurance products or services, including third-party administration
37 or administrative services only, this section shall become operative
38 in the following manner:

39 (A) On or before January 1, 2003, the entities listed in paragraph
40 (1) shall comply with paragraphs (1), (3), (4), and (5) of subdivision

1 (a) as these requirements pertain to individual policyholders or
2 individual contractholders.

3 (B) On or before January 1, 2004, the entities listed in paragraph
4 (1) shall comply with paragraphs (1) to (5), inclusive, of
5 subdivision (a) as these requirements pertain to new individual
6 policyholders or new individual contractholders and new groups,
7 including new groups administered or issued on or after January
8 1, 2004.

9 (C) On or before July 1, 2004, the entities listed in paragraph
10 (1) shall comply with paragraphs (1) to (5), inclusive, of
11 subdivision (a) for all individual policyholders and individual
12 contractholders, for all groups, and for all enrollees of the Healthy
13 Families and Medi-Cal programs, except that for individual
14 policyholders, individual contractholders and groups in existence
15 prior to January 1, 2004, the entities listed in paragraph (1) shall
16 comply upon the renewal date of the policy, contract, or group on
17 or after July 1, 2004, but no later than July 1, 2005.

18 (2) A health care service plan, a provider of health care, an
19 insurer or a pharmacy benefits manager, a contractor, or another
20 person or entity as described in paragraph (1) shall make reasonable
21 efforts to cooperate, through systems testing and other means, to
22 ensure that the requirements of this article are implemented on or
23 before the dates specified in this section.

24 (3) Notwithstanding paragraph (2), the Director of the
25 Department of Managed Health Care, pursuant to the authority
26 granted under Section 1346 of the Health and Safety Code, or the
27 Insurance Commissioner, pursuant to the authority granted under
28 Section 12921 of the Insurance Code, and upon a determination
29 of good cause, may grant extensions not to exceed six months for
30 compliance by health care service plans and insurers with the
31 requirements of this section when requested by the health care
32 service plan or insurer. Any extension granted shall apply to the
33 health care service plan or insurer's affected providers, pharmacy
34 benefits manager, and contractors.

35 (f) If a federal law takes effect requiring the United States
36 Department of Health and Human Services to establish a national
37 unique patient health identifier program, a provider of health care,
38 a health care service plan, a licensed health care professional, or
39 a contractor, as those terms are defined in Section 56.05, that

1 complies with the federal law shall be deemed in compliance with
2 this section.

3 (g) A person or entity may not encode or embed a social security
4 number in or on a card or document, including, but not limited to,
5 using a barcode, chip, magnetic strip, or other technology, in place
6 of removing the social security number, as required by this section.

7 (h) This section shall become operative, with respect to the
8 University of California, in the following manner:

9 (1) On or before January 1, 2004, the University of California
10 shall comply with paragraphs (1), (2), and (3) of subdivision (a).

11 (2) On or before January 1, 2005, the University of California
12 shall comply with paragraphs (4) and (5) of subdivision (a).

13 (i) This section shall become operative with respect to the
14 Franchise Tax Board on January 1, 2007.

15 (j) This section shall become operative with respect to the
16 California community college districts on January 1, 2007.

17 (k) This section shall become operative with respect to the
18 California State University system on July 1, 2005.

19 (l) This section shall become operative, with respect to the
20 California Student Aid Commission and its auxiliary organization,
21 in the following manner:

22 (1) On or before January 1, 2004, the commission and its
23 auxiliary organization shall comply with paragraphs (1), (2), and
24 (3) of subdivision (a).

25 (2) On or before January 1, 2005, the commission and its
26 auxiliary organization shall comply with paragraphs (4) and (5)
27 of subdivision (a).

O