

ASSEMBLY BILL

No. 1710

Introduced by Assembly Members Dickinson and Wieckowski

February 13, 2014

An act to amend Section 1798.82 of the Civil Code, relating to personal information privacy.

LEGISLATIVE COUNSEL'S DIGEST

AB 1710, as introduced, 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.

This bill would make nonsubstantive, technical changes to these provisions.

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 1798.82 of the Civil Code is amended
2 to read:
3 1798.82. (a) ~~Any~~A person or business that conducts business
4 in California, and that owns or licenses computerized data that
5 includes personal information, shall disclose ~~any~~ a breach of the
6 security of the system following discovery or notification of the

1 breach in the security of the data to ~~any~~ a resident of California
2 whose unencrypted personal information was, or is reasonably
3 believed to have been, acquired by an unauthorized person. The
4 disclosure shall be made in the most expedient time possible and
5 without unreasonable delay, consistent with the legitimate needs
6 of law enforcement, as provided in subdivision (c), or any measures
7 necessary to determine the scope of the breach and restore the
8 reasonable integrity of the data system.

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

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

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

23 (1) The security breach notification shall be written in plain
24 language.

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

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

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

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

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

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

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

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

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

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

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

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

38 (e) A covered entity under the federal Health Insurance
39 Portability and Accountability Act of 1996 (42 U.S.C. Sec. 1320d
40 et seq.) will be deemed to have complied with the notice

1 requirements in subdivision (d) if it has complied completely with
2 Section 13402(f) of the federal Health Information Technology
3 for Economic and Clinical Health Act (Public Law 111-5).
4 However, nothing in this subdivision shall be construed to exempt
5 a covered entity from any other provision of this section.

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

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

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

25 (1) An individual’s first name or first initial and last name in
26 combination with any one or more of the following data elements,
27 when either the name or the data elements are not encrypted:

28 (A) Social security number.

29 (B) Driver’s license number or California identification card
30 number.

31 (C) Account number, credit or debit card number, in
32 combination with any required security code, access code, or
33 password that would permit access to an individual’s financial
34 account.

35 (D) Medical information.

36 (E) Health insurance information.

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

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

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

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

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

16 (1) Written notice.

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

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

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

28 (B) Conspicuous posting of the notice on the Internet Web site
29 page of the person or business, if the person or business maintains
30 one.

31 (C) Notification to major statewide media.

32 (k) Notwithstanding subdivision (j), a person or business that
33 maintains its own notification procedures as part of an information
34 security policy for the treatment of personal information and is
35 otherwise consistent with the timing requirements of this part, shall
36 be deemed to be in compliance with the notification requirements
37 of this section if the person or business notifies subject persons in

- 1 accordance with its policies in the event of a breach of security of
- 2 the system.

O