

AMENDED IN ASSEMBLY JUNE 20, 2011

AMENDED IN SENATE MARCH 29, 2011

SENATE BILL

No. 24

Introduced by Senator Simitian
(Coauthor: Senator Fuller)
(Coauthor: Assembly Member Wieckowski)

December 6, 2010

An act to amend Sections 1798.29 and 1798.82 of the Civil Code, relating to personal information.

LEGISLATIVE COUNSEL'S DIGEST

SB 24, as amended, Simitian. Personal information: privacy.

Existing law requires any agency, and any person or business conducting business in California, that owns or licenses computerized data that includes personal information, as defined, to disclose in specified ways, any breach of the security of the system or data, as defined, 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 require any agency, person, or business that is required to issue a security breach notification pursuant to existing law to fulfill certain additional requirements pertaining to the security breach notification, as specified.

The bill would also require any agency, person, or business that is required to issue a security breach notification to more than 500 California residents pursuant to existing law to electronically submit a single sample copy of that security breach notification to the Attorney General, as specified.

This bill would provide that a covered entity under the federal Health Insurance Portability and Accountability Act of 1996 is deemed to have complied with these provisions, if it has complied with existing federal law, as specified.

The bill would also incorporate additional changes made by the Governor’s Reorganization Plan No. 1 of 2009.

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

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

1 SECTION 1. Section 1798.29 of the Civil Code is amended
2 to read:

3 1798.29. (a) Any agency that owns or licenses computerized
4 data that includes personal information shall disclose any breach
5 of the security of the system following discovery or notification
6 of the breach in the security of the data to any resident of California
7 whose unencrypted personal information was, or is reasonably
8 believed to have been, acquired by an unauthorized person. The
9 disclosure shall be made in the most expedient time possible and
10 without unreasonable delay, consistent with the legitimate needs
11 of law enforcement, as provided in subdivision (c), or any measures
12 necessary to determine the scope of the breach and restore the
13 reasonable integrity of the data system.

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

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

25 (d) Any agency that is required to issue a security breach
26 notification pursuant to this section shall meet all of the following
27 requirements:

28 (1) The security breach notification shall be written in plain
29 language.

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

3 (A) The name and contact information of the reporting agency
4 subject to this section.

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

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

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

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

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

22 (3) At the discretion of the agency, the security breach
23 notification may also include any of the following:

24 (A) Information about what the agency has done to protect
25 individuals whose information has been breached.

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

28 (e) Any agency that is required to issue a security breach
29 notification pursuant to this section to more than 500 California
30 residents as a result of a single breach of the security system shall
31 electronically submit a single sample copy of that security breach
32 notification, excluding any personally identifiable information, to
33 the Attorney General. A single sample copy of a security breach
34 notification shall not be deemed to be within subdivision (f) of
35 Section 6254 of the Government Code.

36 (f) For purposes of this section, "breach of the security of the
37 system" means unauthorized acquisition of computerized data that
38 compromises the security, confidentiality, or integrity of personal
39 information maintained by the agency. Good faith acquisition of
40 personal information by an employee or agent of the agency for

1 the purposes of the agency is not a breach of the security of the
2 system, provided that the personal information is not used or
3 subject to further unauthorized disclosure.

4 (g) For purposes of this section, “personal information” means
5 an individual’s first name or first initial and last name in
6 combination with any one or more of the following data elements,
7 when either the name or the data elements are not encrypted:

8 (1) Social security number.

9 (2) Driver’s license number or California Identification Card
10 number.

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

14 (4) Medical information.

15 (5) Health insurance information.

16 (h) (1) For purposes of this section, “personal information”
17 does not include publicly available information that is lawfully
18 made available to the general public from federal, state, or local
19 government records.

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

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

29 (i) For purposes of this section, “notice” may be provided by
30 one of the following methods:

31 (1) Written notice.

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

35 (3) Substitute notice, if the agency demonstrates that the cost
36 of providing notice would exceed two hundred fifty thousand
37 dollars (\$250,000), or that the affected class of subject persons to
38 be notified exceeds 500,000, or the agency does not have sufficient
39 contact information. Substitute notice shall consist of all of the
40 following:

1 (A) E-mail notice when the agency has an e-mail address for
2 the subject persons.

3 (B) Conspicuous posting of the notice on the agency’s Internet
4 Web site page, if the agency maintains one.

5 (C) Notification to major statewide media and the Office of
6 Information Security within the ~~office of the State Chief~~
7 ~~Information Officer~~ *California Technology Agency*.

8 (j) Notwithstanding subdivision (i), an agency that maintains
9 its own notification procedures as part of an information security
10 policy for the treatment of personal information and is otherwise
11 consistent with the timing requirements of this part shall be deemed
12 to be in compliance with the notification requirements of this
13 section if it notifies subject persons in accordance with its policies
14 in the event of a breach of security of the system.

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

16 1798.82. (a) Any person or business that conducts business
17 in California, and that owns or licenses computerized data that
18 includes personal information, shall disclose any breach of the
19 security of the system following discovery or notification of the
20 breach in the security of the data to any resident of California
21 whose unencrypted personal information was, or is reasonably
22 believed to have been, acquired by an unauthorized person. The
23 disclosure shall be made in the most expedient time possible and
24 without unreasonable delay, consistent with the legitimate needs
25 of law enforcement, as provided in subdivision (c), or any measures
26 necessary to determine the scope of the breach and restore the
27 reasonable integrity of the data system.

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

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

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

4 (1) The security breach notification shall be written in plain
5 language.

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

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

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

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

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

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

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

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

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

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

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

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

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

18 (h) For purposes of this section, “personal information” means
19 an individual’s first name or first initial and last name in
20 combination with any one or more of the following data elements,
21 when either the name or the data elements are not encrypted:

22 (1) Social security number.

23 (2) Driver’s license number or California Identification Card
24 number.

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

28 (4) Medical information.

29 (5) Health insurance information.

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

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

38 (3) For purposes of this section, “health insurance information”
39 means an individual’s health insurance policy number or subscriber
40 identification number, any unique identifier used by a health insurer

1 to identify the individual, or any information in an individual’s
2 application and claims history, including any appeals records.

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

5 (1) Written notice.

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

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

15 (A) E-mail notice when the person or business has an e-mail
16 address for the subject persons.

17 (B) Conspicuous posting of the notice on the Internet Web site
18 page of the person or business, if the person or business maintains
19 one.

20 (C) Notification to major statewide media and the Office of
21 Privacy Protection within the State and Consumer Services Agency.

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