

AMENDED IN ASSEMBLY JULY 23, 2009

AMENDED IN ASSEMBLY JULY 7, 2009

AMENDED IN ASSEMBLY JUNE 16, 2009

AMENDED IN SENATE MARCH 4, 2009

SENATE BILL

No. 20

Introduced by Senator Simitian

December 1, 2008

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

LEGISLATIVE COUNSEL'S DIGEST

SB 20, 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.

The bill would also incorporate additional changes made by the Governor's Reorganization Plan.

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.

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

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

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

5 ~~(C) The date, estimated date, or date range within which the~~
6 ~~breach occurred, if that information is possible to determine at the~~
7 ~~time the notice is provided, and the date of the notice.~~

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

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

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

19 (F) The estimated number of persons affected by the breach, if
20 that information is possible to determine at the time the notice is
21 provided.

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

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

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

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

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

(f) 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 agency. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(g) For purposes of this section, “personal information” means 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:

(1) Social security number.

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

(3) Account number, 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.

(4) Medical information.

(5) Health insurance information.

(h) (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.

(i) 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.

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

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

9 (B) Conspicuous posting of the notice on the agency's Web site
10 page, if the agency maintains one.

11 (C) Notification to major statewide media and the Office of
12 Information Security within the office of the State Chief
13 Information Officer.

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

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

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

34 (b) Any person or business that maintains computerized data
35 that includes personal information that the person or business does
36 not own shall notify the owner or licensee of the information of
37 any breach of the security of the data immediately following
38 discovery, if the personal information was, or is reasonably
39 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 after the law enforcement agency determines that it will not compromise the investigation.

(d) Any 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.

(2) The security breach notification 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) The date, or estimated date, or date range within which the breach occurred, if that information is possible to determine at the time the notice is provided, and the date of the notice.~~

(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 estimated number of persons affected by the breach, if that information is possible to determine at the time the notice is provided.

(G) 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.

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

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

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

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

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

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

26 (1) Social security number.

27 (2) Driver’s license number or California Identification Card
28 number.

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

32 (4) Medical information.

33 (5) Health insurance information.

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

38 (2) For purposes of this section, “medical information” means
39 any information regarding an individual’s medical history, mental

1 or physical condition, or medical treatment or diagnosis by a health
2 care professional.

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

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

10 (1) Written notice.

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

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

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

22 (B) Conspicuous posting of the notice on the Web site page of
23 the person or business, if the person or business maintains one.

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

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