

Introduced by Senator Simitian

February 18, 2010

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

LEGISLATIVE COUNSEL'S DIGEST

SB 1166, as introduced, 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:

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

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

(b) Any agency that maintains computerized data that includes personal information that the agency does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably 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 agency 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 agency 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) 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

1 within which the breach occurred. The notification shall also
2 include the date of the notice.

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

6 (E) A general description of the breach incident, if that
7 information is possible to determine at the time the notice is
8 provided.

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

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

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

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

19 (e) Any agency that is required to issue a security breach
20 notification pursuant to this section to more than 500 California
21 residents as a result of a single breach of the security system shall
22 electronically submit a single sample copy of that security breach
23 notification, excluding any personally identifiable information, to
24 the Attorney General. A single sample copy of a security breach
25 notification shall not be deemed to be within subdivision (f) of
26 Section 6254 of the Government Code.

27 ~~(d)~~

28 (f) For purposes of this section, "breach of the security of the
29 system" means unauthorized acquisition of computerized data that
30 compromises the security, confidentiality, or integrity of personal
31 information maintained by the agency. Good faith acquisition of
32 personal information by an employee or agent of the agency for
33 the purposes of the agency is not a breach of the security of the
34 system, provided that the personal information is not used or
35 subject to further unauthorized disclosure.

36 ~~(e)~~

37 (g) For purposes of this section, "personal information" means
38 an individual's first name or first initial and last name in
39 combination with any one or more of the following data elements,
40 when either the name or the data elements are not encrypted:

1 (1) Social security number.

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

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

7 (4) Medical information.

8 (5) Health insurance information.

9 ~~(f)~~

10 (h) (1) For purposes of this section, "personal information"
11 does not include publicly available information that is lawfully
12 made 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 ~~(g)~~

24 (i) For purposes of this section, "notice" may be provided by
25 one of the following methods:

26 (1) Written notice.

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

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

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

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

1 (C) Notification to major statewide media *and the Office of*
2 *Information Security within the office of the State Chief Information*
3 *Officer.*

4 (~~h~~)

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

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

13 1798.82. (a) Any person or business that conducts business
14 in California, and that owns or licenses computerized data that
15 includes personal information, shall disclose any breach of the
16 security of the system following discovery or notification of the
17 breach in the security of the data to any resident of California
18 whose unencrypted personal information was, or is reasonably
19 believed to have been, acquired by an unauthorized person. The
20 disclosure shall be made in the most expedient time possible and
21 without unreasonable delay, consistent with the legitimate needs
22 of law enforcement, as provided in subdivision (c), or any measures
23 necessary to determine the scope of the breach and restore the
24 reasonable integrity of the data system.

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

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

36 (d) *Any person or business that is required to issue a security*
37 *breach notification pursuant to this section shall meet all of the*
38 *following requirements:*

39 (1) *The security breach notification shall be written in plain*
40 *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 person*
4 *or business 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 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 person or business, the security*
23 *breach notification may also include any of the following:*

24 (A) *Information about what the person or business has done to*
25 *protect 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 person or business that is required to issue a security*
29 *breach notification pursuant to this section to more than 500*
30 *California residents as a result of a single breach of the security*
31 *system shall electronically submit a single sample copy of that*
32 *security breach notification, excluding any personally identifiable*
33 *information, to the Attorney General. A single sample copy of a*
34 *security breach notification shall not be deemed to be within*
35 *subdivision (f) of Section 6254 of the Government Code.*

36 ~~(d)~~

37 (f) *For purposes of this section, "breach of the security of the*
38 *system" means unauthorized acquisition of computerized data that*
39 *compromises the security, confidentiality, or integrity of personal*
40 *information maintained by the person or business. Good faith*

1 acquisition of personal information by an employee or agent of
2 the person or business for the purposes of the person or business
3 is not a breach of the security of the system, provided that the
4 personal information is not used or subject to further unauthorized
5 disclosure.

6 ~~(e)~~

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

11 (1) Social security number.

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

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

17 (4) Medical information.

18 (5) Health insurance information.

19 ~~(f)~~

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

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

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

33 ~~(g)~~

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

36 (1) Written notice.

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

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

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

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

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

~~(H)~~

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