

AMENDED IN SENATE JANUARY 7, 2008

SENATE BILL

No. 364

Introduced by Senator Simitian

February 20, 2007

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

LEGISLATIVE COUNSEL'S DIGEST

SB 364, 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. ~~Existing law allows an agency to provide that disclosure by substitute notice, as specified, if the agency demonstrates that the cost of disclosure would exceed \$250,000, or that the affected class exceeds 500,000 persons, or that the agency does not have sufficient contact information.~~

~~In addition to the other substitute notice provisions, this bill would instead allow for substitute notice if the agency demonstrates that the cost of disclosure would exceed \$100,000. The bill would also repeal a duplicative provision of law.~~

This bill would require the agency, person, or business, in addition to the duties specified above, to electronically report the breach to the Office of Information Security and Privacy Protection, as specified. The bill would require the office to establish a Web site where an

agency, person, or business shall submit electronically to the office security breach notifications meeting specified requirements and sent to California residents; the bill would require the office to make those notifications publicly available. The bill would require the office to annually report a summary of the information collected and made available via the Web site to the Legislature.

Vote: majority. Appropriation: no. Fiscal committee: ~~no~~-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 to
2 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, and
9 shall submit electronically any security breach notification sent
10 to California residents pursuant to this section to the Office of
11 Information Security and Privacy Protection in accordance with
12 this section. The disclosure shall be made in the most expedient
13 time possible and without unreasonable delay, consistent with the
14 legitimate needs of law enforcement, as provided in subdivision
15 (c), or any measures necessary to determine the scope of the breach
16 and restore the reasonable integrity of the data system.

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

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

28 (d) The Office of Information Security and Privacy Protection
29 shall establish a Web site where agencies subject to this section

1 shall submit electronically security breach notifications sent to
2 California residents, and shall make these notifications publicly
3 available online.

4 (e) A security breach notification shall meet all of the following
5 requirements:

6 (1) The security breach notification shall be provided by the
7 one of following means:

8 (A) Written notice.

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

12 (C) Substitute notice, if the agency demonstrates that the cost
13 of providing notice would exceed one hundred thousand dollars
14 (\$100,000), or that the affected class of subject persons to be
15 notified exceeds 500,000, or the agency does not have sufficient
16 contact information. Substitute notice shall consist of any of the
17 following:

18 (i) E-mail notice when the agency has an e-mail address for the
19 subject persons.

20 (ii) Conspicuous posting of the notice on the agency's Web site,
21 if the agency maintains one.

22 (iii) Notification to major statewide media and electronic
23 submission of a copy of the security breach notification form or
24 forms to the Office of Information Security and Privacy Protection
25 in accordance with subdivision (d).

26 (2) The security breach notification shall be written in plain
27 English.

28 (3) The security breach notification shall include, at a minimum,
29 the following information:

30 (A) The toll-free telephone numbers and addresses of the major
31 credit reporting agencies.

32 (B) The name and contact information of the reporting agency.

33 (C) A list of the types of information, such as name or social
34 security number, that may have been the subject of a breach.

35 (D) The date of a breach, if known, and the date of discovery
36 of a breach, if known.

37 (E) The date of the notification, and whether the notification
38 was delayed pursuant to subdivision (c).

39 (F) A general description of the breach incident.

40 (G) The estimated number of persons affected by the breach.

1 (H) Whether substitute notice was used.
 2 (4) The Office of Information Security and Privacy Protection
 3 shall annually report a summary of the information collected and
 4 made available via the Web site to the Legislature.

5 ~~(d)~~
 6 (f) For purposes of this section, ~~“breach~~ the following terms
 7 have the following meanings:

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

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

21 ~~(1)~~
 22 (i) Social security number.

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

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

31 ~~(4)~~
 32 (iv) Medical information.

33 ~~(5)~~
 34 (v) Health insurance information.

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

39 ~~(2) For purposes of this section, “medical~~

1 (3) “*Medical* information” means any information regarding
2 an individual’s medical history, mental or physical condition, or
3 medical treatment or diagnosis by a health care professional.
4 ~~(3) For purposes of this section, “health~~
5 (4) “*Health* insurance information” means an individual’s health
6 insurance policy number or subscriber identification number, any
7 unique identifier used by a health insurer to identify the individual,
8 or any information in an individual’s application and claims history,
9 including any appeals records.
10 ~~(g) For purposes of this section, “notice” may be~~
11 ~~provided by one of the following methods:~~
12 ~~(1)~~
13 ~~–Written notice.~~
14 ~~(2)~~
15 ~~–Electronic notice, if the notice provided is consistent with the~~
16 ~~provisions regarding electronic records and signatures set forth in~~
17 ~~Section 7001 of Title 15 of the United States Code.~~
18 ~~(3)~~
19 ~~–Substitute notice, if the agency demonstrates that the cost of~~
20 ~~providing notice would exceed two hundred fifty thousand dollars~~
21 ~~(\$250,000), or that the affected class of subject persons to be~~
22 ~~notified exceeds 500,000, or the agency does not have sufficient~~
23 ~~contact information. Substitute notice shall consist of all of the~~
24 ~~following:~~
25 ~~(A)~~
26 ~~–E-mail notice when the agency has an e-mail address for the~~
27 ~~subject persons.~~
28 ~~(B)~~
29 ~~–Conspicuous posting of the notice on the agency’s Web site~~
30 ~~page, if the agency maintains one.~~
31 ~~(C)~~
32 ~~–Notification to major statewide media.~~
33 ~~(h)~~
34 (g) Notwithstanding subdivision ~~(g)~~ (e), an agency that maintains
35 its own notification procedures as part of an information security
36 policy for the treatment of personal information and is otherwise
37 consistent with the timing requirements of this part shall be deemed
38 to be in compliance with the notification requirements of this
39 section if it notifies subject persons in accordance with its policies
40 in the event of a breach of security of the system.

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

2 1798.82. (a) Any person or business that conducts business
3 in California, and that owns or licenses computerized data that
4 includes personal information, shall disclose any breach of the
5 security of the system following discovery or notification of the
6 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, *and*
9 *shall submit electronically any security breach notification sent*
10 *to California residents pursuant to this section to the Office of*
11 *Information Security and Privacy Protection in accordance with*
12 *this section.* The disclosure shall be made in the most expedient
13 time possible and without unreasonable delay, consistent with the
14 legitimate needs of law enforcement, as provided in subdivision
15 (c), or any measures necessary to determine the scope of the breach
16 and restore the reasonable integrity of the data system.

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

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

28 (d) *The Office of Information Security and Privacy Protection*
29 *shall establish a Web site where any person or business subject*
30 *to this section shall submit electronically security breach*
31 *notifications sent to California residents, and shall make those*
32 *notifications publicly available online.*

33 (e) *A security breach notification shall meet all of the following*
34 *requirements:*

35 (1) *The security breach notification shall be provided by the*
36 *one of following means:*

37 (A) *Written notice.*

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

1 (C) Substitute notice, if the person or business subject to this
2 section demonstrates that the cost of providing notice would exceed
3 one hundred thousand dollars (\$100,000), or that the affected
4 class of subject persons to be notified exceeds 500,000, or that the
5 person or business subject to this section does not have sufficient
6 contact information. Substitute notice shall consist of any of the
7 following:

8 (i) E-mail notice when the person or business subject to this
9 section has an e-mail address for the subject persons.

10 (ii) Conspicuous posting of the notice on the person's or
11 business' Web site, if the person or business subject to this section
12 maintains one.

13 (iii) Notification to major statewide media and electronic
14 submission of a copy of the security breach notification to the
15 Office of Information Security and Privacy Protection in
16 accordance with subdivision (d).

17 (2) The security breach notification shall be written in plain
18 English.

19 (3) The security breach notification shall include, at a minimum,
20 the following information:

21 (A) The toll-free telephone numbers and addresses of the major
22 credit reporting agencies.

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

25 (C) A list of the types of information, such as name or social
26 security number, that may have been the subject of a breach.

27 (D) The date of a breach, if known, and the date of discovery
28 of a breach, if known.

29 (E) The date of the notification, and whether the notification
30 was delayed pursuant to subdivision (c).

31 (F) A general description of the breach incident.

32 (G) The estimated number of persons affected by the breach.

33 (H) Whether substitute notice was used.

34 (4) The Office of Information Security and Privacy Protection
35 shall annually report a summary of the information collected and
36 made available via the Web site to the Legislature.

37 ~~(d)~~

38 (f) For purposes of this section, "breach" of the following terms
39 have the following meanings:

1 (1) “*Breach of the security of the system*” means unauthorized
2 acquisition of computerized data that compromises the security,
3 confidentiality, or integrity of personal information maintained by
4 the person or business. Good faith acquisition of personal
5 information by an employee or agent of the person or business for
6 the purposes of the person or business is not a breach of the security
7 of the system, provided that the personal information is not used
8 or subject to further unauthorized disclosure.

9 ~~(e) For purposes of this section, “personal~~

10 (2) (A) “*Personal information*” means an individual’s first
11 name or first initial and last name in combination with any one or
12 more of the following data elements, when either the name or the
13 data elements are not encrypted:

14 ~~(1)~~

15 (i) Social security number.

16 ~~(2)~~

17 (ii) Driver’s license number or California Identification Card
18 number.

19 ~~(3)~~

20 (iii) Account number, credit or debit card number, in
21 combination with any required security code, access code, or
22 password that would permit access to an individual’s financial
23 account.

24 ~~(4)~~

25 (iv) Medical information.

26 ~~(5)~~

27 (v) Health insurance information.

28 ~~(f) (1) For purposes of this section, “personal~~

29 (B) “*Personal information*” does not include publicly available
30 information that is lawfully made available to the general public
31 from federal, state, or local government records.

32 ~~(2) For purposes of this section, “medical~~

33 (3) “*Medical information*” means any information regarding
34 an individual’s medical history, mental or physical condition, or
35 medical treatment or diagnosis by a health care professional.

36 ~~(3) For purposes of this section, “health~~

37 (4) “*Health insurance information*” means an individual’s health
38 insurance policy number or subscriber identification number, any
39 unique identifier used by a health insurer to identify the individual,

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

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

5 ~~(1)~~

6 ~~–Written notice.~~

7 ~~(2)~~

8 ~~–Electronic notice, if the notice provided is consistent with the~~
9 ~~provisions regarding electronic records and signatures set forth in~~
10 ~~Section 7001 of Title 15 of the United States Code.~~

11 ~~(3)~~

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

18 ~~(A)~~

19 ~~–E-mail notice when the person or business has an e-mail address~~
20 ~~for the subject persons.~~

21 ~~(B)~~

22 ~~–Conspicuous posting of the notice on the Web site page of the~~
23 ~~person or business, if the person or business maintains one.~~

24 ~~(C)~~

25 ~~–Notification to major statewide media.~~

26 ~~(h)~~

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

1
2
3
4
5

**All matter omitted in this version of the bill
appears in the bill as introduced in Senate,
February 20, 2007 (JR11)**

O