

Introduced by Senator SimitianDecember 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 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 must 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 must issue a security breach notification to more than 500 California residents pursuant to existing law to electronically submit that security breach notification to the Attorney General.

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 must issue a security breach notification*
26 *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:*

32 (A) *The name and contact information of the reporting agency*
33 *subject to this section.*

34 (B) *A list of the types of personal information, as defined in*
35 *subdivision (g), that were or are reasonably believed to have been*
36 *the subject of a breach.*

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

4 (D) *Whether the notification was delayed as a result of a law*
5 *enforcement investigation.*

6 (E) *A general description of the breach incident.*

7 (F) *The estimated number of persons affected by the breach.*

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

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

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

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

18 (e) *Any agency that must issue a security breach notification*
19 *pursuant to this section to more than 500 California residents as*
20 *a result of a single breach of the security system shall electronically*
21 *submit that security breach notification to the Attorney General.*

22 ~~(d)~~

23 (f) For purposes of this section, “breach of the security of the
24 system” means unauthorized acquisition of computerized data that
25 compromises the security, confidentiality, or integrity of personal
26 information maintained by the agency. Good faith acquisition of
27 personal information by an employee or agent of the agency for
28 the purposes of the agency is not a breach of the security of the
29 system, provided that the personal information is not used or
30 subject to further unauthorized disclosure.

31 ~~(e)~~

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

36 (1) Social security number.

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

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

4 (4) Medical information.

5 (5) Health insurance information.

6 ~~(f)~~

7 (h) (1) For purposes of this section, "personal information"
8 does not include publicly available information that is lawfully
9 made available to the general public from federal, state, or local
10 government records.

11 (2) For purposes of this section, "medical information" means
12 any information regarding an individual's medical history, mental
13 or physical condition, or medical treatment or diagnosis by a health
14 care professional.

15 (3) For purposes of this section, "health insurance information"
16 means an individual's health insurance policy number or subscriber
17 identification number, any unique identifier used by a health insurer
18 to identify the individual, or any information in an individual's
19 application and claims history, including any appeals records.

20 ~~(g)~~

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

23 (1) Written notice.

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

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

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

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

37 (C) Notification to major statewide media *and the Office of*
38 *Information Security and Privacy Protection.*

39 ~~(h)~~

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

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

9 1798.82. (a) Any person or business that conducts business
10 in California, and that owns or licenses computerized data that
11 includes personal information, shall disclose any breach of the
12 security of the system following discovery or notification of the
13 breach in the security of the data to any resident of California
14 whose unencrypted personal information was, or is reasonably
15 believed to have been, acquired by an unauthorized person. The
16 disclosure shall be made in the most expedient time possible and
17 without unreasonable delay, consistent with the legitimate needs
18 of law enforcement, as provided in subdivision (c), or any measures
19 necessary to determine the scope of the breach and restore the
20 reasonable integrity of the data system.

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

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

32 (d) *Any person or business that must issue a security breach*
33 *notification pursuant to this section shall meet all of the following*
34 *requirements:*

35 (1) *The security breach notification shall be written in plain*
36 *language.*

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

39 (A) *The name and contact information of the reporting person*
40 *or business subject to this section.*

1 (B) A list of the types of personal information, as defined in
2 subdivision (g), that were or are reasonably believed to have been
3 the subject of a breach.

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

7 (D) Whether notification was delayed as a result of a law
8 enforcement investigation.

9 (E) A general description of the breach incident.

10 (F) The estimated number of persons affected by the breach.

11 (G) The toll-free telephone numbers and addresses of the major
12 credit reporting agencies if the breach exposed a bank account or
13 credit card number, a social security number, or a driver's license
14 or California identification card number.

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

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

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

21 (e) Any person or business that must issue a security breach
22 notification pursuant to this section to more than 500 California
23 residents as a result of a single breach of the security system shall
24 electronically submit that security breach notification to the
25 Attorney General.

26 ~~(d)~~

27 (f) For purposes of this section, "breach of the security of the
28 system" means unauthorized acquisition of computerized data that
29 compromises the security, confidentiality, or integrity of personal
30 information maintained by the person or business. Good faith
31 acquisition of personal information by an employee or agent of
32 the person or business for the purposes of the person or business
33 is not a breach of the security of the system, provided that the
34 personal information is not used or subject to further unauthorized
35 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 person or business demonstrates that
31 the cost of providing notice would exceed two hundred fifty
32 thousand dollars (\$250,000), or that the affected class of subject
33 persons to be notified exceeds 500,000, or the person or business
34 does not have sufficient contact information. Substitute notice
35 shall consist of all of the following:

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

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

1 (C) Notification to major statewide media *and the Office of*
2 *Information Security and Privacy Protection.*
3 ~~(h)~~
4 (j) Notwithstanding subdivision ~~(g)~~(i), a person or business that
5 maintains its own notification procedures as part of an information
6 security policy for the treatment of personal information and is
7 otherwise consistent with the timing requirements of this part, shall
8 be deemed to be in compliance with the notification requirements
9 of this section if the person or business notifies subject persons in
10 accordance with its policies in the event of a breach of security of
11 the system.