

Introduced by Senator Corbett

December 14, 2012

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

LEGISLATIVE COUNSEL'S DIGEST

SB 46, as introduced, Corbett. 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 defines "personal information" for these purposes, to include an individual's first name and last name, or first initial and last name, in combination with one or more designated data elements relating to, among other things, social security numbers, driver's license numbers, financial accounts, and medical information.

This bill would revise certain data elements included within the definition of personal information, by adding certain information relating to an account other than a financial account.

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:

1 1798.29. (a) Any agency that owns or licenses computerized
2 data that includes personal information shall disclose any breach
3 of the security of the system following discovery or notification
4 of the breach in the security of the data to any resident of California
5 whose unencrypted personal information was, or is reasonably
6 believed to have been, acquired by an unauthorized person. The
7 disclosure shall be made in the most expedient time possible and
8 without unreasonable delay, consistent with the legitimate needs
9 of law enforcement, as provided in subdivision (c), or any measures
10 necessary to determine the scope of the breach and restore the
11 reasonable integrity of the data system.

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

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

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

26 (1) The security breach notification shall be written in plain
27 language.

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

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

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

34 (C) If the information is possible to determine at the time the
35 notice is provided, then any of the following: (i) the date of the
36 breach, (ii) the estimated date of the breach, or (iii) the date range
37 within which the breach occurred. The notification shall also
38 include the date of the notice.

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

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

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

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

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

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

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

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

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

37 (1) Social security number.

38 (2) Driver’s license number or California Identification Card
39 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 (6) *Password, user name, or security question and answer for*
7 *an account other than a financial account.*

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

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

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

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 Internet
36 Web site page, if the agency maintains one.

37 (C) Notification to major statewide media and the Office of
38 Information Security within the California Technology Agency.

39 (j) Notwithstanding subdivision (i), an agency that maintains
40 its own notification procedures as part of an information security

1 policy for the treatment of personal information and is otherwise
2 consistent with the timing requirements of this part shall be deemed
3 to be in compliance with the notification requirements of this
4 section if it notifies subject persons in accordance with its policies
5 in the event of a breach of security of the system.

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

7 1798.82. (a) Any person or business that conducts business
8 in California, and that owns or licenses computerized data that
9 includes personal information, shall disclose any breach of the
10 security of the system following discovery or notification of the
11 breach in the security of the data to any resident of California
12 whose unencrypted personal information was, or is reasonably
13 believed to have been, acquired by an unauthorized person. The
14 disclosure shall be made in the most expedient time possible and
15 without unreasonable delay, consistent with the legitimate needs
16 of law enforcement, as provided in subdivision (c), or any measures
17 necessary to determine the scope of the breach and restore the
18 reasonable integrity of the data system.

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

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

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

33 (1) The security breach notification shall be written in plain
34 language.

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

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

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

1 (C) If the information is possible to determine at the time the
2 notice is provided, then any of the following: (i) the date of the
3 breach, (ii) the estimated date of the breach, or (iii) the date range
4 within which the breach occurred. The notification shall also
5 include the date of the notice.

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

9 (E) A general description of the breach incident, if that
10 information is possible to determine at the time the notice is
11 provided.

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

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

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

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

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

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

38 (g) For purposes of this section, "breach of the security of the
39 system" means unauthorized acquisition of computerized data that
40 compromises the security, confidentiality, or integrity of personal

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

7 (h) 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 (6) *Password, user name or security question and answer for*
20 *an account other than a financial account.*

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

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

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

34 (j) 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.

1 (3) Substitute notice, if the person or business demonstrates that
2 the cost of providing notice would exceed two hundred fifty
3 thousand dollars (\$250,000), or that the affected class of subject
4 persons to be notified exceeds 500,000, or the person or business
5 does not have sufficient contact information. Substitute notice
6 shall consist of all of the following:
7 (A) E-mail notice when the person or business has an e-mail
8 address for the subject persons.
9 (B) Conspicuous posting of the notice on the Internet Web site
10 page of the person or business, if the person or business maintains
11 one.
12 (C) Notification to major statewide media and the Office of
13 Privacy Protection within the State and Consumer Services Agency.
14 (k) Notwithstanding subdivision (j), a person or business that
15 maintains its own notification procedures as part of an information
16 security policy for the treatment of personal information and is
17 otherwise consistent with the timing requirements of this part, shall
18 be deemed to be in compliance with the notification requirements
19 of this section if the person or business notifies subject persons in
20 accordance with its policies in the event of a breach of security of
21 the system.