

AMENDED IN SENATE APRIL 6, 2015

SENATE BILL

No. 570

Introduced by Senator Jackson

February 26, 2015

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

LEGISLATIVE COUNSEL'S DIGEST

SB 570, as amended, Jackson. Personal information: privacy: breach.

Existing law requires a person or business conducting business in California *and any agency, as defined*, that owns or licenses computerized data that includes personal information, as defined, to disclose a breach of the security of the system in the most expedient time possible and without unreasonable delay, as specified. *Existing law requires a person, business, or agency that is required to issue a security breach notification to meet specific requirements.*

~~This bill would make a nonsubstantive change to this provision.~~

This bill would additionally require that the security breach notification include a one-page notice containing specified information.

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

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

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

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

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

23 (1) The security breach notification shall be written in plain
24 ~~language.~~ *language and shall include a one page notice titled*
25 *“Notice of Data Breach,” in which the content is presented under*
26 *the following headings: “What Happened,” “What Information*
27 *Was Involved,” “What We Are Doing,” “What You Can Do,” and*
28 *“For More Information.” Additional information may be provided*
29 *as a supplement to the one page notice.*

30 (A) *The format of the one page notice shall be designed to call*
31 *attention to the nature and significance of the information it*
32 *contains.*

33 (B) *The title and headings in the one page notice shall be clearly*
34 *and conspicuously displayed.*

35 (C) *The text of the one page notice and any other notice provided*
36 *pursuant to this section shall be no smaller than 10-point type.*

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 agency
40 subject to this section.

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

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

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

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

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

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

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

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

24 (4) In the case of a breach of the security of the system involving
25 personal information defined in paragraph (2) of subdivision (g)
26 for an online account, and no other personal information defined
27 in paragraph (1) of subdivision (g), the agency may comply with
28 this section by providing the security breach notification in
29 electronic or other form that directs the person whose personal
30 information has been breached to promptly change his or her
31 password and security question or answer, as applicable, or to take
32 other steps appropriate to protect the online account with the
33 agency and all other online accounts for which the person uses the
34 same user name or email address and password or security question
35 or answer.

36 (5) In the case of a breach of the security of the system involving
37 personal information defined in paragraph (2) of subdivision (g)
38 for login credentials of an email account furnished by the agency,
39 the agency shall not comply with this section by providing the
40 security breach notification to that email address, but may, instead,

1 comply with this section by providing notice by another method
2 described in subdivision (i) or by clear and conspicuous notice
3 delivered to the resident online when the resident is connected to
4 the online account from an Internet Protocol address or online
5 location from which the agency knows the resident customarily
6 accesses the account.

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

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

23 (g) For purposes of this section, “personal information” means
24 either of the following:

25 (1) An individual’s first name or first initial and last name in
26 combination with any one or more of the following data elements,
27 when either the name or the data elements are not encrypted:

28 (A) Social security number.

29 (B) Driver’s license number or California identification card
30 number.

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

35 (D) Medical information.

36 (E) Health insurance information.

37 (2) A user name or email address, in combination with a
38 password or security question and answer that would permit access
39 to an online account.

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

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

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

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

16 (1) Written notice.

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

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

26 (A) Email notice when the agency has an email address for the
27 subject persons.

28 (B) ~~Conspicuous-posting~~ *posting, for a minimum of 30 days, of*
29 *the notice on the agency’s Internet Web site page, if the agency*
30 *maintains one. For purposes of this subparagraph, conspicuous*
31 *posting on the agency’s Internet Web site means providing a link*
32 *to the notice on the home page that is in larger type than the*
33 *surrounding text, or in contrasting type, font, or color to the*
34 *surrounding text of the same size, or set off from the surrounding*
35 *text of the same size by symbols or other marks that call attention*
36 *to the link.*

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

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 (k) Notwithstanding the exception specified in paragraph (4) of
7 subdivision (b) of Section 1798.3, for purposes of this section,
8 “agency” includes a local agency, as defined in subdivision (a) of
9 Section 6252 of the Government Code.

10 **SECTION 1.**

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

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

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

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

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

38 (1) The security breach notification shall be written in plain
39 ~~language.~~ *language and shall include a one page notice titled*
40 *“Notice of Data Breach,” in which the content is presented under*

1 the following headings: “What Happened,” “What Information
2 Was Involved,” “What We Are Doing,” “What You Can Do,” and
3 “For More Information.” Additional information may be provided
4 as a supplement to the one page notice.

5 (A) The format of the one page notice shall be designed to call
6 attention to the nature and significance of the information it
7 contains.

8 (B) The title and headings in the one page notice shall be clearly
9 and conspicuously displayed.

10 (C) The text of the one page notice and any other notice provided
11 pursuant to this section shall be no smaller than 10-point type.

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

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

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

18 (C) If the information is possible to determine at the time the
19 notice is provided, then any of the following: (i) the date of the
20 breach, (ii) the estimated date of the breach, or (iii) the date range
21 within which the breach occurred. The notification shall also
22 include the date of the notice.

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

26 (E) A general description of the breach incident, if that
27 information is possible to determine at the time the notice is
28 provided.

29 (F) The toll-free telephone numbers and addresses of the major
30 credit reporting agencies if the breach exposed a social security
31 number or a driver’s license or California identification card
32 number.

33 (G) If the person or business providing the notification was the
34 source of the breach, an offer to provide appropriate identity theft
35 prevention and mitigation ~~services, if any, services~~ shall be
36 provided at no cost to the affected person for not less than ~~one~~
37 ~~year, 12 months~~ along with all information necessary to take
38 advantage of the offer to any person whose information was or
39 may have been breached if the breach exposed or may have

1 exposed personal information defined in subparagraphs (A) and
2 (B) of paragraph (1) of subdivision (h).

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

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

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

9 (4) In the case of a breach of the security of the system involving
10 personal information defined in paragraph (2) of subdivision (h)
11 for an online account, and no other personal information defined
12 in paragraph (1) of subdivision (h), the person or business may
13 comply with this section by providing the security breach
14 notification in electronic or other form that directs the person whose
15 personal information has been breached promptly to change his
16 or her password and security question or answer, as applicable, or
17 to take other steps appropriate to protect the online account with
18 the person or business and all other online accounts for which the
19 person whose personal information has been breached uses the
20 same user name or email address and password or security question
21 or answer.

22 (5) In the case of a breach of the security of the system involving
23 personal information defined in paragraph (2) of subdivision (h)
24 for login credentials of an email account furnished by the person
25 or business, the person or business shall not comply with this
26 section by providing the security breach notification to that email
27 address, but may, instead, comply with this section by providing
28 notice by another method described in subdivision (j) or by clear
29 and conspicuous notice delivered to the resident online when the
30 resident is connected to the online account from an Internet
31 Protocol address or online location from which the person or
32 business knows the resident customarily accesses the account.

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

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

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

(h) For purposes of this section, “personal information” means either of the following:

(1) 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:

(A) Social security number.

(B) Driver’s license number or California identification card number.

(C) 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.

(D) Medical information.

(E) Health insurance information.

(2) A user name or email address, in combination with a password or security question and answer that would permit access to an online account.

(i) (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

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 (j) 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) Email notice when the person or business has an email
21 address for the subject persons.

22 (B) ~~Conspicuous posting~~ *posting, for a minimum of 30 days, of*
23 *the notice on the Internet Web site page of the person or business,*
24 *if the person or business maintains one. For purposes of this*
25 *subparagraph, conspicuous posting on the agency’s Internet Web*
26 *site means providing a link to the notice on the home page that is*
27 *in larger type than the surrounding text, or in contrasting type,*
28 *font, or color to the surrounding text of the same size, or set off*
29 *from the surrounding text of the same size by symbols or other*
30 *marks that call attention to the link.*

31 (C) Notification to major statewide media.

32 (k) Notwithstanding subdivision (j), a person or business that
33 maintains its own notification procedures as part of an information
34 security policy for the treatment of personal information and is
35 otherwise consistent with the timing requirements of this part, shall
36 be deemed to be in compliance with the notification requirements
37 of this section if the person or business notifies subject persons in

- 1 accordance with its policies in the event of a breach of security of
- 2 the system.

O