

AMENDED IN ASSEMBLY JULY 2, 2015

AMENDED IN SENATE MAY 21, 2015

AMENDED IN SENATE APRIL 6, 2015

**SENATE BILL**

**No. 570**

---

---

**Introduced by Senator Jackson**

February 26, 2015

---

---

An act to amend 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, including that the notification be written in plain language.

This bill would additionally require the security breach notification to be titled "Notice of Data ~~Breach,~~<sup>2</sup> *Breach*" and to present the ~~content information~~ under prescribed ~~headings, and, in the case of written notices, to present the information on one page.~~ *headings*. The bill would prescribe a model security breach notification ~~form~~ *form, as specified*.

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 is required to issue a security breach  
26 notification 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, shall be titled "Notice of Data Breach," and shall present  
30 ~~the content~~ *information described in paragraph (2)* under the  
31 following headings: "What Happened," "What Information Was  
32 Involved," "What We Are Doing," "What You Can Do," and "For  
33 More Information." ~~In the case of written notices, as specified in~~  
34 ~~paragraph (1) of subdivision (i), the information shall be presented~~  
35 ~~on one page.~~ Additional information may be provided as a  
36 supplement to the ~~one page~~ notice.

1 (A) The format of the ~~one-page~~ notice shall be designed to call  
2 attention to the nature and significance of the information it  
3 contains.

4 (B) The title and headings in the ~~one-page~~ notice shall be clearly  
5 and conspicuously displayed.

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

8 (D) ~~Use~~ *For a written notice described in paragraph (1) of*  
9 *subdivision (i), use of the model security breach notification form*  
10 *prescribed below shall constitute compliance with this paragraph,*  
11 *although use of the model security breach notification form is not*  
12 *required. or use of the headings described in this paragraph with*  
13 *the information described in paragraph (2), written in plain*  
14 *language, shall be deemed to be in compliance with this*  
15 *subdivision.*

[NAME OF INSTITUTION / LOGO]		Date: [insert date]
NOTICE OF DATA BREACH		
What Happened?		
What Information Was Involved?		
What We Are Doing.		

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39

What You Can Do.	
Other Important Information. [insert other important information]	
For More Information.	Call [telephone number] or go to <del>Web</del> [Internet Web site]

(E) For an electronic notice described in paragraph (2) of subdivision (i), use of the headings described in this paragraph with the information described in paragraph (2), written in plain language, shall be deemed to be in compliance with this subdivision.

(2) The security breach notification described in paragraph (1) 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 within which the breach occurred. The notification shall also 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 either of the following:

35 (1) An individual's first name or first initial and last name in  
36 combination with any one or more of the following data elements,  
37 when either the name or the data elements are not encrypted:

38 (A) Social security number.

39 (B) Driver's license number or California identification card  
40 number.

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

5 (D) Medical information.

6 (E) Health insurance information.

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

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

25 (1) Written notice.

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

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

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

37 (B) Conspicuous posting, for a minimum of 30 days, of the  
38 notice on the agency's Internet Web site page, if the agency  
39 maintains one. For purposes of this subparagraph, conspicuous  
40 posting on the agency's Internet Web site means providing a link

1 to the notice on the home page *or first significant page after*  
2 *entering the Internet Web site* that is in larger type than the  
3 surrounding text, or in contrasting type, font, or color to the  
4 surrounding text of the same size, or set off from the surrounding  
5 text of the same size by symbols or other marks that call attention  
6 to the link.

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

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

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

32 (j) Notwithstanding subdivision (i), an agency that maintains  
33 its own notification procedures as part of an information security  
34 policy for the treatment of personal information and is otherwise  
35 consistent with the timing requirements of this part shall be deemed  
36 to be in compliance with the notification requirements of this  
37 section if it notifies subject persons in accordance with its policies  
38 in the event of a breach of security of the system.

39 (k) Notwithstanding the exception specified in paragraph (4) of  
40 subdivision (b) of Section 1798.3, for purposes of this section,

1 “agency” includes a local agency, as defined in subdivision (a) of  
2 Section 6252 of the Government Code.

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

4 1798.82. (a) A person or business that conducts business in  
5 California, and that owns or licenses computerized data that  
6 includes personal information, shall disclose a breach of the  
7 security of the system following discovery or notification of the  
8 breach in the security of the data to a resident of California whose  
9 unencrypted personal information was, or is reasonably believed  
10 to have been, acquired by an unauthorized person. The disclosure  
11 shall be made in the most expedient time possible and without  
12 unreasonable delay, consistent with the legitimate needs of law  
13 enforcement, as provided in subdivision (c), or any measures  
14 necessary to determine the scope of the breach and restore the  
15 reasonable integrity of the data system.

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

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

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

30 (1) The security breach notification shall be written in plain  
31 language, shall be titled “Notice of Data Breach,” and shall present  
32 the ~~content~~ *information described in paragraph (2)* under the  
33 following headings: “What Happened,” “What Information Was  
34 Involved,” “What We Are Doing,” “What You Can Do,” and “For  
35 More Information.” ~~In the case of written notices, as specified in~~  
36 ~~paragraph (1) of subdivision (j), the information shall be presented~~  
37 ~~on one page.~~ Additional information may be provided as a  
38 supplement to the ~~one page~~ notice.

1 (A) The format of the ~~one-page~~ notice shall be designed to call  
2 attention to the nature and significance of the information it  
3 contains.

4 (B) The title and headings in the ~~one-page~~ notice shall be clearly  
5 and conspicuously displayed.

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

8 ~~Use~~ *For a written notice described in paragraph (1) of*  
9 *subdivision (j), use of the model security breach notification form*  
10 *prescribed below shall constitute compliance with this paragraph,*  
11 *although use of the model security breach notification form is not*  
12 *required. or use of the headings described in this paragraph with*  
13 *the information described in paragraph (2), written in plain*  
14 *language, shall be deemed to be in compliance with this*  
15 *subdivision.*

[NAME OF INSTITUTION / LOGO]		Date: [insert date]
NOTICE OF DATA BREACH		
What Happened?		
What Information Was Involved?		
What We Are Doing.		

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39

What You Can Do.	
Other Important Information. [insert other important information]	
For More Information.	Call [telephone number] or go to <del>Web</del> [Internet Web site]

(E) For an electronic notice described in paragraph (2) of subdivision (j), use of the headings described in this paragraph with the information described in paragraph (2), written in plain language, shall be deemed to be in compliance with this subdivision.

(2) The security breach notification described in paragraph (1) shall include, at a minimum, the following information:

(A) The name and contact information of the reporting person or business 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 within which the breach occurred. The notification shall also include the date of the notice.

1 (D) Whether 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 (G) If the person or business providing the notification was the  
12 source of the breach, an offer to provide appropriate identity theft  
13 prevention and mitigation ~~services~~ *services, if any*, shall be  
14 provided at no cost to the affected person for not less than 12  
15 months along with all information necessary to take advantage of  
16 the offer to any person whose information was or may have been  
17 breached if the breach exposed or may have exposed personal  
18 information defined in subparagraphs (A) and (B) of paragraph  
19 (1) of subdivision (h).

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

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

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

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

34 (f) A person or business that is required to issue a security breach  
35 notification pursuant to this section to more than 500 California  
36 residents as a result of a single breach of the security system shall  
37 electronically submit a single sample copy of that security breach  
38 notification, excluding any personally identifiable information, to  
39 the Attorney General. A single sample copy of a security breach

1 notification shall not be deemed to be within subdivision (f) of  
2 Section 6254 of the Government Code.

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

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

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

17 (A) Social security number.

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

20 (C) 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 (D) Medical information.

25 (E) Health insurance information.

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

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

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

37 (3) For purposes of this section, “health insurance information”  
38 means an individual’s health insurance policy number or subscriber  
39 identification number, any unique identifier used by a health insurer

1 to identify the individual, or any information in an individual's  
2 application and claims history, including any appeals records.

3 (j) For purposes of this section, "notice" may be provided by  
4 one of the following methods:

5 (1) Written notice.

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

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

15 (A) Email notice when the person or business has an email  
16 address for the subject persons.

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

27 (C) Notification to major statewide media.

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

1 (5) In the case of a breach of the security of the system involving  
2 personal information defined in paragraph (2) of subdivision (h)  
3 for login credentials of an email account furnished by the person  
4 or business, the person or business shall not comply with this  
5 section by providing the security breach notification to that email  
6 address, but may, instead, comply with this section by providing  
7 notice by another method described in this subdivision or by clear  
8 and conspicuous notice delivered to the resident online when the  
9 resident is connected to the online account from an Internet  
10 Protocol address or online location from which the person or  
11 business knows the resident customarily accesses the account.

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