

AMENDED IN ASSEMBLY MAY 28, 2015  
AMENDED IN ASSEMBLY MAY 13, 2015  
AMENDED IN ASSEMBLY MAY 5, 2015  
AMENDED IN ASSEMBLY APRIL 23, 2015  
AMENDED IN ASSEMBLY MARCH 26, 2015  
CALIFORNIA LEGISLATURE—2015–16 REGULAR SESSION

## **ASSEMBLY BILL**

**No. 964**

---

**Introduced by Assembly Member Chau**

February 26, 2015

---

An act to amend Sections 1798.29 and 1798.82 of the Civil Code, relating to civil law.

### LEGISLATIVE COUNSEL'S DIGEST

AB 964, as amended, Chau. Civil law: privacy.

Existing law requires a person or business conducting business in California, or any state or local agency, that owns or licenses computerized data that includes personal information, as defined, to disclose in specified ways, a 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 requires the disclosure to be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

This bill would define “encrypted” for purpose of these provisions to mean rendered unusable, unreadable, or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information technology.

~~Existing law requires a person, business, or a state or local agency, that is required to issue a security breach notification to more than 500 California residents as a result of a single breach of the security system to electronically submit a single sample copy of that security breach notification to the Attorney General.~~

~~This bill would also require a person or business, or state or local agency that is required to issue a security breach notification under these circumstances to inform the Attorney General of the date of the discovery of the breach.~~

Vote: majority. Appropriation: no. Fiscal committee: ~~yes~~-no. 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

1 section shall be made after the law enforcement agency determines  
2 that it will not compromise the investigation.

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

6 (1) The security breach notification shall be written in plain  
7 language.

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

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

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

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

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

22 (E) A general description of the breach incident, if that  
23 information is possible to determine at the time the notice is  
24 provided.

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

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

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

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

35 (4) In the case of a breach of the security of the system involving  
36 personal information defined in paragraph (2) of subdivision (g)  
37 for an online account, and no other personal information defined  
38 in paragraph (1) of subdivision (g), the agency may comply with  
39 this section by providing the security breach notification in  
40 electronic or other form that directs the person whose personal

1 information has been breached to promptly change his or her  
2 password and security question or answer, as applicable, or to take  
3 other steps appropriate to protect the online account with the  
4 agency and all other online accounts for which the person uses the  
5 same user name or email address and password or security question  
6 or answer.

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

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

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 agency. Good faith acquisition of  
31 personal information by an employee or agent of the agency for  
32 the purposes of the agency is not a breach of the security of the  
33 system, provided that the personal information is not used or  
34 subject to further unauthorized disclosure.

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

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

40 (A) Social security number.

1 (B) Driver's license number or California identification card  
2 number.

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

7 (D) Medical information.

8 (E) Health insurance information.

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

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

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

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

25 (4) For purposes of this section, "encrypted" means rendered  
26 unusable, unreadable, or indecipherable to an unauthorized person  
27 through a security technology or methodology generally accepted  
28 in the field of information security.

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

31 (1) Written notice.

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

35 (3) Substitute notice, if the agency demonstrates that the cost  
36 of providing notice would exceed two hundred fifty thousand  
37 dollars (\$250,000), or that the affected class of subject persons to  
38 be notified exceeds 500,000, or the agency does not have sufficient  
39 contact information. Substitute notice shall consist of all of the  
40 following:

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

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

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

7 (j) Notwithstanding subdivision (i), an agency that maintains  
8 its own notification procedures as part of an information security  
9 policy for the treatment of personal information and is otherwise  
10 consistent with the timing requirements of this part shall be deemed  
11 to be in compliance with the notification requirements of this  
12 section if it notifies subject persons in accordance with its policies  
13 in the event of a breach of security of the system.

14 (k) Notwithstanding the exception specified in paragraph (4) of  
15 subdivision (b) of Section 1798.3, for purposes of this section,  
16 "agency" includes a local agency, as defined in subdivision (a) of  
17 Section 6252 of the Government Code.

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

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

32 (b) A person or business that maintains computerized data that  
33 includes personal information that the person or business does not  
34 own shall notify the owner or licensee of the information of the  
35 breach of the security of the data immediately following discovery,  
36 if the personal information was, or is reasonably believed to have  
37 been, acquired by an unauthorized person.

38 (c) The notification required by this section may be delayed if  
39 a law enforcement agency determines that the notification will  
40 impede a criminal investigation. The notification required by this

1 section shall be made promptly after the law enforcement agency  
2 determines that it will not compromise the investigation.

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

6 (1) The security breach notification shall be written in plain  
7 language.

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

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

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

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

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

22 (E) A general description of the breach incident, if that  
23 information is possible to determine at the time the notice is  
24 provided.

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

29 (G) If the person or business providing the notification was the  
30 source of the breach, an offer to provide appropriate identity theft  
31 prevention and mitigation services, if any, shall be provided at no  
32 cost to the affected person for not less than 12 months, along with  
33 all information necessary to take advantage of the offer to any  
34 person whose information was or may have been breached if the  
35 breach exposed or may have exposed personal information defined  
36 in subparagraphs (A) and (B) of paragraph (1) of subdivision (h).

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

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

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

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

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

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

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



1 information, to the Attorney General. A single sample copy of a  
2 security breach notification shall not be deemed to be within  
3 subdivision (f) of Section 6254 of the Government Code.

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

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

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

18 (A) Social security number.

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

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

25 (D) Medical information.

26 (E) Health insurance information.

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

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

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

38 (3) For purposes of this section, “health insurance information”  
39 means an individual’s health insurance policy number or subscriber  
40 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 (4) For purposes of this section, "encrypted" means rendered  
4 unusable, unreadable, or indecipherable to an unauthorized person  
5 through a security technology or methodology generally accepted  
6 in the field of information security.

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

9 (1) Written notice.

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

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

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

21 (B) Conspicuous posting of the notice on the Internet Web site  
22 page of the person or business, if the person or business maintains  
23 one.

24 (C) Notification to major statewide media.

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