

**ASSEMBLY BILL**

**No. 259**

---

---

**Introduced by Assembly Member Dababneh**

February 9, 2015

---

---

An act to amend Section 1798.29 of the Civil Code, relating to personal information privacy.

LEGISLATIVE COUNSEL'S DIGEST

AB 259, as introduced, Dababneh. Personal information: privacy.

Existing law requires an agency that owns or licenses computerized data that includes personal information, as defined, to provide notification of any breach in the security of that data to any California resident whose personal information may have been compromised by the breach, as specified. Existing law requires the notification to be written in plain language and contain specified information, including, but not limited to, the agency's contact information and a list of the types of personal information that were or are reasonably believed to have been the subject of the breach.

This bill would additionally require an agency, if the agency was the source of the breach and the breach compromised a person's social security number, driver's license number, or California identification card number, to offer to provide the person with identity theft prevention and mitigation services at no cost for not less than 12 months, 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~~*An* agency that owns or licenses  
4 computerized data that includes personal information shall disclose  
5 ~~any~~ a breach of the security of the system following discovery or  
6 notification of the breach in the security of the data to ~~any~~ a  
7 resident of California whose unencrypted personal information  
8 was, or is reasonably believed to have been, acquired by an  
9 unauthorized person. The disclosure shall be made in the most  
10 expedient time possible and without unreasonable delay, consistent  
11 with the legitimate needs of law enforcement, as provided in  
12 subdivision (c), or any measures necessary to determine the scope  
13 of the breach and restore the reasonable integrity of the data system.

14 (b) ~~Any~~*An* agency that maintains computerized data that  
15 includes personal information that the agency does not own shall  
16 notify the owner or licensee of the information of ~~any~~ the breach  
17 of the security of the data immediately following discovery, if the  
18 personal information was, or is reasonably believed to have been,  
19 acquired 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 *promptly* after the law enforcement agency  
24 determines that it will not compromise the investigation.

25 (d) ~~Any~~*An* 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.

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 that were or are  
35 reasonably believed to have been the subject of a breach.

36 (C) If the information is possible to determine at the time the  
37 notice is provided, then any of the following: (i) the date of the  
38 breach, (ii) the estimated date of the breach, or (iii) the date range

1 within which the breach occurred. The notification shall also  
2 include the date of the notice.

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

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

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

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

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

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

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

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

39 (5) In the case of a breach of the security of the system involving  
40 personal information defined in paragraph (2) of subdivision (g)

1 for login credentials of an email account furnished by the agency,  
2 the agency shall not comply with this section by providing the  
3 security breach notification to that email address, but may, instead,  
4 comply with this section by providing notice by another method  
5 described in subdivision (i) or by clear and conspicuous notice  
6 delivered to the resident online when the resident is connected to  
7 the online account from an Internet Protocol address or online  
8 location from which the agency knows the resident customarily  
9 accesses the account.

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

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

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

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

31 (A) Social security number.

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

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

38 (D) Medical information.

39 (E) Health insurance information.

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

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

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

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

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

19 (1) Written notice.

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

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

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

31 (B) Conspicuous posting of the notice on the agency’s Internet  
32 Web site page, if the agency maintains one.

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

35 (j) Notwithstanding subdivision (i), an agency that maintains  
36 its own notification procedures as part of an information security  
37 policy for the treatment of personal information and is otherwise  
38 consistent with the timing requirements of this part shall be deemed  
39 to be in compliance with the notification requirements of this

1 section if it notifies subject persons in accordance with its policies  
2 in the event of a breach of security of the system.  
3 (k) Notwithstanding the exception specified in paragraph (4) of  
4 subdivision (b) of Section 1798.3, for purposes of this section,  
5 “agency” includes a local agency, as defined in subdivision (a) of  
6 Section 6252 of the Government Code.

O