

AMENDED IN ASSEMBLY MAY 14, 2007

AMENDED IN ASSEMBLY MAY 1, 2007

AMENDED IN ASSEMBLY APRIL 10, 2007

CALIFORNIA LEGISLATURE—2007—08 REGULAR SESSION

**ASSEMBLY BILL**

**No. 779**

---

---

**Introduced by Assembly Member Jones**  
**(Coauthors: Assembly Members DeSaulnier and Huffman)**  
*(Coauthor: Senator Migden)*

February 22, 2007

---

---

An act to add Section 1724 to, and to repeal and amend Sections 1798.29 and 1798.82 of, the Civil Code, relating to personal information.

LEGISLATIVE COUNSEL'S DIGEST

AB 779, as amended, Jones. Personal information: state agencies and businesses.

(1) Existing law imposes specified duties upon certain persons or businesses that conduct business in California to, among other things, take reasonable steps to destroy customer records, implement and maintain reasonable security measures, disclose a breach of computerized data, and, upon request, provide specified information to a customer in relation to the disclosure of personal information to 3rd parties. For a violation of any of the above-described provisions, existing law allows an injured customer to institute a civil action to recover damages or for injunctive relief.

~~This bill would subject a retail seller to the above-described provisions. The bill would also prohibit a retail seller from retaining personal information for longer than 90 days after the date of an original transaction or as specified.~~

*This bill would prohibit a person, business, or public agency that sells goods or services to any resident of California and accepts as payment a credit card, debit card, or other payment device, from storing, retaining, sending, or failing to limit access to payment related data, as defined, retaining a primary account number, or storing sensitive authentication data subsequent to the authorization, as specified and unless a specified exception applies.*

(2) Existing law requires any state agency, or a person or business that conducts business in California, that owns or licenses computerized data that includes personal information, as defined, to disclose any breach of the security of that data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

This bill would require that notification to include, among other things, a description of the categories of personal information that was, or may have been, acquired, a toll-free telephone number or electronic mail address an individual may use to contact the agency or person or business, and the telephone numbers and addresses of the major credit reporting agencies, and would require a copy of the notice to be provided to the Office of Privacy Protection. The bill would also allow a person or business subject to the above-described provisions to, if applicable, be reimbursed by whomever maintains the personal information for all reasonable costs of providing notice regarding a breach. The bill would also repeal duplicative provisions of law.

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 1724 is added to the Civil Code, to read:~~  
 2     ~~1724. (a) For purposes of this section, “personal information”~~  
 3     ~~has the same meaning as in subdivision (e) of Section 1798.80.~~  
 4     ~~(b) Any retail seller that sells goods or services to any resident~~  
 5     ~~of California that collects or maintains personal information for~~  
 6     ~~any purpose shall be subject to the provisions of Title 1.81~~  
 7     ~~(commencing with Section 1798.80) of Part 4.~~  
 8     ~~(c) A retail seller that sells goods or services to any resident of~~  
 9     ~~California shall not retain personal information for longer than 90~~  
 10    ~~days after the date of the original transaction, or the period of time~~

1 ~~during which goods may be returned for a refund or exchange,~~  
2 ~~whichever is shorter.~~

3 *SECTION 1. Section 1724 is added to the Civil Code, to read:*

4 *1724. (a) For purposes of this section, “payment related data”*  
5 *means any information described in paragraph (3) of subdivision*  
6 *(e) of Section 1798.82, whether individually or in combination*  
7 *with any other information described in paragraph (3) of*  
8 *subdivision (e) of Section 1798.82.*

9 *(b) In addition to being subject to the provisions of Title 1.81*  
10 *(commencing with Section 1798.80) of Part 4, a person, business,*  
11 *or public agency that sells goods or services to any resident of*  
12 *California and accepts as payment a credit card, debit card, or*  
13 *other payment device shall not do any of the following:*

14 *(1) Store payment related data, except when the person,*  
15 *business, or public agency has a payment data retention and*  
16 *disposal policy, which limits the amount of payment related data*  
17 *and the time that data is retained to the amount and time that is*  
18 *required for business, legal, or regulatory purposes as documented*  
19 *in the payment data retention policy, and payment related data is*  
20 *stored only for a time period and in a matter that is permitted by*  
21 *the policy.*

22 *(2) Store sensitive authentication data subsequent to*  
23 *authorization, even if that data is encrypted. Sensitive*  
24 *authentication data includes, but is not limited to, all of the*  
25 *following:*

26 *(A) The full contents of any data track from a payment card or*  
27 *other payment device.*

28 *(B) The card verification code or any value used to verify*  
29 *transactions when the payment device is not present.*

30 *(C) The personal identification number (PIN) or the encrypted*  
31 *PIN block.*

32 *(3) Store any payment related data that is not needed for*  
33 *business purposes.*

34 *(4) Store any of the following data elements:*

35 *(A) Payment verification code.*

36 *(B) Payment verification value.*

37 *(C) PIN verification value.*

38 *(5) Retain the primary account number unless retained in a*  
39 *manner consistent with the other requirements of this subdivision*

1 *and in a form that is expected to be indecipherable by unauthorized*  
 2 *persons.*

3 *(6) Send payment related data across any network unless the*  
 4 *data is encrypted using strong cryptography and security protocols.*

5 *(7) Fail to limit access to payment related data only to those*  
 6 *individuals whose job requires that access.*

7 *(c) This section shall not apply to any person or business who*  
 8 *is in compliance with Sections 6801 to 6809, inclusive, of Title 15*  
 9 *of the United States Code and who is subject to compliance*  
 10 *oversight by a state or federal regulatory agency with respect to*  
 11 *those sections.*

12 SEC. 2. Section 1798.29 of the Civil Code, as added by Section  
 13 2 of Chapter 915 of the Statutes of 2002, is repealed.

14 SEC. 3. Section 1798.29 of the Civil Code, as added by Section  
 15 2 of Chapter 1054 of the Statutes of 2002, is amended to read:

16 1798.29. (a) (1) Any agency that owns or licenses  
 17 computerized data that includes personal information shall disclose  
 18 any breach of the security of the system following discovery or  
 19 notification of the breach in the security of the data to any resident  
 20 of California whose unencrypted personal information was, or is  
 21 reasonably believed to have been, acquired by an unauthorized  
 22 person. The disclosure shall be made in the most expedient time  
 23 possible and without unreasonable delay, consistent with the  
 24 legitimate needs of law enforcement, as provided in subdivision  
 25 (c), or any measures necessary to determine the scope of the breach  
 26 and restore the reasonable integrity of the data system.

27 *(2) Notification to California residents pursuant to this*  
 28 *subdivision shall be written in plain language and shall include,*  
 29 *at a minimum, all of the following information if that information*  
 30 *is available at the time the notice is provided:*

31 *(A) The date of the notice.*

32 *(B) The name of the agency that maintained the computerized*  
 33 *data at the time of the breach.*

34 *(C) The date, or estimated date, that the breach occurred, if the*  
 35 *breach is possible to determine.*

36 *(D) A description of the categories of personal information that*  
 37 *was, or is reasonably believed to have been, acquired by an*  
 38 *unauthorized person.*

39 *(E) A toll-free telephone number for the agency subject to the*  
 40 *breach of the security of that agency's system or, if the primary*

1 *method used by that agency to communicate with the individual*  
2 *is by electronic means, an electronic mail address that the*  
3 *individual may use to contact the agency so that the individual*  
4 *may learn what types of personal information that agency*  
5 *maintained about the individual was subject to the security breach.*  
6 *If the agency that experienced the breach does not have a toll-free*  
7 *telephone number, a local telephone number may be provided to*  
8 *the California resident to contact the agency.*

9 *(F) The toll-free telephone numbers and addresses for the major*  
10 *credit reporting agencies.*

11 *(3) A copy of the notice sent to California residents pursuant*  
12 *to this section shall be provided to the Office of Privacy Protection.*

13 *(b) (1) Any agency that maintains computerized data that*  
14 *includes personal information that the agency does not own shall*  
15 *notify the owner or licensee of the information of any breach of*  
16 *the security of the data immediately following discovery, if the*  
17 *personal information was, or is reasonably believed to have been,*  
18 *acquired by an unauthorized person.*

19 ~~*(2) A copy of the notice sent pursuant to this section shall be*~~  
20 ~~*provided to the Office of Privacy Protection. Notification pursuant*~~  
21 ~~*to this section shall be written in plain English and shall include,*~~  
22 ~~*at a minimum, all of the following:*~~

23 ~~*(A) The date of the notice.*~~

24 ~~*(B) The name of the agency that maintained the computerized*~~  
25 ~~*data at the time of the breach.*~~

26 ~~*(C) The date on which the breach, if it is possible to determine.*~~

27 ~~*(D) A description of the categories of personal information that*~~  
28 ~~*was, or is reasonably believed to have been, acquired by an*~~  
29 ~~*unauthorized person.*~~

30 ~~*(E) A toll-free telephone number or, if the primary method used*~~  
31 ~~*by the agency to communicate with the individual is by electronic*~~  
32 ~~*means, an electronic mail address that the individual may use to*~~  
33 ~~*contact the agency, so that the individual may learn what types of*~~  
34 ~~*personal information the agency maintained about that individual*~~  
35 ~~*that was subject to the security breach.*~~

36 ~~*(F) The toll-free telephone numbers and addresses for the major*~~  
37 ~~*credit reporting agencies.*~~

38 *(2) Notification pursuant to this subdivision shall include, at a*  
39 *minimum, all of the information described in subparagraphs (B)*  
40 *to (E), inclusive, of paragraph (2) of subdivision (a), and*

1 *information sufficient to identify the person or persons whose*  
2 *encrypted personal information was, or may have been, acquired*  
3 *by an unauthorized person.*

4 (c) The notification required by this section may be delayed if  
5 a law enforcement agency determines that the notification will  
6 impede a criminal investigation. The notification required by this  
7 section shall be made after the law enforcement agency determines  
8 that it will not compromise the investigation.

9 (d) For purposes of this section, “breach of the security of the  
10 system” means unauthorized acquisition of computerized data that  
11 compromises the security, confidentiality, or integrity of personal  
12 information maintained by the agency. Good faith acquisition of  
13 personal information by an employee or agent of the agency for  
14 the purposes of the agency is not a breach of the security of the  
15 system, provided that the personal information is not used or  
16 subject to further unauthorized disclosure.

17 (e) For purposes of this section, “personal information” means  
18 an individual’s first name or first initial and last name in  
19 combination with any one or more of the following data elements,  
20 when either the name or the data elements are not encrypted:

21 (1) Social security number.

22 (2) Driver’s license number or California identification card  
23 number.

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

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

31 (g) For purposes of this section, “notice” may be provided by  
32 one of the following methods:

33 (1) Written notice.

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

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

1 contact information. Substitute notice shall consist of all of the  
2 following:

3 (A) E-mail notice when the agency has an e-mail address for  
4 the subject persons.

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

7 (C) Notification to major statewide media.

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

15 *(i) If notice is required to be provided pursuant to this section,*  
16 *the owner or licensee of the personal information shall be entitled*  
17 *to reimbursement from the agency that maintains the computerized*  
18 *data for all reasonable and actual costs of providing notice to*  
19 *consumers regarding the breach of the security of the system as*  
20 *required by this section. Reasonable and actual costs shall include,*  
21 *but are not limited to, the cost of card replacement as a result of*  
22 *the breach of the security of the system.*

23 SEC. 4. Section 1798.82 of the Civil Code, as added by Section  
24 4 of Chapter 915 of the Statutes of 2002, is repealed.

25 SEC. 5. Section 1798.82 of the Civil Code, as added by Section  
26 4 of Chapter 1054 of the Statutes of 2002, is amended to read:

27 1798.82. (a) (1) Any person or business that conducts business  
28 in California, and that owns or licenses computerized data that  
29 includes personal information, shall disclose any breach of the  
30 security of the system following discovery or notification of the  
31 breach in the security of the data to any resident of California  
32 whose unencrypted personal information was, or is reasonably  
33 believed to have been, acquired by an unauthorized person. The  
34 disclosure shall be made in the most expedient time possible and  
35 without unreasonable delay, consistent with the legitimate needs  
36 of law enforcement, as provided in subdivision (c), or any measures  
37 necessary to determine the scope of the breach and restore the  
38 reasonable integrity of the data system.

39 *(2) Notification to California residents pursuant to this*  
40 *subdivision shall be written in plain language and shall include,*

1 at a minimum, all of the following information if that information  
2 is available at the time the notice is provided:

3 (A) The date of the notice.

4 (B) The name of the person or business that maintained the  
5 computerized data at the time of the breach.

6 (C) The date, or estimated date, that the breach occurred, if the  
7 breach is possible to determine.

8 (D) A description of the categories of personal information that  
9 was, or is reasonably believed to have been, acquired by an  
10 unauthorized person.

11 (E) A toll-free telephone number for the person or business  
12 subject to the breach of the security of the system of that person  
13 or business or, if the primary method used by that person or  
14 business to communicate with the individual is by electronic means,  
15 an electronic mail address that the individual may use to contact  
16 the person or business so that the individual may learn what types  
17 of personal information that person or business maintained about  
18 the individual was subject to the security breach. If the person or  
19 business that experienced the breach does not have a toll-free  
20 telephone number, a local telephone number may be provided to  
21 the California resident to contact the person or business.

22 (F) The toll-free telephone numbers and addresses for the major  
23 credit reporting agencies.

24 (3) A copy of the notice sent to California residents pursuant  
25 to this section shall be provided to the Office of Privacy Protection.

26 (b) (1) Any person or business that maintains computerized  
27 data that includes personal information that the person or business  
28 does not own shall notify the owner or licensee of the information  
29 of any breach of the security of the data immediately following  
30 discovery, if the personal information was, or is reasonably  
31 believed to have been, acquired by an unauthorized person.

32 ~~(2) A copy of the notice sent pursuant to this section shall be  
33 provided to the Office of Privacy Protection. Notification pursuant  
34 to this section shall be written in plain English and shall include,  
35 at a minimum, all of the following:~~

36 ~~(A) The date of the notice.~~

37 ~~(B) The name of the person or business that maintained the  
38 computerized data at the time of the breach.~~

39 ~~(C) The date on which the breach occurred, if it is possible to  
40 determine.~~

1 ~~(D) A description of the categories of personal information that~~  
2 ~~was, or is reasonably believed to have been, acquired by an~~  
3 ~~unauthorized person.~~

4 ~~(E) A toll-free telephone number or, if the primary method used~~  
5 ~~by the person or business to communicate with the individual is~~  
6 ~~by electronic means, an electronic mail address that the individual~~  
7 ~~may use to contact the person or business or their agent, so that~~  
8 ~~the individual may learn what types of personal information the~~  
9 ~~person or business maintained about that individual that was subject~~  
10 ~~to the security breach.~~

11 ~~(F) The toll-free telephone numbers and addresses for the major~~  
12 ~~credit reporting agencies.~~

13 *(2) Notification pursuant to this subdivision shall include, at a*  
14 *minimum, all of the information described in subparagraphs (B)*  
15 *to (E), inclusive, of paragraph (2) of subdivision (a), and*  
16 *information sufficient to identify the person or persons whose*  
17 *encrypted personal information was, or may have been, acquired*  
18 *by an unauthorized person.*

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

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

33 (e) For purposes of this section, “personal information” means  
34 an individual’s first name or first initial and last name in  
35 combination with 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 (f) For purposes of this section, "personal information" does  
5 not include publicly available information that is lawfully made  
6 available to the general public from federal, state, or local  
7 government records.

8 (g) 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) E-mail notice when the person or business has an e-mail  
21 address for the subject persons.

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

25 (C) Notification to major statewide media.

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

34 (i) If notice is required to be provided pursuant to this section,  
35 the owner or licensee of the personal information shall be entitled  
36 to reimbursement from the person or business that maintains the  
37 computerized data for all reasonable and actual costs of providing  
38 notice to consumers regarding the breach of the security of the  
39 system as required by this section. *Reasonable and actual costs*

- 1 *shall include, but are not limited to, the cost of card replacement*
- 2 *as a result of the breach of the security of the system.*

O