

AMENDED IN ASSEMBLY AUGUST 5, 2002  
AMENDED IN ASSEMBLY JULY 25, 2002  
AMENDED IN ASSEMBLY JUNE 30, 2002  
AMENDED IN ASSEMBLY JUNE 20, 2002  
AMENDED IN ASSEMBLY JUNE 6, 2002  
AMENDED IN SENATE MARCH 20, 2002

**SENATE BILL**

**No. 1386**

---

---

**Introduced by Senator Peace**  
(Principal coauthor: Assembly Member Simitian)

February 12, 2002

---

---

An act to amend, renumber, and add Section 1798.82 of, and to add Section 1798.29 to, the Civil Code, relating to personal information, and declaring the urgency thereof, to take effect immediately.

LEGISLATIVE COUNSEL'S DIGEST

SB 1386, as amended, Peace. Personal information: privacy.

(1) Existing law regulates the maintenance and dissemination of personal information by state agencies, as defined, and requires each agency to keep an accurate account of disclosures made pursuant to specified provisions. Existing law also requires a business, as defined, to take all reasonable steps to destroy a customer's records that contain personal information when the business will no longer retain those records. Existing law provides civil remedies for violations of these provisions.

This bill would require a state agency, person, or business that owns or licenses computerized data that includes personal information, as

defined, to disclose in specified ways, any breach of the security of the data, as defined, to any person whose unencrypted personal information was, or is reasonably believed to have been, accessed by an unauthorized person. The bill would permit the notifications required by its provisions to be delayed if a law enforcement agency determines that it would impede a criminal investigation. The bill would require an agency, person, or business that maintains computerized data that includes personal information owned by another to notify the owner or licensee of the information of any breach of security of the data, as specified. This bill would also make a statement of legislative findings and declarations regarding privacy and financial security.

(2) This bill would declare that it is to take effect immediately as an urgency statute.

Vote: <sup>2</sup>/<sub>3</sub>. Appropriation: no. Fiscal committee: yes. State-mandated local program: no.

*The people of the State of California do enact as follows:*

1 SECTION 1. (a) The privacy and financial security of  
2 individuals is increasingly at risk due to the ever more widespread  
3 collection of personal information by both the private and public  
4 sector.

5 (b) Credit card transactions, magazine subscriptions, telephone  
6 numbers, real estate records, automobile registrations, consumer  
7 surveys, warranty registrations, credit reports, and Internet Web  
8 sites are all sources of personal information and form the source  
9 material for identity thieves.

10 (c) Identity theft is one of the fastest growing crimes committed  
11 in California. Criminals who steal personal information such as  
12 social security numbers use the information to open credit card  
13 accounts, write bad checks, buy cars, and commit other financial  
14 crimes with other people's identities. The Los Angeles County  
15 Sheriff's Department reports that the 1,932 identity theft cases it  
16 received in the year 2000 represented a 108 percent increase over  
17 the previous year's caseload.

18 (d) Identity theft is costly to the marketplace and to consumers.  
19 The Secret Service estimated the cost of identity theft at seven  
20 hundred forty-five million dollars (\$745,000,000) in the year  
21 1997. According to a May 2000 survey by CalPIRG and the  
22 Privacy Rights Clearinghouse, the average consumer victim



1 spends 175 hours and eight hundred dollars (\$800) resolving  
2 identity theft problems. During this time, consumers often have  
3 trouble establishing new credit, renting apartments, and finding  
4 employment, since many applications require a credit check as  
5 part of the approval process.

6 (e) According to the Attorney General, victims of identity theft  
7 must act quickly to minimize the damage; therefore expeditious  
8 notification of possible misuse of a person’s personal information  
9 is imperative.

10 SEC. 2. Section 1798.29 is added to the Civil Code, to read:

11 1798.29. (a) Any agency that owns or licenses computerized  
12 data that includes personal information shall disclose any breach  
13 of the security of the system ~~immediately~~ following discovery or  
14 notification of the breach in the security of the data to any person  
15 whose unencrypted personal information was, or is reasonably  
16 believed to have been, accessed by an unauthorized person. The  
17 disclosure shall be made in the most expedient time possible and  
18 without unreasonable delay, consistent with the legitimate needs  
19 of law enforcement, as provided in subdivision (c), ~~and~~ or any  
20 measures necessary to determine the scope of the breach and  
21 restore the reasonable integrity of the data system.

22 (b) Any agency that maintains computerized data that includes  
23 personal information that the agency does not own shall notify the  
24 owner or licensee of the information of any breach of the security  
25 of the data immediately following discovery, if the personal  
26 information was, or is reasonably believed to have been, accessed  
27 by an unauthorized person.

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

33 (d) For purposes of this section, “breach of the security of the  
34 system” means unauthorized access to computerized data that  
35 compromises the security, confidentiality, or integrity of personal  
36 information maintained by the agency.

37 (e) For purposes of this section, “personal information” means  
38 an individual’s first and last name in combination with any one or  
39 more of the following:

40 (1) Social security number.



1 (2) Driver's license number or California Identification Card  
2 number.

3 (3) 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 (f) For purposes of this section, "personal information" does  
8 not include publicly available information that is lawfully made  
9 available to the general public from federal, state, or local  
10 government records.

11 (g) For purposes of this section, ~~notice~~ "notice" may be  
12 provided by one of the following methods:

13 (1) Written notice.

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

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

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

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

28 (C) Notification to major statewide media.

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

36 SEC. 3. Section 1798.82 of the Civil Code is amended and  
37 renumbered to read:

38 1798.84. (a) Any customer injured by a violation of this title  
39 may institute a civil action to recover damages.



1 (b) Any business that violates, proposes to violate, or has  
2 violated this title may be enjoined.

3 (c) The rights and remedies available under this section are  
4 cumulative to each other and to any other rights and remedies  
5 available under law.

6 SEC. 4. Section 1798.82 is added to the Civil Code, to read:

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

19 (b) Any person or business that maintains computerized data  
20 that includes personal information that the person or business does  
21 not own shall notify the owner or licensee of the information of any  
22 breach of the security of the data immediately following discovery,  
23 if the personal information was, or is reasonably believed to have  
24 been, accessed by an unauthorized person.

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

30 (d) For purposes of this section, “breach of the security of the  
31 system” means unauthorized access to computerized data that  
32 compromises the security, confidentiality, or integrity of personal  
33 information maintained by the person or business.

34 (e) For purposes of this section, “personal information” means  
35 an individual’s first and last name in combination with any one or  
36 more of the following:

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  
2 combination with any required security code, access code, or  
3 password that would permit access to an individual's financial  
4 account.

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

9 (g) For purposes of this section, ~~"notice"~~ "notice" may be  
10 provided by one of the following methods:

11 (1) Written notice.

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

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

22 (A) E-mail notice when the person or business has an e-mail  
23 address for the subject persons.

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

26 (C) Notification to major statewide media.

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

35 SEC. 5. This act is an urgency statute necessary for the  
36 immediate preservation of the public peace, health, or safety  
37 within the meaning of Article IV of the Constitution and shall go  
38 into immediate effect. The facts constituting the necessity are:

39 Because the recent incident at the Stephen P. Teale Data Center  
40 has put the financial information of hundreds of thousands of state



1 workers at risk of identity theft, and because, currently, an entity  
2 is not required to notify affected people when the security of its  
3 computer data system is compromised, it is necessary that this act  
4 take immediate effect.

O

