

ASSEMBLY BILL

No. 786

Introduced by Assembly Member Ruskin

February 18, 2005

An act to repeal and amend Section 1798.29 of the Civil Code, relating to identity theft.

LEGISLATIVE COUNSEL'S DIGEST

AB 786, as introduced, Ruskin. Identity theft: California State University employees.

Existing law requires an agency that owns or licenses computerized data that includes personal information to disclose any breach of the security of that system 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 the California State University system to provide an employee, upon request, with 4 hours of time off with pay following a disclosure by the university that there is, or could have been, a breach of security of employee personal information data, 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, as added by
- 2 Section 2 of Chapter 915 of the Statutes of 2002, is repealed.
- 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~~

1 of the breach in the security of the data to any resident of
2 California whose unencrypted personal information was, or is
3 reasonably believed to have been, acquired by an unauthorized
4 person. The disclosure shall be made in the most expedient time
5 possible and without unreasonable delay, consistent with the
6 legitimate needs of law enforcement, as provided in subdivision
7 (c), or any measures necessary to determine the scope of the
8 breach and restore the reasonable integrity of the data system.

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

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

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

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

33 (1) Social security number.

34 (2) Driver’s license number or California Identification Card
35 number.

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

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

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

7 ~~(1) Written notice.~~

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

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

17 ~~(A) E-mail notice when the agency has an e-mail address for~~
18 ~~the subject persons.~~

19 ~~(B) Conspicuous posting of the notice on the agency’s Web~~
20 ~~site page, if the agency maintains one.~~

21 ~~(C) Notification to major statewide media.~~

22 ~~(h) Notwithstanding subdivision (g), an agency that maintains~~
23 ~~its own notification procedures as part of an information security~~
24 ~~policy for the treatment of personal information and is otherwise~~
25 ~~consistent with the timing requirements of this part shall be~~
26 ~~deemed to be in compliance with the notification requirements of~~
27 ~~this section if it notifies subject persons in accordance with its~~
28 ~~policies in the event of a breach of security of the system.~~

29 SEC. 2. Section 1798.29 of the Civil Code, as added by
30 Section 2 of Chapter 1054 of the Statutes of 2002, is amended to
31 read:

32 1798.29. (a) Any agency that owns or licenses computerized
33 data that includes personal information shall disclose any breach
34 of the security of the system following discovery or notification
35 of the breach in the security of the data to any resident of
36 California whose unencrypted personal information was, or is
37 reasonably believed to have been, acquired by an unauthorized
38 person. The disclosure shall be made in the most expedient time
39 possible and without unreasonable delay, consistent with the
40 legitimate needs of law enforcement, as provided in subdivision

1 (c), or any measures necessary to determine the scope of the
2 breach and restore the reasonable integrity of the data system.

3 (b) Any agency that maintains computerized data that includes
4 personal information that the agency does not own shall notify
5 the owner or licensee of the information of any breach of the
6 security of the data immediately following discovery, if the
7 personal information was, or is reasonably believed to have been,
8 acquired by an unauthorized person.

9 (c) The notification required by this section may be delayed if
10 a law enforcement agency determines that the notification will
11 impede a criminal investigation. The notification required by this
12 section shall be made after the law enforcement agency
13 determines that it will not compromise the investigation.

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

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

27 (1) Social security number.

28 (2) Driver’s license number or California Identification Card
29 number.

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

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

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

40 (1) Written notice.

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

4 (3) Substitute notice, if the agency demonstrates that the cost
5 of providing notice would exceed two hundred fifty thousand
6 dollars (\$250,000), or that the affected class of subject persons to
7 be notified exceeds 500,000, or the agency does not have
8 sufficient contact information. Substitute notice shall consist of
9 all of the following:

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

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

14 (C) Notification to major statewide media.

15 (h) Notwithstanding subdivision (g), an agency that maintains
16 its own notification procedures as part of an information security
17 policy for the treatment of personal information and is otherwise
18 consistent with the timing requirements of this part shall be
19 deemed to be in compliance with the notification requirements of
20 this section if it notifies subject persons in accordance with its
21 policies in the event of a breach of security of the system.

22 *(i) Upon request by a California State University employee*
23 *following disclosure by the California State University to*
24 *employees that there is, or could have been, a breach of security*
25 *of personal information data pursuant to subdivision (a), the*
26 *university shall provide that employee with four hours time off*
27 *with pay to take all necessary steps to minimize damages*
28 *resulting, or that could result, from that breach, and to contact*
29 *law enforcement agencies pursuant to the Sections 530.6 and*
30 *530.8 of the Penal Code.*