

AMENDED IN ASSEMBLY AUGUST 30, 2013

AMENDED IN SENATE APRIL 15, 2013

SENATE BILL

No. 46

Introduced by Senator Corbett

December 14, 2012

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

LEGISLATIVE COUNSEL'S DIGEST

SB 46, as amended, Corbett. Personal information: privacy.

Existing law requires any agency, and any person or business conducting business in California, that owns or licenses computerized data that includes personal information, as defined, to disclose in specified ways, any 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 defines "personal information" for these purposes, to include an individual's first name and last name, or first initial and last name, in combination with one or more designated data elements relating to, among other things, social security numbers, driver's license numbers, financial accounts, and medical information.

This bill would revise certain data elements included within the definition of personal information, by adding certain information that would permit access to an online account.

This bill would impose additional requirements on the disclosure of a breach of the security of the system or data in situations where the breach involves personal information that would permit access to an online or email account.

This bill would incorporate additional changes to Section 1798.29 of the Civil Code proposed by AB 1149 that would become operative if this bill and AB 1149 are enacted and this bill is enacted last.

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

25 (d) Any 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:

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

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

5 (C) If the information is possible to determine at the time the
6 notice is provided, then any of the following: (i) the date of the
7 breach, (ii) the estimated date of the breach, or (iii) the date range
8 within which the breach occurred. The notification shall also
9 include the date of the notice.

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

13 (E) A general description of the breach incident, if that
14 information is possible to determine at the time the notice is
15 provided.

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

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

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

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

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

38 (5) *In the case of a breach of the security of the system involving*
39 *personal information defined in paragraph (2) of subdivision (g)*
40 *for login credentials of an email account furnished by the agency,*

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

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

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

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

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

30 (A) Social security number.

31 (B) Driver’s license number or California ~~Identification Card~~
32 *identification card* number.

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

37 (D) Medical information.

38 (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 ~~California Technology Agency~~.
35 *Department of Technology*.

36 (j) Notwithstanding subdivision (i), an agency that maintains
37 its own notification procedures as part of an information security
38 policy for the treatment of personal information and is otherwise
39 consistent with the timing requirements of this part shall be deemed
40 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 *SEC. 1.5. Section 1798.29 of the Civil Code is amended to*
4 *read:*

5 1798.29. (a) Any agency that owns or licenses computerized
6 data that includes personal information shall disclose any breach
7 of the security of the system following discovery or notification
8 of the breach in the security of the data to any resident of California
9 whose unencrypted personal information was, or is reasonably
10 believed to have been, acquired by an unauthorized person. The
11 disclosure shall be made in the most expedient time possible and
12 without unreasonable delay, consistent with the legitimate needs
13 of law enforcement, as provided in subdivision (c), or any measures
14 necessary to determine the scope of the breach and restore the
15 reasonable integrity of the data system.

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

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

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

30 (1) The security breach notification shall be written in plain
31 language.

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

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

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

38 (C) If the information is possible to determine at the time the
39 notice is provided, then any of the following: (i) the date of the
40 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 (3) At the discretion of the agency, the security breach
14 notification may also include any of the following:

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

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

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

31 (5) *In the case of a breach of the security of the system involving*
32 *personal information defined in paragraph (2) of subdivision (g)*
33 *for login credentials of an email account furnished by the agency,*
34 *the agency shall not comply with this section by providing the*
35 *security breach notification to that email address, but may, instead,*
36 *comply with this section by providing notice by another method*
37 *described in subdivision (i) or by clear and conspicuous notice*
38 *delivered to the resident online when the resident is connected to*
39 *the online account from an Internet Protocol address or online*

1 *location from which the agency knows the resident customarily*
2 *accesses the account.*

3 (e) Any agency that is required to issue a security breach
4 notification pursuant to this section to more than 500 California
5 residents as a result of a single breach of the security system shall
6 electronically submit a single sample copy of that security breach
7 notification, excluding any personally identifiable information, to
8 the Attorney General. A single sample copy of a security breach
9 notification shall not be deemed to be within subdivision (f) of
10 Section 6254 of the Government Code.

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

19 (g) For purposes of this section, “personal information” means
20 ~~an~~ *either of the following:*

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

24 ~~(1)~~

25 (A) Social security number.

26 ~~(2)~~

27 (B) Driver’s license number or ~~California Identification Card~~
28 *identification card* number.

29 ~~(3)~~

30 (C) 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 ~~(4)~~

35 (D) Medical information.

36 ~~(5)~~

37 (E) Health insurance information.

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

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

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

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

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

16 (1) Written notice.

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

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

26 (A) ~~E-mail~~ *Email* notice when the agency has an ~~e-mail~~ *email*
27 address for the subject persons.

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

30 (C) Notification to major statewide media and the Office of
31 Information Security within the ~~California Technology Agency~~.
32 *Department of Technology*.

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

1 (k) *Notwithstanding the exception specified in paragraph (4)*
2 *of subdivision (b) of Section 1798.3, for purposes of this section,*
3 *“agency” includes a local agency, as defined in subdivision (a)*
4 *of Section 6252 of the Government Code.*

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

6 1798.82. (a) Any person or business that conducts business
7 in California, and that owns or licenses computerized data that
8 includes personal information, shall disclose any breach of the
9 security of the system following discovery or notification of the
10 breach in the security of the data to any resident of California
11 whose unencrypted personal information was, or is reasonably
12 believed to have been, acquired by an unauthorized person. The
13 disclosure shall be made in the most expedient time possible and
14 without unreasonable delay, consistent with the legitimate needs
15 of law enforcement, as provided in subdivision (c), or any measures
16 necessary to determine the scope of the breach and restore the
17 reasonable integrity of the data system.

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

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

29 (d) Any person or business that is required to issue a security
30 breach notification pursuant to this section shall meet all of the
31 following requirements:

32 (1) The security breach notification shall be written in plain
33 language.

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

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

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

1 (C) If the information is possible to determine at the time the
2 notice is provided, then any of the following: (i) the date of the
3 breach, (ii) the estimated date of the breach, or (iii) the date range
4 within which the breach occurred. The notification shall also
5 include the date of the notice.

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

9 (E) A general description of the breach incident, if that
10 information is possible to determine at the time the notice is
11 provided.

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

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

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

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

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

35 (5) *In the case of a breach of the security of the system involving*
36 *personal information defined in paragraph (2) of subdivision (h)*
37 *for login credentials of an email account furnished by the person*
38 *or business, the person or business shall not comply with this*
39 *section by providing the security breach notification to that email*
40 *address, but may, instead, comply with this section by providing*

1 notice by another method described in subdivision (j) or by clear
2 and conspicuous notice delivered to the resident online when the
3 resident is connected to the online account from an Internet
4 Protocol address or online location from which the person or
5 business knows the resident customarily accesses the account.

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

14 (f) Any person or business that is required to issue a security
15 breach notification pursuant to this section to more than 500
16 California residents as a result of a single breach of the security
17 system shall electronically submit a single sample copy of that
18 security breach notification, excluding any personally identifiable
19 information, to the Attorney General. A single sample copy of a
20 security breach notification shall not be deemed to be within
21 subdivision (f) of Section 6254 of the Government Code.

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

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

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

36 (A) Social security number.

37 (B) Driver’s license number or ~~California Identification Card~~
38 *identification card* number.

39 (C) Account number, credit or debit card number, in
40 combination with any required security code, access code, or

1 password that would permit access to an individual’s financial
2 account.

3 (D) Medical information.

4 (E) Health insurance information.

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

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

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

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

21 (j) For purposes of this section, “notice” may be provided by
22 one of the following methods:

23 (1) Written notice.

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

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

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

35 (B) Conspicuous posting of the notice on the Internet Web site
36 page of the person or business, if the person or business maintains
37 one.

38 (C) Notification to major statewide ~~media and the Office of~~
39 ~~Privacy Protection within the State and Consumer Services Agency.~~
40 *media.*

1 (k) Notwithstanding subdivision (j), a person or business that
2 maintains its own notification procedures as part of an information
3 security policy for the treatment of personal information and is
4 otherwise consistent with the timing requirements of this part, shall
5 be deemed to be in compliance with the notification requirements
6 of this section if the person or business notifies subject persons in
7 accordance with its policies in the event of a breach of security of
8 the system.

9 *SEC. 3. Section 1.5 of this bill incorporates amendments to*
10 *Section 1798.29 of the Civil Code proposed by both this bill and*
11 *Assembly Bill 1149. It shall only become operative if (1) both bills*
12 *are enacted and become effective on or before January 1, 2014,*
13 *(2) each bill amends Section 1798.29 of the Civil Code, and (3)*
14 *this bill is enacted after Assembly Bill 1149, in which case Section*
15 *1 of this bill shall not become operative.*