

AMENDED IN ASSEMBLY MAY 27, 2016

CALIFORNIA LEGISLATURE—2015–16 REGULAR SESSION

ASSEMBLY BILL

No. 2828

Introduced by Assembly Member Chau

February 19, 2016

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

LEGISLATIVE COUNSEL'S DIGEST

AB 2828, as amended, Chau. Personal information: privacy: breach.

Existing law requires a person or business conducting business in California and any agency, as defined, that owns or licenses computerized data that includes personal information, as defined, to disclose a breach in the security of the data to a resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person in the most expedient time possible and without unreasonable delay, as specified.

This bill would also require a person or business conducting business in California, and any agency, that owns or licenses computerized data that includes personal information to disclose a breach of the security of the data to a resident of California whose encrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person ~~if the encryption key or security credential, as defined, has, or is reasonably believed to have been, acquired by an unauthorized person at any time before or after the breach of security of the data.~~ *and the encryption key or security credential was, or is reasonably believed to have been, acquired by an unauthorized person and the person, business, or agency that owns or licenses the encrypted*

information has a reasonable belief that the encryption key or security credential could render that personal information readable or useable.

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 (1) whose unencrypted personal information was, or is reasonably
8 believed to have been, acquired by an unauthorized person, or, ~~if~~
9 ~~the encryption key or security credential has, or is reasonably~~
10 ~~believed to have been, acquired by an unauthorized person at any~~
11 ~~time before or after the breach of security of the data, to a resident~~
12 ~~of California whose encrypted personal information was, or is~~
13 ~~reasonably believed to have been, acquired by an unauthorized~~
14 ~~person.~~ (2) *whose encrypted personal information was, or is*
15 *reasonably believed to have been, acquired by an unauthorized*
16 *person and the encryption key or security credential was, or is*
17 *reasonably believed to have been, acquired by an unauthorized*
18 *person and the agency that owns or licenses the encrypted*
19 *information has a reasonable belief that the encryption key or*
20 *security credential could render that personal information readable*
21 *or useable.* The disclosure shall be made in the most expedient
22 time possible and without unreasonable delay, consistent with the
23 legitimate needs of law enforcement, as provided in subdivision
24 (c), or any measures necessary to determine the scope of the breach
25 and restore the reasonable integrity of the data system.
26 (b) Any agency that maintains computerized data that includes
27 personal information that the agency does not own shall notify the
28 owner or licensee of the information of any breach of the security
29 of the data immediately following discovery, if the personal
30 information was, or is reasonably believed to have been, acquired
31 by an unauthorized person.
32 (c) The notification required by this section may be delayed if
33 a law enforcement agency determines that the notification will

1 impede a criminal investigation. The notification required by this
2 section shall be made after the law enforcement agency determines
3 that it will not compromise the investigation.

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

7 (1) The security breach notification shall be written in plain
8 language, shall be titled “Notice of Data Breach,” and shall present
9 the information described in paragraph (2) under the following
10 headings: “What Happened,” “What Information Was Involved,”
11 “What We Are Doing,” “What You Can Do,” and “For More
12 Information.” Additional information may be provided as a
13 supplement to the notice.

14 (A) The format of the notice shall be designed to call attention
15 to the nature and significance of the information it contains.

16 (B) The title and headings in the notice shall be clearly and
17 conspicuously displayed.

18 (C) The text of the notice and any other notice provided pursuant
19 to this section shall be no smaller than 10-point type.

20 (D) For a written notice described in paragraph (1) of
21 subdivision (i), use of the model security breach notification form
22 prescribed below or use of the headings described in this paragraph
23 with the information described in paragraph (2), written in plain
24 language, shall be deemed to be in compliance with this
25 subdivision.

| | | |
|------------------------------|--|---------------------|
| [NAME OF INSTITUTION / LOGO] | | Date: [insert date] |
| NOTICE OF DATA BREACH | | |
| What Happened? | | |
| | | |

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33

| | |
|--|--|
| What Information Was Involved? | |
| What We Are Doing. | |
| What You Can Do. | |
| Other Important Information. [insert other important information] | |
| For More Information. | Call [telephone number] or go to [Internet Web site] |

34 (E) For an electronic notice described in paragraph (2) of
35 subdivision (i), use of the headings described in this paragraph
36 with the information described in paragraph (2), written in plain
37 language, shall be deemed to be in compliance with this
38 subdivision.

1 (2) The security breach notification described in paragraph (1)
2 shall include, at a minimum, the following information:

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

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

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

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

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

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

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

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

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

28 (e) Any agency that is required to issue a security breach
29 notification pursuant to this section to more than 500 California
30 residents as a result of a single breach of the security system shall
31 electronically submit a single sample copy of that security breach
32 notification, excluding any personally identifiable information, to
33 the Attorney General. A single sample copy of a security breach
34 notification shall not be deemed to be within subdivision (f) of
35 Section 6254 of the Government Code.

36 (f) For purposes of this section, "breach of the security of the
37 system" means unauthorized acquisition of computerized data that
38 compromises the security, confidentiality, or integrity of personal
39 information maintained by the agency. Good faith acquisition of
40 personal information by an employee or agent of the agency for

1 the purposes of the agency is not a breach of the security of the
2 system, provided that the personal information is not used or
3 subject to further unauthorized disclosure.

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

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

9 (A) Social security number.

10 (B) Driver’s license number or California identification card
11 number.

12 (C) Account ~~number~~, *number* or credit or debit card number,
13 in combination with any required security code, access code, or
14 password that would permit access to an individual’s financial
15 account.

16 (D) Medical information.

17 (E) Health insurance information.

18 (F) Information or data collected through the use or operation
19 of an automated license plate recognition system, as defined in
20 Section 1798.90.5.

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

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

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

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

37 (4) For purposes of this section, “encrypted” means rendered
38 unusable, unreadable, or indecipherable to an unauthorized person
39 through a security technology or methodology generally accepted
40 in the field of information security.

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

3 (1) Written notice.

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

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

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

15 (B) Conspicuous posting, for a minimum of 30 days, of the
16 notice on the agency’s Internet Web site page, if the agency
17 maintains one. For purposes of this subparagraph, conspicuous
18 posting on the agency’s Internet Web site means providing a link
19 to the notice on the home page or first significant page after
20 entering the Internet Web site that is in larger type than the
21 surrounding text, or in contrasting type, font, or color to the
22 surrounding text of the same size, or set off from the surrounding
23 text of the same size by symbols or other marks that call attention
24 to the link.

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

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

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

21 (l) For purposes of this section, “encryption key” and “security
22 credential” mean ~~any information that could be used by an~~
23 ~~unauthorized person to access or decrypt encrypted personal~~
24 ~~information contained in a data system.~~ *the confidential key or*
25 *process designed to render the data useable, readable, and*
26 *decipherable.*

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

28 1798.82. (a) A person or business that conducts business in
29 California, and that owns or licenses computerized data that
30 includes personal information, shall disclose a breach of the
31 security of the system following discovery or notification of the
32 breach in the security of the data to a resident of California (1)
33 whose unencrypted personal information was, or is reasonably
34 believed to have been, acquired by an unauthorized person, or, ~~if~~
35 ~~the encryption key or security credential has, or is reasonably~~
36 ~~believed to have been, acquired by an unauthorized person at any~~
37 ~~time before or after the breach of security of the data, to a resident~~
38 ~~of California whose encrypted personal information was, or is~~
39 ~~reasonably believed to have been, acquired by an unauthorized~~
40 ~~person.~~ (2) *whose encrypted personal information was, or is*

1 *reasonably believed to have been, acquired by an unauthorized*
2 *person and the encryption key or security credential was, or is*
3 *reasonably believed to have been, acquired by an unauthorized*
4 *person and the person or business that owns or licenses the*
5 *encrypted information has a reasonable belief that the encryption*
6 *key or security credential could render that personal information*
7 *readable or useable. The disclosure shall be made in the most*
8 expedient time possible and without unreasonable delay, consistent
9 with the legitimate needs of law enforcement, as provided in
10 subdivision (c), or any measures necessary to determine the scope
11 of the breach and restore the reasonable integrity of the data system.

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

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

23 (d) A person or business that is required to issue a security
24 breach notification pursuant to this section shall meet all of the
25 following requirements:

26 (1) The security breach notification shall be written in plain
27 language, shall be titled "Notice of Data Breach," and shall present
28 the information described in paragraph (2) under the following
29 headings: "What Happened," "What Information Was Involved,"
30 "What We Are Doing," "What You Can Do," and "For More
31 Information." Additional information may be provided as a
32 supplement to the notice.

33 (A) The format of the notice shall be designed to call attention
34 to the nature and significance of the information it contains.

35 (B) The title and headings in the notice shall be clearly and
36 conspicuously displayed.

37 (C) The text of the notice and any other notice provided pursuant
38 to this section shall be no smaller than 10-point type.

39 (D) For a written notice described in paragraph (1) of
40 subdivision (j), use of the model security breach notification form

1 prescribed below or use of the headings described in this paragraph
 2 with the information described in paragraph (2), written in plain
 3 language, shall be deemed to be in compliance with this
 4 subdivision.

5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39

| | | |
|--|--|---------------------|
| [NAME OF INSTITUTION / LOGO] | | Date: [insert date] |
| NOTICE OF DATA BREACH | | |
| What Happened? | | |
| What Information Was Involved? | | |
| What We Are Doing. | | |
| What You Can Do. | | |
| Other Important Information. [insert other important information] | | |

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38

| | |
|-----------------------|--|
| | |
| For More Information. | Call [telephone number] or go to [Internet Web site] |

(E) For an electronic notice described in paragraph (2) of subdivision (j), use of the headings described in this paragraph with the information described in paragraph (2), written in plain language, shall be deemed to be in compliance with this subdivision.

(2) The security breach notification described in paragraph (1) shall include, at a minimum, the following information:

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

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

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

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

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

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

1 (G) If the person or business providing the notification was the
2 source of the breach, an offer to provide appropriate identity theft
3 prevention and mitigation services, if any, shall be provided at no
4 cost to the affected person for not less than 12 months along with
5 all information necessary to take advantage of the offer to any
6 person whose information was or may have been breached if the
7 breach exposed or may have exposed personal information defined
8 in subparagraphs (A) and (B) of paragraph (1) of subdivision (h).

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

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

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

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

23 (f) A person or business that is required to issue a security breach
24 notification pursuant to this section to more than 500 California
25 residents as a result of a single breach of the security system shall
26 electronically submit a single sample copy of that security breach
27 notification, excluding any personally identifiable information, to
28 the Attorney General. A single sample copy of a security breach
29 notification shall not be deemed to be within subdivision (f) of
30 Section 6254 of the Government Code.

31 (g) For purposes of this section, “breach of the security of the
32 system” means unauthorized acquisition of computerized data that
33 compromises the security, confidentiality, or integrity of personal
34 information maintained by the person or business. Good faith
35 acquisition of personal information by an employee or agent of
36 the person or business for the purposes of the person or business
37 is not a breach of the security of the system, provided that the
38 personal information is not used or subject to further unauthorized
39 disclosure.

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

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

6 (A) Social security number.

7 (B) Driver’s license number or California identification card
8 number.

9 (C) ~~Account number~~, *number or credit or debit card number*,
10 in combination with any required security code, access code, or
11 password that would permit access to an individual’s financial
12 account.

13 (D) Medical information.

14 (E) Health insurance information.

15 (F) Information or data collected through the use or operation
16 of an automated license plate recognition system, as defined in
17 Section 1798.90.5.

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

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

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

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

34 (4) For purposes of this section, “encrypted” means rendered
35 unusable, unreadable, or indecipherable to an unauthorized person
36 through a security technology or methodology generally accepted
37 in the field of information security.

38 (j) 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 forth
3 in Section 7001 of Title 15 of the United States Code.

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

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

12 (B) Conspicuous posting, for a minimum of 30 days, of the
13 notice on the Internet Web site page of the person or business, if
14 the person or business maintains one. For purposes of this
15 subparagraph, conspicuous posting on the person's or business's
16 Internet Web site means providing a link to the notice on the home
17 page or first significant page after entering the Internet Web site
18 that is in larger type than the surrounding text, or in contrasting
19 type, font, or color to the surrounding text of the same size, or set
20 off from the surrounding text of the same size by symbols or other
21 marks that call attention to the link.

22 (C) Notification to major statewide media.

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

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

1 address, but may, instead, comply with this section by providing
2 notice by another method described in this subdivision or by clear
3 and conspicuous notice delivered to the resident online when the
4 resident is connected to the online account from an Internet
5 Protocol address or online location from which the person or
6 business knows the resident customarily accesses the account.

7 (k) For purposes of this section, “encryption key” and “security
8 credential” mean ~~any information that could be used by an~~
9 ~~unauthorized person to access or decrypt encrypted personal~~
10 ~~information contained in a data system.~~ *the confidential key or*
11 *process designed to render data useable, readable, and*
12 *decipherable.*

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