

AMENDED IN ASSEMBLY MAY 5, 2015

AMENDED IN ASSEMBLY APRIL 23, 2015

AMENDED IN ASSEMBLY MARCH 26, 2015

CALIFORNIA LEGISLATURE—2015–16 REGULAR SESSION

ASSEMBLY BILL

No. 964

Introduced by Assembly Member Chau

February 26, 2015

An act to amend Sections 1798.29 and 1798.82 of the Civil Code, relating to civil law.

LEGISLATIVE COUNSEL’S DIGEST

AB 964, as amended, Chau. Civil law: privacy.

Existing law requires a person or business conducting business in California, or any state or local agency, that owns or licenses computerized data that includes personal information, as defined, to disclose in specified ways, a 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 requires the disclosure to be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

This bill would define “encrypted” for purpose of these provisions to mean rendered unusable, unreadable, or indecipherable through a security technology or methodology generally accepted in the field of information technology.

Existing law requires a person, business, or a state or local agency, that is required to issue a security breach notification to more than 500 California residents as a result of a single breach of the security system to electronically submit a single sample copy of that security breach notification to the Attorney General.

This bill would also require a person or business, or state or local agency that is required to issue a security breach notification under these circumstances to inform the Attorney General of the date of the discovery of the breach.

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.

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

4 (1) The security breach notification shall be written in plain
5 language.

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

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

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

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

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

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

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

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

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

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

33 (4) In the case of a breach of the security of the system involving
34 personal information defined in paragraph (2) of subdivision (g)
35 for an online account, and no other personal information defined
36 in paragraph (1) of subdivision (g), the agency may comply with
37 this section by providing the security breach notification in
38 electronic or other form that directs the person whose personal
39 information has been breached to promptly change his or her
40 password and security question or answer, as applicable, or to take

1 other steps appropriate to protect the online account with the
2 agency and all other online accounts for which the person uses the
3 same user name or email address and password or security question
4 or answer.

5 (5) In the case of a breach of the security of the system involving
6 personal information defined in paragraph (2) of subdivision (g)
7 for login credentials of an email account furnished by the agency,
8 the agency shall not comply with this section by providing the
9 security breach notification to that email address, but may, instead,
10 comply with this section by providing notice by another method
11 described in subdivision (i) or by clear and conspicuous notice
12 delivered to the resident online when the resident is connected to
13 the online account from an Internet Protocol address or online
14 location from which the agency knows the resident customarily
15 accesses the account.

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

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

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

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

38 (A) Social security number.

39 (B) Driver’s license number or California identification card
40 number.

1 (C) 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 (D) Medical information.

6 (E) Health insurance information.

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

10 (h) (1) For purposes of this section, "personal information"
11 does not include publicly available information that is lawfully
12 made available to the general public from federal, state, or local
13 government records.

14 (2) For purposes of this section, "medical information" means
15 any information regarding an individual's medical history, mental
16 or physical condition, or medical treatment or diagnosis by a health
17 care professional.

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

23 (4) For purposes of this section, "encrypted" means rendered
24 unusable, unreadable, or indecipherable through a security
25 technology or methodology generally accepted in the field of
26 information security.

27 (i) For purposes of this section, "notice" may be provided by
28 one of the following methods:

29 (1) Written notice.

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

33 (3) Substitute notice, if the agency demonstrates that the cost
34 of providing notice would exceed two hundred fifty thousand
35 dollars (\$250,000), or that the affected class of subject persons to
36 be notified exceeds 500,000, or the agency does not have sufficient
37 contact information. Substitute notice shall consist of all of the
38 following:

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

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

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

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

12 (k) Notwithstanding the exception specified in paragraph (4) of
13 subdivision (b) of Section 1798.3, for purposes of this section,
14 "agency" includes a local agency, as defined in subdivision (a) of
15 Section 6252 of the Government Code.

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

17 1798.82. (a) A person or business that conducts business in
18 California, and that owns or licenses computerized data that
19 includes personal information, shall disclose a breach of the
20 security of the system following discovery or notification, pursuant
21 to subdivision (b), of the breach in the security of the data to a
22 resident of California whose unencrypted personal information
23 was, or is reasonably believed to have been, acquired by an
24 unauthorized person. The disclosure shall be made in the most
25 expedient time possible and without unreasonable delay, consistent
26 with the legitimate needs of law enforcement, as provided in
27 subdivision (c), or any measures ~~reasonably~~ necessary to determine
28 the scope of the breach and restore the reasonable integrity of the
29 data system.

30 (b) A person or business that maintains computerized data that
31 includes personal information that the person or business does not
32 own shall notify the owner or licensee of the information of the
33 breach of the security of the data immediately following discovery,
34 if the personal information was, or is reasonably believed to have
35 been, acquired by an unauthorized person.

36 (c) The notification required by this section may be delayed if
37 a law enforcement agency determines that the notification will
38 impede a criminal investigation. The notification required by this
39 section shall be made promptly after the law enforcement agency
40 determines that it will not compromise the investigation.

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

4 (1) The security breach notification shall be written in plain
5 language.

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

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

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

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

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

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

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

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

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

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

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

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

(5) In the case of a breach of the security of the system involving personal information defined in paragraph (2) of subdivision (h) for login credentials of an email account furnished by the person or business, the person or business shall not comply with this section by providing the security breach notification to that email address, but may, instead, comply with this section by providing notice by another method described in subdivision (j) or by clear and conspicuous notice delivered to the resident online when the resident is connected to the online account from an Internet Protocol address or online location from which the person or business knows the resident customarily accesses the account.

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

(f) A person or business that is required to issue a security breach notification pursuant to this section to more than 500 California residents as a result of a single breach of the security system shall inform the Attorney General of the date of the discovery of the breach, and electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. A single sample copy of a

1 security breach notification shall not be deemed to be within
2 subdivision (f) of Section 6254 of the Government Code.

3 (g) For purposes of this section, “breach of the security of the
4 system” means unauthorized acquisition of computerized data that
5 compromises the security, confidentiality, or integrity of personal
6 information maintained by the person or business. Good faith
7 acquisition of personal information by an employee or agent of
8 the person or business for the purposes of the person or business
9 is not a breach of the security of the system, provided that the
10 personal information is not used or subject to further unauthorized
11 disclosure.

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

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

17 (A) Social security number.

18 (B) Driver’s license number or California identification card
19 number.

20 (C) Account number, credit or debit card number, in
21 combination with any required security code, access code, or
22 password that would permit access to an individual’s financial
23 account.

24 (D) Medical information.

25 (E) Health insurance information.

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

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

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

37 (3) For purposes of this section, “health insurance information”
38 means an individual’s health insurance policy number or subscriber
39 identification number, any unique identifier used by a health insurer

1 to identify the individual, or any information in an individual's
2 application and claims history, including any appeals records.

3 (4) For purposes of this section, "encrypted" means rendered
4 unusable, unreadable, or indecipherable through a security
5 technology or methodology generally accepted in the field of
6 information security.

7 (j) For purposes of this section, "notice" may be provided by
8 one of the following methods:

9 (1) Written notice.

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

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

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

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

24 (C) Notification to major statewide media.

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