

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 ~~Section~~ *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 instead require the disclosure to be made within 30 days, consistent with the legitimate needs of law enforcement.~~

~~The bill would authorize the Attorney General to grant a person or business an additional period of time, not exceeding 30 days, in which to make the disclosure if the Attorney General determines that the person~~

or business needs additional time in order to determine the scope of the security breach, prevent further disclosures, conduct a risk assessment, restore the integrity of the data system, or provide notice to an entity designated to receive reports and information about information security incidents.

~~The bill would also provide that if the data containing personal information was encrypted, as defined, there would be a presumption that a breach of the security of the data does not compromise the security, confidentiality, or integrity of the personal information, and no disclosure would be required. That presumption would be rebuttable in a civil action against a person or business for failure to comply with these provisions by facts demonstrating that in the present instance, the security technologies or methodologies used to encrypt the data have been, or are reasonably likely to have been, compromised.~~

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 to*
2 *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

1 disclosure shall be made in the most expedient time possible and
2 without unreasonable delay, consistent with the legitimate needs
3 of law enforcement, as provided in subdivision (c), or any measures
4 necessary to determine the scope of the breach and restore the
5 reasonable integrity of the data system.

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

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

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

20 (1) The security breach notification shall be written in plain
21 language.

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

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

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

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

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

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

39 (F) The toll-free telephone numbers and addresses of the major
40 credit reporting agencies, if the breach exposed a social security

1 number or a driver's license or California identification card
2 number.

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

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

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

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

21 (5) In the case of a breach of the security of the system involving
22 personal information defined in paragraph (2) of subdivision (g)
23 for login credentials of an email account furnished by the agency,
24 the agency shall not comply with this section by providing the
25 security breach notification to that email address, but may, instead,
26 comply with this section by providing notice by another method
27 described in subdivision (i) or by clear and conspicuous notice
28 delivered to the resident online when the resident is connected to
29 the online account from an Internet Protocol address or online
30 location from which the agency knows the resident customarily
31 accesses the account.

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

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

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

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

14 (A) Social security number.

15 (B) Driver’s license number or California identification card
16 number.

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

21 (D) Medical information.

22 (E) Health insurance information.

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

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

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

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

39 (4) *For purposes of this section, “encrypted” means rendered*
40 *unusable, unreadable, or indecipherable through a security*

1 *technology or methodology generally accepted in the field of*
2 *information security.*

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

5 (1) Written notice.

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

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

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

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

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

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

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

32 **SECTION 1.**

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

34 1798.82. (a) ~~(1)~~—A person or business that conducts business
35 in California, and that owns or licenses computerized data that
36 includes personal information, shall disclose a breach of the
37 security of the system following discovery or notification, pursuant
38 to subdivision (b), of the breach in the security of the data to a
39 resident of California whose unencrypted personal information
40 was, or is reasonably believed to have been, acquired by an

1 unauthorized person. The disclosure shall be made in the most
2 expedient time possible and ~~within 30 days~~, *without unreasonable*
3 *delay*, consistent with the legitimate needs of law enforcement, as
4 provided in subdivision ~~(e)~~. *(c)*, or any measures reasonably
5 necessary to determine the scope of the breach and restore the
6 reasonable integrity of the data system.

7 ~~(2) If the data containing personal information was encrypted,~~
8 ~~there shall be a presumption that a breach of the data does not~~
9 ~~comprise the security, confidentiality, or integrity of the personal~~
10 ~~information contained therein, and no disclosure is required. That~~
11 ~~presumption shall be rebuttable in a civil action pursuant to~~
12 ~~subdivision (b) of Section 1798.84 against a person or business~~
13 ~~for failure to make the required disclosure by facts demonstrating~~
14 ~~that in the present instance the security technologies or~~
15 ~~methodologies used to encrypt the data have been, or are reasonably~~
16 ~~likely to have been, compromised and disclosure is required in~~
17 ~~accordance with paragraph (1).~~

18 ~~(3) If a person or business requires additional time to disclose~~
19 ~~a breach, it shall provide the Attorney General records or other~~
20 ~~evidence demonstrating the need to delay disclosure. If the~~
21 ~~Attorney General determines that the person or business needs~~
22 ~~additional time in order to determine the scope of a security breach,~~
23 ~~prevent further disclosures, conduct a risk assessment, restore the~~
24 ~~integrity of the data system, or provide notice to an entity~~
25 ~~designated to receive reports and information about information~~
26 ~~security incidents, threats, and vulnerabilities, it may grant the~~
27 ~~person or business an additional period of time, not exceeding 30~~
28 ~~days, in which to make the disclosure. The Attorney General shall~~
29 ~~grant additional time to make the disclosure in writing specifying~~
30 ~~the amount of additional time granted.~~

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

37 (c) The notification required by this section may be delayed if
38 a law enforcement agency determines that the notification will
39 impede a criminal investigation. The notification required by this

1 section shall be made promptly after the law enforcement agency
2 determines that it will not compromise the investigation.

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

6 (1) The security breach notification shall be written in plain
7 language.

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

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

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

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

19 (D) Whether notification was delayed pursuant to paragraph (3)
20 of subdivision (a) or as a result of a law enforcement investigation,
21 if that information is possible to determine at the time the notice
22 is provided.

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

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

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

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

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

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

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

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

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

37 (f) A person or business that is required to issue a security breach
38 notification pursuant to this section to more than 500 California
39 residents as a result of a single breach of the security system shall
40 *inform the Attorney General of the date of the discovery of the*

1 *breach*, and electronically submit a single sample copy of that
2 security breach notification, excluding any personally identifiable
3 information, to the Attorney General. A single sample copy of a
4 security breach notification shall not be deemed to be within
5 subdivision (f) of Section 6254 of the Government Code.

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

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

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

20 (A) Social security number.

21 (B) Driver’s license number or California identification card
22 number.

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

27 (D) Medical information.

28 (E) Health insurance information.

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

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

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

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

6 (4) For purposes of this section, “encrypted” means rendered
7 unusable, unreadable, or indecipherable through a security
8 technology or methodology generally accepted in the field of
9 information security.

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

12 (1) Written notice.

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

16 (3) Substitute notice, if the person or business demonstrates that
17 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) Email notice when the person or business has an email
23 address for the subject persons.

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

27 (C) Notification to major statewide media.

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

O