

AMENDED IN SENATE SEPTEMBER 1, 2015

AMENDED IN ASSEMBLY MAY 28, 2015

AMENDED IN ASSEMBLY MAY 13, 2015

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 to an unauthorized person through a security technology or methodology generally accepted in the field of information technology.

*This bill would incorporate additional changes to Section 1798.29 of the Civil Code proposed by SB 34 and SB 570 that would become operative if this bill and one or both of those bills are enacted and this bill is enacted last.*

*This bill also would incorporate additional changes to Section 1798.82 of the Civil Code proposed by SB 34 and SB 570 that would become operative if this bill and one or both of those bills are enacted and this bill is enacted last.*

Vote: majority. Appropriation: no. Fiscal committee: no.  
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

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.

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

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

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

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

20 (D) Whether the notification was delayed as a result of a law  
21 enforcement investigation, if that information is possible to  
22 determine at the time the notice 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 (3) At the discretion of the agency, the security breach  
31 notification may also include any of the following:

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

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

36 (4) In the case of a breach of the security of the system involving  
37 personal information defined in paragraph (2) of subdivision (g)  
38 for an online account, and no other personal information defined  
39 in paragraph (1) of subdivision (g), the agency may comply with  
40 this section by providing the security breach notification in

1 electronic or other form that directs the person whose personal  
2 information has been breached to promptly change his or her  
3 password and security question or answer, as applicable, or to take  
4 other steps appropriate to protect the online account with the  
5 agency and all other online accounts for which the person uses the  
6 same user name or email address and password or security question  
7 or answer.

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

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

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

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

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

40 (A) Social security number.

1 (B) Driver’s license number or California identification card  
2 number.

3 (C) Account number, credit or debit card number, in  
4 combination with any required security code, access code, or  
5 password that would permit access to an individual’s financial  
6 account.

7 (D) Medical information.

8 (E) Health insurance information.

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

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

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

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

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

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

31 (1) Written notice.

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

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

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

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

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

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

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

18 *SEC. 1.1. Section 1798.29 of the Civil Code is amended to*  
19 *read:*

20 1798.29. (a) Any agency that owns or licenses computerized  
21 data that includes personal information shall disclose any breach  
22 of the security of the system following discovery or notification  
23 of the breach in the security of the data to any resident of California  
24 whose unencrypted personal information was, or is reasonably  
25 believed to have been, acquired by an unauthorized person. The  
26 disclosure shall be made in the most expedient time possible and  
27 without unreasonable delay, consistent with the legitimate needs  
28 of law enforcement, as provided in subdivision (c), or any measures  
29 necessary to determine the scope of the breach and restore the  
30 reasonable integrity of the data system.

31 (b) Any agency that maintains computerized data that includes  
32 personal information that the agency does not own shall notify the  
33 owner or licensee of the information of any breach of the security  
34 of the data immediately following discovery, if the personal  
35 information was, or is reasonably believed to have been, acquired  
36 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 after the law enforcement agency determines  
2 that it will not compromise the investigation.

3 (d) Any agency that is required to issue a security breach  
4 notification pursuant to this section shall meet all of the following  
5 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 agency  
11 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 the notification was delayed as a result of a law  
20 enforcement investigation, if that information is possible to  
21 determine at the time the notice is provided.

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

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

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

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

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

35 (4) In the case of a breach of the security of the system involving  
36 personal information defined in paragraph (2) of subdivision (g)  
37 for an online account, and no other personal information defined  
38 in paragraph (1) of subdivision (g), the agency may comply with  
39 this section by providing the security breach notification in  
40 electronic or other form that directs the person whose personal

1 information has been breached to promptly change his or her  
2 password and security question or answer, as applicable, or to take  
3 other steps appropriate to protect the online account with the  
4 agency and all other online accounts for which the person uses the  
5 same user name or email address and password or security question  
6 or answer.

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

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

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

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

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

39 (A) Social security number.

1 (B) Driver’s license number or California identification card  
2 number.

3 (C) Account number, credit or debit card number, in  
4 combination with any required security code, access code, or  
5 password that would permit access to an individual’s financial  
6 account.

7 (D) Medical information.

8 (E) Health insurance information.

9 (F) *Information or data collected through the use or operation*  
10 *of an automated license plate recognition system, as defined in*  
11 *Section 1798.90.5.*

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

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

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

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

28 (4) *For purposes of this section, “encrypted” means rendered*  
29 *unusable, unreadable, or indecipherable to an unauthorized person*  
30 *through a security technology or methodology generally accepted*  
31 *in the field of information security.*

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

34 (1) Written notice.

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

38 (3) Substitute notice, if the agency demonstrates that the cost  
39 of providing notice would exceed two hundred fifty thousand  
40 dollars (\$250,000), or that the affected class of subject persons to

1 be notified exceeds 500,000, or the agency does not have sufficient  
2 contact information. Substitute notice shall consist of all of the  
3 following:

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

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

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

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 *SEC. 1.2. Section 1798.29 of the Civil Code is amended to*  
22 *read:*

23 1798.29. (a) Any agency that owns or licenses computerized  
24 data that includes personal information shall disclose any breach  
25 of the security of the system following discovery or notification  
26 of the breach in the security of the data to any resident of California  
27 whose unencrypted personal information was, or is reasonably  
28 believed to have been, acquired by an unauthorized person. The  
29 disclosure shall be made in the most expedient time possible and  
30 without unreasonable delay, consistent with the legitimate needs  
31 of law enforcement, as provided in subdivision (c), or any measures  
32 necessary to determine the scope of the breach and restore the  
33 reasonable integrity of the data system.

34 (b) Any agency that maintains computerized data that includes  
35 personal information that the agency does not own shall notify the  
36 owner or licensee of the information of any breach of the security  
37 of the data immediately following discovery, if the personal  
38 information was, or is reasonably believed to have been, acquired  
39 by an unauthorized person.

1 (c) The notification required by this section may be delayed if  
 2 a law enforcement agency determines that the notification will  
 3 impede a criminal investigation. The notification required by this  
 4 section shall be made after the law enforcement agency determines  
 5 that it will not compromise the investigation.

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

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

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

18 (B) *The title and headings in the notice shall be clearly and*  
 19 *conspicuously displayed.*

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

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

[NAME OF INSTITUTION / LOGO]		Date: [insert date]
<b>NOTICE OF DATA BREACH</b>		
<i>What Happened?</i>		

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

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

*(E) For an electronic notice described in paragraph (2) of subdivision (i), use of the headings described in this paragraph with the information described in paragraph (2), written in plain*

1 *language, shall be deemed to be in compliance with this*  
2 *subdivision.*

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

5 (A) The name and contact information of the reporting agency  
6 *subject to this section.*

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

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

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

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

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

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

26 (A) Information about what the agency has done to protect  
27 *individuals whose information has been breached.*

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

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

1 same user name or email address and password or security question  
2 or answer.

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

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

22 (f) 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 agency. Good faith acquisition of  
26 personal information by an employee or agent of the agency for  
27 the purposes of the agency is not a breach of the security of the  
28 system, provided that the personal information is not used or  
29 subject to further unauthorized disclosure.

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

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

35 (A) Social security number.

36 (B) Driver’s license number or California identification card  
37 number.

38 (C) Account number, credit or debit card number, in  
39 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 (h) (1) For purposes of this section, “personal information”  
9 does not include publicly available information that is lawfully  
10 made 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 (4) *For purposes of this section, “encrypted” means rendered*  
22 *unusable, unreadable, or indecipherable to an unauthorized person*  
23 *through a security technology or methodology generally accepted*  
24 *in the field of information security.*

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

27 (1) Written notice.

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

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

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

39 (B) ~~Conspicuous posting~~ *posting, for a minimum of 30 days*, of  
40 the notice on the agency’s Internet Web site page, if the agency

1 maintains one. *For purposes of this subparagraph, conspicuous*  
2 *posting on the agency's Internet Web site means providing a link*  
3 *to the notice on the home page or first significant page after*  
4 *entering the Internet Web site that is in larger type than the*  
5 *surrounding text, or in contrasting type, font, or color to the*  
6 *surrounding text of the same size, or set off from the surrounding*  
7 *text of the same size by symbols or other marks that call attention*  
8 *to the link.*

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

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

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

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

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

5 *SEC. 1.3. Section 1798.29 of the Civil Code is amended to*  
6 *read:*

7 1798.29. (a) Any agency that owns or licenses computerized  
8 data that includes personal information shall disclose any breach  
9 of the security of the system following discovery or notification  
10 of the 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 agency that maintains computerized data that includes  
19 personal information that the agency does not own shall notify the  
20 owner or licensee of the information of any breach of the security  
21 of the data immediately following discovery, if the personal  
22 information was, or is reasonably believed to have been, acquired  
23 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 agency that is required to issue a security breach  
30 notification pursuant to this section shall meet all of the following  
31 requirements:

32 (1) The security breach notification shall be written in plain  
33 ~~language.~~ *language, shall be titled “Notice of Data Breach,” and*  
34 *shall present the information described in paragraph (2) under*  
35 *the following headings: “What Happened,” “What Information*  
36 *Was Involved,” “What We Are Doing,” “What You Can Do,” and*  
37 *“For More Information.” Additional information may be provided*  
38 *as a supplement to the notice.*

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

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

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

5 (D) For a written notice described in paragraph (1) of  
6 subdivision (i), use of the model security breach notification form  
7 prescribed below or use of the headings described in this  
8 paragraph with the information described in paragraph (2), written  
9 in plain language, shall be deemed to be in compliance with this  
10 subdivision.

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

<i>[NAME OF INSTITUTION / LOGO]</i>		<i>Date: [insert date]</i>
<i>NOTICE OF DATA BREACH</i>		
<i>What Happened?</i>		
<i>What Information Was Involved?</i>		
<i>What We Are Doing.</i>		
<i>What You Can Do.</i>		

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

<i>Other Important Information.</i> <i>[insert other important information]</i>	
<i>For More Information.</i>	<i>Call [telephone number] or go to [Internet Web site]</i>

(E) For an electronic notice described in paragraph (2) of subdivision (i), 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 agency 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 the 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.

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

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

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

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

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

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

26 ~~(5) 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 login credentials of an email account furnished by the agency,  
29 the agency shall not comply with this section by providing the  
30 security breach notification to that email address, but may, instead,  
31 comply with this section by providing notice by another method  
32 described in subdivision (i) or by clear and conspicuous notice  
33 delivered to the resident online when the resident is connected to  
34 the online account from an Internet Protocol address or online  
35 location from which the agency knows the resident customarily  
36 accesses the account.~~

37 (e) Any agency 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 electronically submit a single sample copy of that security breach

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

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

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

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

18 (A) Social security number.

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

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

25 (D) Medical information.

26 (E) Health insurance information.

27 (F) *Information or data collected through the use or operation*  
28 *of an automated license plate recognition system, as defined in*  
29 *Section 1798.90.5.*

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

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

37 (2) For purposes of this section, “medical information” means  
38 any information regarding an individual’s medical history, mental  
39 or physical condition, or medical treatment or diagnosis by a health  
40 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 to an unauthorized person*  
8 *through a security technology or methodology generally accepted*  
9 *in the field of information security.*

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

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

24 (B) ~~Conspicuous posting~~ *posting, for a minimum of 30 days, of*  
25 *the notice on the agency’s Internet Web site page, if the agency*  
26 *maintains one. For purposes of this subparagraph, conspicuous*  
27 *posting on the agency’s Internet Web site means providing a link*  
28 *to the notice on the home page or first significant page after*  
29 *entering the Internet Web site that is in larger type than the*  
30 *surrounding text, or in contrasting type, font, or color to the*  
31 *surrounding text of the same size, or set off from the surrounding*  
32 *text of the same size by symbols or other marks that call attention*  
33 *to the link.*

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

36 (4) *In the case of a breach of the security of the system involving*  
37 *personal information defined in paragraph (2) of subdivision (g)*  
38 *for an online account, and no other personal information defined*  
39 *in paragraph (1) of subdivision (g), the agency may comply with*  
40 *this section by providing the security breach notification in*

1 *electronic or other form that directs the person whose personal*  
2 *information has been breached to promptly change his or her*  
3 *password and security question or answer, as applicable, or to*  
4 *take other steps appropriate to protect the online account with the*  
5 *agency and all other online accounts for which the person uses*  
6 *the same user name or email address and password or security*  
7 *question or answer.*

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

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

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

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

31 1798.82. (a) A person or business that conducts business in  
32 California, and that owns or licenses computerized data that  
33 includes personal information, shall disclose a breach of the  
34 security of the system following discovery or notification of the  
35 breach in the security of the data to a resident of California whose  
36 unencrypted personal information was, or is reasonably believed  
37 to have been, acquired by an unauthorized person. The disclosure  
38 shall be made in the most expedient time possible and without  
39 unreasonable delay, consistent with the legitimate needs of law  
40 enforcement, as provided in subdivision (c), or any measures

1 necessary to determine the scope of the breach and restore the  
2 reasonable integrity of the data system.

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

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

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

17 (1) The security breach notification shall be written in plain  
18 language.

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

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

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

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

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

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

36 (F) The toll-free telephone numbers and addresses of the major  
37 credit reporting agencies if the breach exposed a social security  
38 number or a driver's license or California identification card  
39 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 (4) In the case of a breach of the security of the system involving  
16 personal information defined in paragraph (2) of subdivision (h)  
17 for an online account, and no other personal information defined  
18 in paragraph (1) of subdivision (h), the person or business may  
19 comply with this section by providing the security breach  
20 notification in electronic or other form that directs the person whose  
21 personal information has been breached promptly to change his  
22 or her password and security question or answer, as applicable, or  
23 to take other steps appropriate to protect the online account with  
24 the person or business and all other online accounts for which the  
25 person whose personal information has been breached uses the  
26 same user name or email address and password or security question  
27 or answer.

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

39 (e) A covered entity under the federal Health Insurance  
40 Portability and Accountability Act of 1996 (42 U.S.C. Sec. 1320d

1 et seq.) will be deemed to have complied with the notice  
2 requirements in subdivision (d) if it has complied completely with  
3 Section 13402(f) of the federal Health Information Technology  
4 for Economic and Clinical Health Act (Public Law 111-5).  
5 However, nothing in this subdivision shall be construed to exempt  
6 a covered entity from any other provision of this section.

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

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

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

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

29 (A) Social security number.

30 (B) Driver’s license number or California identification card  
31 number.

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

36 (D) Medical information.

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

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

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

20 (1) Written notice.

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

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

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

32 (B) Conspicuous posting of the notice on the Internet Web site  
33 page of the person or business, if the person or business maintains  
34 one.

35 (C) Notification to major statewide media.

36 (k) Notwithstanding subdivision (j), a person or business that  
37 maintains its own notification procedures as part of an information  
38 security policy for the treatment of personal information and is  
39 otherwise consistent with the timing requirements of this part, shall  
40 be deemed to be in compliance with the notification requirements

1 of this section if the person or business notifies subject persons in  
2 accordance with its policies in the event of a breach of security of  
3 the system.

4 *SEC. 2.1. Section 1798.82 of the Civil Code is amended to*  
5 *read:*

6 1798.82. (a) A person or business that conducts business in  
7 California, and that owns or licenses computerized data that  
8 includes personal information, shall disclose a breach of the  
9 security of the system following discovery or notification of the  
10 breach in the security of the data to a resident of California whose  
11 unencrypted personal information was, or is reasonably believed  
12 to have been, acquired by an unauthorized person. The disclosure  
13 shall be made in the most expedient time possible and without  
14 unreasonable delay, consistent with the legitimate needs of law  
15 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) A person or business that maintains computerized data that  
19 includes personal information that the person or business does not  
20 own shall notify the owner or licensee of the information of the  
21 breach of the security of the data immediately following discovery,  
22 if the personal information was, or is reasonably believed to have  
23 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 promptly after the law enforcement agency  
28 determines that it will not compromise the investigation.

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

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

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

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

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

1 same user name or email address and password or security question  
2 or answer.

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

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

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

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

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

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

4 (A) Social security number.

5 (B) Driver’s license number or California identification card  
6 number.

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

11 (D) Medical information.

12 (E) Health insurance information.

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

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

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

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

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

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

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

38 (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 of the notice on the Internet Web site  
13 page of the person or business, if the person or business maintains  
14 one.

15 (C) Notification to major statewide media.

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

24 *SEC. 2.2. Section 1798.82 of the Civil Code is amended to*  
25 *read:*

26 1798.82. (a) A person or business that conducts business in  
27 California, and that owns or licenses computerized data that  
28 includes personal information, shall disclose a breach of the  
29 security of the system following discovery or notification of the  
30 breach in the security of the data to a resident of California whose  
31 unencrypted personal information was, or is reasonably believed  
32 to have been, acquired by an unauthorized person. The disclosure  
33 shall be made in the most expedient time possible and without  
34 unreasonable delay, consistent with the legitimate needs of law  
35 enforcement, as provided in subdivision (c), or any measures  
36 necessary to determine the scope of the breach and restore the  
37 reasonable integrity of the data system.

38 (b) A person or business that maintains computerized data that  
39 includes personal information that the person or business does not  
40 own shall notify the owner or licensee of the information of the

1 breach of the security of the data immediately following discovery,  
2 if the personal information was, or is reasonably believed to have  
3 been, acquired by an unauthorized person.

4 (c) The notification required by this section may be delayed if  
5 a law enforcement agency determines that the notification will  
6 impede a criminal investigation. The notification required by this  
7 section shall be made promptly after the law enforcement agency  
8 determines that it will not compromise the investigation.

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

12 (1) The security breach notification shall be written in plain  
13 ~~language.~~ *language, shall be titled "Notice of Data Breach," and*  
14 *shall present the information described in paragraph (2) under*  
15 *the following headings: "What Happened," "What Information*  
16 *Was Involved," "What We Are Doing," "What You Can Do," and*  
17 *"For More Information." Additional information may be provided*  
18 *as a supplement to the notice.*

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

21 (B) *The title and headings in the notice shall be clearly and*  
22 *conspicuously displayed.*

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

25 (D) *For a written notice described in paragraph (1) of*  
26 *subdivision (j), use of the model security breach notification form*  
27 *prescribed below or use of the headings described in this*  
28 *paragraph with the information described in paragraph (2), written*  
29 *in plain language, shall be deemed to be in compliance with this*  
30 *subdivision.*

31  
32  
33  
34  
35  
36  
37  
38  
39

<i>[NAME OF INSTITUTION / LOGO]</i>		<i>Date: [insert date]</i>
<i>NOTICE OF DATA BREACH</i>		

1 2 3 4	<i>What Happened?</i>	
5 6 7 8 9 10	<i>What Information Was Involved?</i>	
11 12 13 14 15 16	<i>What We Are Doing.</i>	
17 18 19 20 21 22 23	<i>What You Can Do.</i>	
24 25 26 27 28 29 30 31 32	<i>Other Important Information.</i> <i>[insert other important information]</i>	
33 34 35 36 37 38	<i>For More Information.</i>	<i>Call [telephone number] or go to [Internet Web site]</i>

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

6 (2) The security breach notification described in paragraph (1)  
7 shall include, at a minimum, 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~~, *months*  
31 along with all information necessary to take advantage of the offer  
32 to any person whose information was or may have been breached  
33 if the breach exposed or may have exposed personal information  
34 defined in subparagraphs (A) and (B) of paragraph (1) of  
35 subdivision (h).

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

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

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

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

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

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

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

1 notification shall not be deemed to be within subdivision (f) of  
2 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 to an unauthorized person*  
 5 *through a security technology or methodology generally accepted*  
 6 *in the field of 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~~ *posting, for a minimum of 30 days, of*  
 22 *the notice on the Internet Web site page of the person or business,*  
 23 *if the person or business maintains one. For purposes of this*  
 24 *subparagraph, conspicuous posting on the person’s or business’s*  
 25 *Internet Web site means providing a link to the notice on the home*  
 26 *page or first significant page after entering the Internet Web site*  
 27 *that is in larger type than the surrounding text, or in contrasting*  
 28 *type, font, or color to the surrounding text of the same size, or set*  
 29 *off from the surrounding text of the same size by symbols or other*  
 30 *marks that call attention to the link.*

31 (C) Notification to major statewide media.

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

1 with the person or business and all other online accounts for which  
2 the person whose personal information has been breached uses  
3 the same user name or email address and password or security  
4 question 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 (h)  
7 for login credentials of an email account furnished by the person  
8 or business, the person or business shall not comply with this  
9 section by providing the security breach notification to that email  
10 address, but may, instead, comply with this section by providing  
11 notice by another method described in this subdivision or by clear  
12 and conspicuous notice delivered to the resident online when the  
13 resident is connected to the online account from an Internet  
14 Protocol address or online location from which the person or  
15 business knows the resident customarily accesses the account.

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

24 *SEC. 2.3. Section 1798.82 of the Civil Code is amended to*  
25 *read:*

26 1798.82. (a) A person or business that conducts business in  
27 California, and that owns or licenses computerized data that  
28 includes personal information, shall disclose a breach of the  
29 security of the system following discovery or notification of the  
30 breach in the security of the data to a resident of California whose  
31 unencrypted personal information was, or is reasonably believed  
32 to have been, acquired by an unauthorized person. The disclosure  
33 shall be made in the most expedient time possible and without  
34 unreasonable delay, consistent with the legitimate needs of law  
35 enforcement, as provided in subdivision (c), or any measures  
36 necessary to determine the scope of the breach and restore the  
37 reasonable integrity of the data system.

38 (b) A person or business that maintains computerized data that  
39 includes personal information that the person or business does not  
40 own shall notify the owner or licensee of the information of the

1 breach of the security of the data immediately following discovery,  
2 if the personal information was, or is reasonably believed to have  
3 been, acquired by an unauthorized person.

4 (c) The notification required by this section may be delayed if  
5 a law enforcement agency determines that the notification will  
6 impede a criminal investigation. The notification required by this  
7 section shall be made promptly after the law enforcement agency  
8 determines that it will not compromise the investigation.

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

12 (1) The security breach notification shall be written in plain  
13 ~~language.~~ *language, shall be titled "Notice of Data Breach," and*  
14 *shall present the information described in paragraph (2) under*  
15 *the following headings: "What Happened," "What Information*  
16 *Was Involved," "What We Are Doing," "What You Can Do," and*  
17 *"For More Information." Additional information may be provided*  
18 *as a supplement to the notice.*

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

21 (B) *The title and headings in the notice shall be clearly and*  
22 *conspicuously displayed.*

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

25 (D) *For a written notice described in paragraph (1) of*  
26 *subdivision (j), use of the model security breach notification form*  
27 *prescribed below or use of the headings described in this*  
28 *paragraph with the information described in paragraph (2), written*  
29 *in plain language, shall be deemed to be in compliance with this*  
30 *subdivision.*

31  
32  
33  
34  
35  
36  
37  
38  
39

<i>[NAME OF INSTITUTION / LOGO]</i>		<i>Date: [insert date]</i>
<i>NOTICE OF DATA BREACH</i>		

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

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

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

6 (2) The security breach notification described in paragraph (1)  
7 shall include, at a minimum, 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~~, *months*  
31 along with all information necessary to take advantage of the offer  
32 to any person whose information was or may have been breached  
33 if the breach exposed or may have exposed personal information  
34 defined in subparagraphs (A) and (B) of paragraph (1) of  
35 subdivision (h).

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

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

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

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

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

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

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

1 notification shall not be deemed to be within subdivision (f) of  
2 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 (F) *Information or data collected through the use or operation*  
27 *of an automated license plate recognition system, as defined in*  
28 *Section 1798.90.5.*

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 to an unauthorized person*  
8 *through a security technology or methodology generally accepted*  
9 *in the field of 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~~ *posting, for a minimum of 30 days, of*  
25 *the notice on the Internet Web site page of the person or business,*  
26 *if the person or business maintains one. For purposes of this*  
27 *subparagraph, conspicuous posting on the person’s or business’s*  
28 *Internet Web site means providing a link to the notice on the home*  
29 *page or first significant page after entering the Internet Web site*  
30 *that is in larger type than the surrounding text, or in contrasting*  
31 *type, font, or color to the surrounding text of the same size, or set*  
32 *off from the surrounding text of the same size by symbols or other*  
33 *marks that call attention to the link.*

34 (C) Notification to major statewide media.

35 (4) *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 an online account, and no other personal information defined*  
38 *in paragraph (1) of subdivision (h), the person or business may*  
39 *comply with this section by providing the security breach*  
40 *notification in electronic or other form that directs the person*

1 *whose personal information has been breached promptly to change*  
2 *his or her password and security question or answer, as applicable,*  
3 *or to take other steps appropriate to protect the online account*  
4 *with the person or business and all other online accounts for which*  
5 *the person whose personal information has been breached uses*  
6 *the same user name or email address and password or security*  
7 *question or answer.*

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

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

27 *SEC. 3. (a) Section 1.1 of this bill incorporates amendments*  
28 *to Section 1798.29 of the Civil Code proposed by both this bill*  
29 *and Senate Bill 34. It shall only become operative if (1) both bills*  
30 *are enacted and become effective on or before January 1, 2016,*  
31 *(2) each bill amends Section 1798.29 of the Civil Code, (3) Senate*  
32 *Bill 570 is not enacted or as enacted does not amend that section,*  
33 *and (4) this bill is enacted after Senate Bill 34, in which case*  
34 *Sections 1, 1.2, and 1.3 of this bill shall not become operative.*

35 *(b) Section 1.2 of this bill incorporates amendments to Section*  
36 *1798.29 of the Civil Code proposed by both this bill and Senate*  
37 *Bill 570. It shall only become operative if (1) both bills are enacted*  
38 *and become effective on or before January 1, 2016, (2) each bill*  
39 *amends Section 1798.29 of the Civil Code, (3) Senate Bill 34 is*  
40 *not enacted or as enacted does not amend that section, and (4)*

1 *this bill is enacted after Senate Bill 570, in which case Sections 1,*  
2 *1.1, and 1.3 of this bill shall not become operative.*

3 *(c) Section 1.3 of this bill incorporates amendments to Section*  
4 *1798.29 of the Civil Code proposed by this bill, Senate Bill 34,*  
5 *and Senate Bill 570. It shall only become operative if (1) all three*  
6 *bills are enacted and become effective on or before January 1,*  
7 *2016, (2) all three bills amend Section 1798.29 of the Civil Code,*  
8 *and (3) this bill is enacted after Senate Bill 34 and Senate Bill 570,*  
9 *in which case Sections 1, 1.1, and 1.2 of this bill shall not become*  
10 *operative.*

11 *SEC. 4. (a) Section 2.1 of this bill incorporates amendments*  
12 *to Section 1798.82 of the Civil Code proposed by both this bill*  
13 *and Senate Bill 34. It shall only become operative if (1) both bills*  
14 *are enacted and become effective on or before January 1, 2016,*  
15 *(2) each bill amends Section 1798.82 of the Civil Code, (3) Senate*  
16 *Bill 570 is not enacted or as enacted does not amend that section,*  
17 *and (4) this bill is enacted after Senate Bill 34, in which case*  
18 *Sections 2, 2.2, and 2.3 of this bill shall not become operative.*

19 *(b) Section 2.2 of this bill incorporates amendments to Section*  
20 *1798.82 of the Civil Code proposed by both this bill and Senate*  
21 *Bill 570. It shall only become operative if (1) both bills are enacted*  
22 *and become effective on or before January 1, 2016, (2) each bill*  
23 *amends Section 1798.82 of the Civil Code, (3) Senate Bill 34 is*  
24 *not enacted or as enacted does not amend that section, and (4)*  
25 *this bill is enacted after Senate Bill 570, in which case Sections 2,*  
26 *2.1, and 2.3 of this bill shall not become operative.*

27 *(c) Section 2.3 of this bill incorporates amendments to Section*  
28 *1798.82 of the Civil Code proposed by this bill, Senate Bill 34,*  
29 *and Senate Bill 570. It shall only become operative if (1) all three*  
30 *bills are enacted and become effective on or before January 1,*  
31 *2016, (2) all three bills amend Section 1798.82 of the Civil Code,*  
32 *and (3) this bill is enacted after Senate Bill 34 and Senate Bill 570,*  
33 *in which case Sections 2, 2.1, and 2.2 of this bill shall not become*  
34 *operative.*

O