

AMENDED IN ASSEMBLY SEPTEMBER 1, 2015

AMENDED IN ASSEMBLY JULY 13, 2015

AMENDED IN ASSEMBLY JULY 2, 2015

AMENDED IN SENATE APRIL 22, 2015

**SENATE BILL**

**No. 34**

---

---

**Introduced by Senator Hill**  
(Coauthor: Assembly Member Gatto)

December 1, 2014

---

---

An act to amend Sections 1798.29 and 1798.82 of, and to add Title 1.81.23 (commencing with Section 1798.90.5) to Part 4 of Division 3 of, the Civil Code, relating to personal information.

LEGISLATIVE COUNSEL'S DIGEST

SB 34, as amended, Hill. Automated license plate recognition systems: use of data.

(1) Existing law authorizes the Department of the California Highway Patrol to retain license plate data captured by license plate recognition (LPR) technology, also referred to as an automated license plate recognition (ALPR) system, for not more than 60 days unless the data is being used as evidence or for the investigation of felonies. Existing law prohibits the department from selling the data or from making the data available to an agency that is not a law enforcement agency or an individual that is not a law enforcement officer.

Existing law authorizes the department to use LPR data for the purpose of locating vehicles or persons reasonably suspected of being involved in the commission of a public offense, and requires the department to monitor the internal use of the data to prevent unauthorized use and to

submit to the Legislature, as a part of the annual automobile theft report, information on the department's LPR practices and usage.

This bill would impose specified requirements on an "ALPR operator" as defined, including, among others, maintaining reasonable security procedures and practices to protect ALPR information and implementing a usage and privacy policy with respect to that information, as specified. The bill would impose similar requirements on an "ALPR end-user," as defined.

The bill would require an ALPR operator that accesses or provides access to ALPR information to maintain a specified record of that access and require that ALPR information only be used for authorized purposes.

The bill would, in addition to any other sanctions, penalties, or remedies provided by law, authorize an individual who has been harmed by a violation of these provisions to bring a civil action in any court of competent jurisdiction against a person who knowingly caused the harm.

The bill would require a public agency, as defined, that operates or intends to operate an ALPR system to provide an opportunity for public comment at a regularly scheduled public meeting of the governing body of the public agency before implementing the program. The bill would also prohibit a public agency from selling, sharing, or transferring ALPR information, except to another public agency, as specified.

(2) Existing law requires any agency, and any person or business conducting business in California, that owns or licenses computerized data that includes personal information, as defined, to disclose in specified ways, any breach of the security of the system or data, as defined, following discovery or notification of the security breach, to any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Existing law defines "personal information" for these purposes to include an individual's first name and last name, or first initial and last name, in combination with one or more designated data elements relating to, among other things, social security numbers, driver's license numbers, financial accounts, and medical information.

This bill would include information or data collected through the use or operation of an automated license plate recognition system, when that information is not encrypted and is used in combination with an individual's name, in the definition of "personal information" discussed above.

*This bill would incorporate additional changes to Section 1798.29 of the Civil Code proposed by SB 570 and AB 964 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 570 and AB 964 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: yes.  
State-mandated local program: no.

*The people of the State of California do enact as follows:*

1 SECTION 1. Section 1798.29 of the Civil Code is amended  
2 to read:  
3 1798.29. (a) Any agency that owns or licenses computerized  
4 data that includes personal information shall disclose any breach  
5 of the security of the system following discovery or notification  
6 of the breach in the security of the data to any resident of California  
7 whose unencrypted personal information was, or is reasonably  
8 believed to have been, acquired by an unauthorized person. The  
9 disclosure shall be made in the most expedient time possible and  
10 without unreasonable delay, consistent with the legitimate needs  
11 of law enforcement, as provided in subdivision (c), or any measures  
12 necessary to determine the scope of the breach and restore the  
13 reasonable integrity of the data system.  
14 (b) Any agency that maintains computerized data that includes  
15 personal information that the agency does not own shall notify the  
16 owner or licensee of the information of any breach of the security  
17 of the data immediately following discovery, if the personal  
18 information was, or is reasonably believed to have been, acquired  
19 by an unauthorized person.  
20 (c) The notification required by this section may be delayed if  
21 a law enforcement agency determines that the notification will  
22 impede a criminal investigation. The notification required by this  
23 section shall be made after the law enforcement agency determines  
24 that it will not compromise the investigation.  
25 (d) Any agency that is required to issue a security breach  
26 notification pursuant to this section shall meet all of the following  
27 requirements:

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

3 (2) The security breach notification shall include, at a minimum,  
4 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 (F) Information or data collected through the use or operation  
6 of an automated license plate recognition system, as defined in  
7 Section 1798.90.5.

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

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

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

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

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

26 (1) Written notice.

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

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

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

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

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

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

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

14 *SEC. 1.1. Section 1798.29 of the Civil Code is amended to*  
15 *read:*

16 1798.29. (a) Any agency that owns or licenses computerized  
17 data that includes personal information shall disclose any breach  
18 of the security of the system following discovery or notification  
19 of the breach in the security of the data to any resident of California  
20 whose unencrypted personal information was, or is reasonably  
21 believed to have been, acquired by an unauthorized person. The  
22 disclosure shall be made in the most expedient time possible and  
23 without unreasonable delay, consistent with the legitimate needs  
24 of law enforcement, as provided in subdivision (c), or any measures  
25 necessary to determine the scope of the breach and restore the  
26 reasonable integrity of the data system.

27 (b) Any agency that maintains computerized data that includes  
28 personal information that the agency does not own shall notify the  
29 owner or licensee of the information of any breach of the security  
30 of the data immediately following discovery, if the personal  
31 information was, or is reasonably believed to have been, acquired  
32 by an unauthorized person.

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

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

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

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

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

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

14 (D) For a written notice described in paragraph (1) of  
 15 subdivision (i), use of the model security breach notification form  
 16 prescribed below or use of the headings described in this  
 17 paragraph with the information described in paragraph (2), written  
 18 in plain language, shall be deemed to be in compliance with this  
 19 subdivision.

20

21

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

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

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 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 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.*

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

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

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

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

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

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

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

34 ~~(5) In the case of a breach of the security of the system involving  
35 personal information defined in paragraph (2) of subdivision (g)  
36 for login credentials of an email account furnished by the agency,  
37 the agency shall not comply with this section by providing the  
38 security breach notification to that email address, but may, instead,  
39 comply with this section by providing notice by another method  
40 described in subdivision (i) or by clear and conspicuous notice~~

1 ~~delivered to the resident online when the resident is connected to~~  
2 ~~the online account from an Internet Protocol address or online~~  
3 ~~location from which the agency knows the resident customarily~~  
4 ~~accesses the account.~~

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

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

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

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

26 (A) Social security number.

27 (B) Driver’s license number or California identification card  
28 number.

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

33 (D) Medical information.

34 (E) Health insurance information.

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

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

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

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

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

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

16 (1) Written notice.

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

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

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

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

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

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

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

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

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

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

37     1798.29. (a) Any agency that owns or licenses computerized  
38 data that includes personal information shall disclose any breach  
39 of the security of the system following discovery or notification  
40 of the breach in the security of the data to any resident of California

1 whose unencrypted personal information was, or is reasonably  
2 believed to have been, acquired by an unauthorized person. The  
3 disclosure shall be made in the most expedient time possible and  
4 without unreasonable delay, consistent with the legitimate needs  
5 of law enforcement, as provided in subdivision (c), or any measures  
6 necessary to determine the scope of the breach and restore the  
7 reasonable integrity of the data system.

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

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

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

22 (1) The security breach notification shall be written in plain  
23 language.

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

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

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

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

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

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

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

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

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

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

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 take  
19 other steps appropriate to protect the online account with the  
20 agency and all other online accounts for which the person uses the  
21 same user name or email address and password or security question  
22 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 subdivision (i) 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 (e) Any agency that is required to issue a security breach  
35 notification pursuant to this section to more than 500 California  
36 residents as a result of a single breach of the security system shall  
37 electronically submit a single sample copy of that security breach  
38 notification, excluding any personally identifiable information, to  
39 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 (f) 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 agency. Good faith acquisition of  
7 personal information by an employee or agent of the agency for  
8 the purposes of the agency is not a breach of the security of the  
9 system, provided that the personal information is not used or  
10 subject to further unauthorized disclosure.

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

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

16 (A) Social security number.

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

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

23 (D) Medical information.

24 (E) Health insurance information.

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

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

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

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

39 (3) For purposes of this section, “health insurance information”  
40 means an individual’s health insurance policy number or subscriber

1 identification number, any unique identifier used by a health insurer  
2 to identify the individual, or any information in an individual's  
3 application and claims history, including any appeals records.

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

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

10 (1) Written notice.

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

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

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

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

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

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

33 (k) Notwithstanding the exception specified in paragraph (4) of  
34 subdivision (b) of Section 1798.3, for purposes of this section,  
35 "agency" includes a local agency, as defined in subdivision (a) of  
36 Section 6252 of the Government Code.

37 *SEC. 1.3. Section 1798.29 of the Civil Code is amended to*  
38 *read:*

39 1798.29. (a) Any agency that owns or licenses computerized  
40 data that includes personal information shall disclose any breach

1 of the security of the system following discovery or notification  
2 of the breach in the security of the data to any resident of California  
3 whose unencrypted personal information was, or is reasonably  
4 believed to have been, acquired by an unauthorized person. The  
5 disclosure shall be made in the most expedient time possible and  
6 without unreasonable delay, consistent with the legitimate needs  
7 of law enforcement, as provided in subdivision (c), or any measures  
8 necessary to determine the scope of the breach and restore the  
9 reasonable integrity of the data system.

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

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

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

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

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

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

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

37 (D) *For a written notice described in paragraph (1) of*  
38 *subdivision (i), use of the model security breach notification form*  
39 *prescribed below or use of the headings described in this*  
40 *paragraph with the information described in paragraph (2), written*

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

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  
39

<i>[NAME OF INSTITUTION / LOGO]</i> <span style="float: right;"><i>Date: [insert date]</i></span>	
<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>	
<i>Other Important Information.</i> <i>[insert other important information]</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>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.

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

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

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

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

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

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

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

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

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

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

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

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

9 (A) Social security number.

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

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

16 (D) Medical information.

17 (E) Health insurance information.

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

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

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

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

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

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

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

3 (1) Written notice.

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

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

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

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

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

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

39 (5) *In the case of a breach of the security of the system involving*  
40 *personal information defined in paragraph (2) of subdivision (g)*

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

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

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

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

22 1798.82. (a) A person or business that conducts business in  
23 California, and that owns or licenses computerized data that  
24 includes personal information, shall disclose a breach of the  
25 security of the system following discovery or notification of the  
26 breach in the security of the data to a resident of California whose  
27 unencrypted personal information was, or is reasonably believed  
28 to have been, acquired by an unauthorized person. The disclosure  
29 shall be made in the most expedient time possible and without  
30 unreasonable delay, consistent with the legitimate needs of law  
31 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) A person or business that maintains computerized data that  
35 includes personal information that the person or business does not  
36 own shall notify the owner or licensee of the information of the  
37 breach of the security of the data immediately following discovery,  
38 if the personal information was, or is reasonably believed to have  
39 been, acquired 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 promptly after the law enforcement agency  
5 determines that it will not compromise the investigation.

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

9 (1) The security breach notification shall be written in plain  
10 language.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

39 (f) A person or business that is required to issue a security breach  
40 notification pursuant to this section to more than 500 California

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

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

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

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

21 (A) Social security number.

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

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

28 (D) Medical information.

29 (E) Health insurance information.

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

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

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

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

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

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

12 (1) Written notice.

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

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

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

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

27 (C) Notification to major statewide media.

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

36 *SEC. 2.1. Section 1798.82 of the Civil Code is amended to*  
37 *read:*

38 1798.82. (a) A person or business that conducts business in  
39 California, and that owns or licenses computerized data that  
40 includes personal information, shall disclose a breach of the

1 security of the system following discovery or notification of the  
2 breach in the security of the data to a resident of California whose  
3 unencrypted personal information was, or is reasonably believed  
4 to have been, acquired by an unauthorized person. The disclosure  
5 shall be made in the most expedient time possible and without  
6 unreasonable delay, consistent with the legitimate needs of law  
7 enforcement, as provided in subdivision (c), or any measures  
8 necessary to determine the scope of the breach and restore the  
9 reasonable integrity of the data system.

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

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

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

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

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

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

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

37 (D) *For a written notice described in paragraph (1) of*  
38 *subdivision (j), use of the model security breach notification form*  
39 *prescribed below or use of the headings described in this*  
40 *paragraph with the information described in paragraph (2), written*

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

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  
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>		
<i>Other Important Information.</i> <i>[insert other important information]</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  
39

<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 (j), use of the headings described in this paragraph with the information described in paragraph (2), written in plain language, shall be deemed to be in compliance with this subdivision.*

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

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

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

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

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

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

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

(G) If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no

1 cost to the affected person for not less than 12 ~~months~~, *months*  
2 along with all information necessary to take advantage of the offer  
3 to any person whose information was or may have been breached  
4 if the breach exposed or may have exposed personal information  
5 defined in subparagraphs (A) and (B) of paragraph (1) of  
6 subdivision (h).

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

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

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

13 ~~(4) In the case of a breach of the security of the system involving  
14 personal information defined in paragraph (2) of subdivision (h)  
15 for an online account, and no other personal information defined  
16 in paragraph (1) of subdivision (h), the person or business may  
17 comply with this section by providing the security breach  
18 notification in electronic or other form that directs the person whose  
19 personal information has been breached promptly to change his  
20 or her password and security question or answer, as applicable, or  
21 to take other steps appropriate to protect the online account with  
22 the person or business and all other online accounts for which the  
23 person whose personal information has been breached 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 (h)  
28 for login credentials of an email account furnished by the person  
29 or business, the person or business shall not comply with this  
30 section by providing the security breach notification to that email  
31 address, but may, instead, comply with this section by providing  
32 notice by another method described in subdivision (j) or by clear  
33 and conspicuous notice delivered to the resident online when the  
34 resident is connected to the online account from an Internet  
35 Protocol address or online location from which the person or  
36 business knows the resident customarily accesses the account.~~

37 (e) A covered entity under the federal Health Insurance  
38 Portability and Accountability Act of 1996 (42 U.S.C. Sec. 1320d  
39 et seq.) will be deemed to have complied with the notice  
40 requirements in subdivision (d) if it has complied completely with

1 Section 13402(f) of the federal Health Information Technology  
2 for Economic and Clinical Health Act (Public Law 111-5).  
3 However, nothing in this subdivision shall be construed to exempt  
4 a covered entity from any other provision of this section.

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

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

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

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

27 (A) Social security number.

28 (B) Driver’s license number or California identification card  
29 number.

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

34 (D) Medical information.

35 (E) Health insurance information.

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

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

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

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

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

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

19 (1) Written notice.

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

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

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

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

1 (C) Notification to major statewide media.

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

15 (5) *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 login credentials of an email account furnished by the person*  
18 *or business, the person or business shall not comply with this*  
19 *section by providing the security breach notification to that email*  
20 *address, but may, instead, comply with this section by providing*  
21 *notice by another method described in this subdivision or by clear*  
22 *and conspicuous notice delivered to the resident online when the*  
23 *resident is connected to the online account from an Internet*  
24 *Protocol address or online location from which the person or*  
25 *business knows the resident customarily accesses the account.*

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

34 *SEC. 2.2. Section 1798.82 of the Civil Code is amended to*  
35 *read:*

36 1798.82. (a) A person or business that conducts business in  
37 California, and that owns or licenses computerized data that  
38 includes personal information, shall disclose a breach of the  
39 security of the system following discovery or notification of the  
40 breach in the security of the data to a resident of California whose

1 unencrypted personal information was, or is reasonably believed  
2 to have been, acquired by an unauthorized person. The disclosure  
3 shall be made in the most expedient time possible and without  
4 unreasonable delay, consistent with the legitimate needs of law  
5 enforcement, as provided in subdivision (c), or any measures  
6 necessary to determine the scope of the breach and restore the  
7 reasonable integrity of the data system.

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

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

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

22 (1) The security breach notification shall be written in plain  
23 language.

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

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

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

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

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

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

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

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

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

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

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

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

32 (5) 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 login credentials of an email account furnished by the person  
35 or business, the person or business shall not comply with this  
36 section by providing the security breach notification to that email  
37 address, but may, instead, comply with this section by providing  
38 notice by another method described in subdivision (j) or by clear  
39 and conspicuous notice delivered to the resident online when the  
40 resident is connected to the online account from an Internet

1 Protocol address or online location from which the person or  
2 business knows the resident customarily accesses the account.

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

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

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

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

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

33 (A) Social security number.

34 (B) Driver’s license number or California identification card  
35 number.

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

40 (D) Medical information.

1 (E) Health insurance information.

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

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

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

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

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

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

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

1 (B) Conspicuous posting of the notice on the Internet Web site  
2 page of the person or business, if the person or business maintains  
3 one.

4 (C) Notification to major statewide media.

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

13 *SEC. 2.3. Section 1798.82 of the Civil Code is amended to*  
14 *read:*

15 1798.82. (a) A person or business that conducts business in  
16 California, and that owns or licenses computerized data that  
17 includes personal information, shall disclose a breach of the  
18 security of the system following discovery or notification of the  
19 breach in the security of the data to a resident of California whose  
20 unencrypted personal information was, or is reasonably believed  
21 to have been, acquired by an unauthorized person. The disclosure  
22 shall be made in the most expedient time possible and without  
23 unreasonable delay, consistent with the legitimate needs of law  
24 enforcement, as provided in subdivision (c), or any measures  
25 necessary to determine the scope of the breach and restore the  
26 reasonable integrity of the data system.

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

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

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

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

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

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

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

14 (D) For a written notice described in paragraph (1) of  
 15 subdivision (j), use of the model security breach notification form  
 16 prescribed below or use of the headings described in this  
 17 paragraph with the information described in paragraph (2), written  
 18 in plain language, shall be deemed to be in compliance with this  
 19 subdivision.

[NAME OF INSTITUTION / LOGO]		Date: [insert date]
<b>NOTICE OF DATA BREACH</b>		
<i>What Happened?</i>		
<i>What Information Was Involved?</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 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 (j), use of the headings described in this paragraph with the information described in paragraph (2), written in plain language, shall be deemed to be in compliance with this subdivision.*

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

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

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

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~~, *months*  
20 along with all information necessary to take advantage of the offer  
21 to any person whose information was or may have been breached  
22 if the breach exposed or may have exposed personal information  
23 defined in subparagraphs (A) and (B) of paragraph (1) of  
24 subdivision (h).

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

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

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

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

1 person whose personal information has been breached uses the  
2 same user name or email address and password or security question  
3 or answer.

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

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

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

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

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

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

6 (A) Social security number.

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

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

13 (D) Medical information.

14 (E) Health insurance information.

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

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

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

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

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

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

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

40 (1) Written notice.

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

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

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

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

22 (C) Notification to major statewide media.

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

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

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

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

15 SEC. 3. Title 1.81.23 (commencing with Section 1798.90.5)  
16 is added to Part 4 of Division 3 of the Civil Code, to read:

17  
18 TITLE 1.81.23. COLLECTION OF LICENSE PLATE  
19 INFORMATION  
20

21 1798.90.5. The following definitions shall apply for purposes  
22 of this title:

23 (a) “Automated license plate recognition end-user” or “ALPR  
24 end-user” means a person that accesses or uses an ALPR system,  
25 but does not include any of the following:

26 (1) A transportation agency when subject to Section 31490 of  
27 the Streets and Highways Code.

28 (2) A person that is subject to Sections 6801 to 6809, inclusive,  
29 of Title 15 of the United States Code and state or federal statutes  
30 or regulations implementing those sections, if the person is subject  
31 to compliance oversight by a state or federal regulatory agency  
32 with respect to those sections.

33 (3) A person, other than a law enforcement agency, to whom  
34 information may be disclosed as a permissible use pursuant to  
35 Section 2721 of Title 18 of the United States Code.

36 (b) “Automated license plate recognition information,” or  
37 “ALPR information” means information or data collected through  
38 the use of an ALPR system.

39 (c) “Automated license plate recognition operator” or “ALPR  
40 operator” means a person that operates an ALPR system, but does

1 not include a transportation agency when subject to Section 31490  
2 of the Streets and Highways Code.

3 (d) “Automated license plate recognition system” or “ALPR  
4 system” means a searchable computerized database resulting from  
5 the operation of one or more mobile or fixed cameras combined  
6 with computer algorithms to read and convert images of registration  
7 plates and the characters they contain into computer-readable data.

8 (e) “Person” means any natural person, public agency,  
9 partnership, firm, association, corporation, limited liability  
10 company, or other legal entity.

11 (f) “Public agency” means the state, any city, county, or city  
12 and county, or any agency or political subdivision of the state or  
13 a city, county, or city and county, including, but not limited to, a  
14 law enforcement agency.

15 1798.90.51. An ALPR operator shall do all of the following:

16 (a) Maintain reasonable security procedures and practices,  
17 including operational, administrative, technical, and physical  
18 safeguards, to protect ALPR information from unauthorized access,  
19 destruction, use, modification, or disclosure.

20 (b) (1) Implement a usage and privacy policy in order to ensure  
21 that the collection, use, maintenance, sharing, and dissemination  
22 of ALPR information is consistent with respect for individuals’  
23 privacy and civil liberties. The usage and privacy policy shall be  
24 available to the public in writing, and, if the ALPR operator has  
25 an Internet Web site, the usage and privacy policy shall be posted  
26 conspicuously on that Internet Web site.

27 (2) The usage and privacy policy shall, at a minimum, include  
28 all of the following:

29 (A) The authorized purposes for using the ALPR system and  
30 collecting ALPR information.

31 (B) A description of the job title or other designation of the  
32 employees and independent contractors who are authorized to use  
33 or access the ALPR system, or to collect ALPR information. The  
34 policy shall identify the training requirements necessary for those  
35 authorized employees and independent contractors.

36 (C) A description of how the ALPR system will be monitored  
37 to ensure the security of the information and compliance with  
38 applicable privacy laws.

39 (D) The purposes of, process for, and restrictions on, the sale,  
40 sharing, or transfer of ALPR information to other persons.

1 (E) The title of the official custodian, or owner, of the ALPR  
2 system responsible for implementing this section.

3 (F) A description of the reasonable measures that will be used  
4 to ensure the accuracy of ALPR information and correct data errors.

5 (G) The length of time ALPR information will be retained, and  
6 the process the ALPR operator will utilize to determine if and  
7 when to destroy retained ALPR information.

8 1798.90.52. If an ALPR operator accesses or provides access  
9 to ALPR information, the ALPR operator shall do both of the  
10 following:

11 (a) Maintain a record of that access. At a minimum, the record  
12 shall include all of the following:

13 (1) The date and time the information is accessed.

14 (2) The license plate number or other data elements used to  
15 query the ALPR system.

16 (3) The username of the person who accesses the information,  
17 and, as applicable, the organization or entity with whom the person  
18 is affiliated.

19 (4) The purpose for accessing the information.

20 (b) Require that ALPR information only be used for the  
21 authorized purposes described in the usage and privacy policy  
22 required by subdivision (b) of Section 1798.90.51.

23 1798.90.53. An ALPR end-user shall do all of the following:

24 (a) Maintain reasonable security procedures and practices,  
25 including operational, administrative, technical, and physical  
26 safeguards, to protect ALPR information from unauthorized access,  
27 destruction, use, modification, or disclosure.

28 (b) (1) Implement a usage and privacy policy in order to ensure  
29 that the access, use, sharing, and dissemination of ALPR  
30 information is consistent with respect for individuals' privacy and  
31 civil liberties. The usage and privacy policy shall be available to  
32 the public in writing, and, if the ALPR end-user has an Internet  
33 Web site, the usage and privacy policy shall be posted  
34 conspicuously on that Internet Web site.

35 (2) The usage and privacy policy shall, at a minimum, include  
36 all of the following:

37 (A) The authorized purposes for accessing and using ALPR  
38 information.

39 (B) A description of the job title or other designation of the  
40 employees and independent contractors who are authorized to

1 access and use ALPR information. The policy shall identify the  
2 training requirements necessary for those authorized employees  
3 and independent contractors.

4 (C) A description of how the ALPR system will be monitored  
5 to ensure the security of the information accessed or used, and  
6 compliance with all applicable privacy laws and a process for  
7 periodic system audits.

8 (D) The purposes of, process for, and restrictions on, the sale,  
9 sharing, or transfer of ALPR information to other persons.

10 (E) The title of the official custodian, or owner, of the ALPR  
11 information responsible for implementing this section.

12 (F) A description of the reasonable measures that will be used  
13 to ensure the accuracy of ALPR information and correct data errors.

14 (G) The length of time ALPR information will be retained, and  
15 the process the ALPR end-user will utilize to determine if and  
16 when to destroy retained ALPR information.

17 1798.90.54. (a) In addition to any other sanctions, penalties,  
18 or remedies provided by law, an individual who has been harmed  
19 by a violation of this title, including, but not limited to,  
20 unauthorized access or use of ALPR information or a breach of  
21 security of an ALPR system, may bring a civil action in any court  
22 of competent jurisdiction against a person who knowingly caused  
23 the harm.

24 (b) The court may award a combination of any one or more of  
25 the following:

26 (1) Actual damages, but not less than liquidated damages in the  
27 amount of two thousand five hundred dollars (\$2,500).

28 (2) Punitive damages upon proof of willful or reckless disregard  
29 of the law.

30 (3) Reasonable attorney’s fees and other litigation costs  
31 reasonably incurred.

32 (4) Other preliminary and equitable relief as the court determines  
33 to be appropriate.

34 1798.90.55. Notwithstanding any other law or regulation:

35 (a) A public agency that operates or intends to operate an ALPR  
36 system shall provide an opportunity for public comment at a  
37 regularly scheduled public meeting of the governing body of the  
38 public agency before implementing the program.

39 (b) A public agency shall not sell, share, or transfer ALPR  
40 information, except to another public agency, and only as otherwise

1 permitted by law. For purposes of this section, the provision of  
2 data hosting or towing services shall not be considered the sale,  
3 sharing, or transferring of ALPR information.

4 *SEC. 4. (a) Section 1.1 of this bill incorporates amendments*  
5 *to Section 1798.29 of the Civil Code proposed by both this bill*  
6 *and Senate Bill 570. It shall only become operative if (1) both bills*  
7 *are enacted and become effective on or before January 1, 2016,*  
8 *(2) each bill amends Section 1798.29 of the Civil Code, (3)*  
9 *Assembly Bill 964 is not enacted or as enacted does not amend*  
10 *that section, and (4) this bill is enacted after Senate Bill 570, in*  
11 *which case Sections 1, 1.2, and 1.3 of this bill shall not become*  
12 *operative.*

13 *(b) Section 1.2 of this bill incorporates amendments to Section*  
14 *1798.29 of the Civil Code proposed by both this bill and Assembly*  
15 *Bill 964. It shall only become operative if (1) both bills are enacted*  
16 *and become effective on or before January 1, 2016, (2) each bill*  
17 *amends Section 1798.29 of the Civil Code, (3) Senate Bill 570 is*  
18 *not enacted or as enacted does not amend that section, and (4)*  
19 *this bill is enacted after Assembly Bill 964, in which case Sections*  
20 *1, 1.1, and 1.3 of this bill shall not become operative.*

21 *(c) Section 1.3 of this bill incorporates amendments to Section*  
22 *1798.29 of the Civil Code proposed by this bill, Senate Bill 570,*  
23 *and Assembly Bill 964. It shall only become operative if (1) all*  
24 *three bills are enacted and become effective on or before January*  
25 *1, 2016, (2) all three bills amend Section 1798.29 of the Civil Code,*  
26 *and (3) this bill is enacted after Senate Bill 570 and Assembly Bill*  
27 *964, in which case Sections 1, 1.1, and 1.2 of this bill shall not*  
28 *become operative.*

29 *SEC. 5. (a) Section 2.1 of this bill incorporates amendments*  
30 *to Section 1798.82 of the Civil Code proposed by both this bill*  
31 *and Senate Bill 570. It shall only become operative if (1) both bills*  
32 *are enacted and become effective on or before January 1, 2016,*  
33 *(2) each bill amends Section 1798.82 of the Civil Code, (3)*  
34 *Assembly Bill 964 is not enacted or as enacted does not amend*  
35 *that section, and (4) this bill is enacted after Senate Bill 570, in*  
36 *which case Sections 2, 2.2, and 2.3 of this bill shall not become*  
37 *operative.*

38 *(b) Section 2.2 of this bill incorporates amendments to Section*  
39 *1798.82 of the Civil Code proposed by both this bill and Assembly*  
40 *Bill 964. It shall only become operative if (1) both bills are enacted*

1 and become effective on or before January 1, 2016, (2) each bill  
2 amends Section 1798.82 of the Civil Code, (3) Senate Bill 570 is  
3 not enacted or as enacted does not amend that section, and (4)  
4 this bill is enacted after Assembly Bill 964, in which case Sections  
5 2, 2.1, and 2.3 of this bill shall not become operative.

6 (c) Section 2.3 of this bill incorporates amendments to Section  
7 1798.82 of the Civil Code proposed by this bill, Senate Bill 570,  
8 and Assembly Bill 964. It shall only become operative if (1) all  
9 three bills are enacted and become effective on or before January  
10 1, 2016, (2) all three bills amend Section 1798.82 of the Civil Code,  
11 and (3) this bill is enacted after Senate Bill 570 and Assembly Bill  
12 964, in which case Sections 2, 2.1, and 2.2 of this bill shall not  
13 become operative.