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.


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

SECTION 1. Section 1798.29 of the Civil Code is amended to read:

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

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

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

(d) Any agency that is required to issue a security breach notification pursuant to this section shall meet all of the following requirements:
(1) The security breach notification shall be written in plain language.

(2) The security breach notification 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:

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

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

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

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

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

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

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

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

(A) Social security number.

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

(C) Account number, credit or debit card number, in combination with any required security code, access code, or
password that would permit access to an individual’s financial
account.
(D) Medical information.
(E) Health insurance information.
(F) Information or data collected through the use or operation
of an automated license plate recognition system, as defined in
Section 1798.90.5.
(2) A user name or email address, in combination with a
password or security question and answer that would permit access
to an online account.
(h) (1) For purposes of this section, “personal information”
does not include publicly available information that is lawfully
made available to the general public from federal, state, or local
government records.
(2) For purposes of this section, “medical information” means
any information regarding an individual’s medical history, mental
or physical condition, or medical treatment or diagnosis by a health
care professional.
(3) For purposes of this section, “health insurance information”
means an individual’s health insurance policy number or subscriber
identification number, any unique identifier used by a health insurer
to identify the individual, or any information in an individual’s
application and claims history, including any appeals records.
(i) For purposes of this section, “notice” may be provided by
one of the following methods:
(1) Written notice.
(2) Electronic notice, if the notice provided is consistent with
the provisions regarding electronic records and signatures set forth
in Section 7001 of Title 15 of the United States Code.
(3) Substitute notice, if the agency demonstrates that the cost
of providing notice would exceed two hundred fifty thousand
dollars ($250,000), or that the affected class of subject persons to
be notified exceeds 500,000, or the agency does not have sufficient
contact information. Substitute notice shall consist of all of the
following:
(A) Email notice when the agency has an email address for the
subject persons.
(B) Conspicuous posting of the notice on the agency’s Internet
Web site page, if the agency maintains one.
(C) Notification to major statewide media and the Office of Information Security within the Department of Technology.

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

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

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

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

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

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

(d) Any agency that is required to issue a security breach notification pursuant to this section shall meet all of the following requirements:
The security breach notification shall be written in plain language, shall be titled “Notice of Data Breach,” and shall present the information described in paragraph (2) under the following headings: “What Happened,” “What Information Was Involved,” “What We Are Doing,” “What You Can Do,” and “For More Information.” Additional information may be provided as a supplement to the notice.

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

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

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

(D) For a written notice described in paragraph (1) of subdivision (i), use of the model security breach notification form prescribed below or 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.

---

[NAME OF INSTITUTION / LOGO]  Date: [insert date]

<table>
<thead>
<tr>
<th>NOTICE OF DATA BREACH</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td>What Happened?</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>What Information</td>
</tr>
<tr>
<td>Was Involved?</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>What We Are Doing.</td>
</tr>
<tr>
<td>--------------------</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>What You Can Do.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Other Important Information.</th>
</tr>
</thead>
<tbody>
<tr>
<td>[insert other important information]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Call [telephone number] or go to [Internet Web site]</th>
</tr>
</thead>
<tbody>
<tr>
<td>For More Information.</td>
</tr>
</tbody>
</table>

(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:

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

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

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

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

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

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

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

(1) An individual’s first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:
   (A) Social security number.
   (B) Driver’s license number or California identification card number.
   (C) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account.
   (D) Medical information.
   (E) Health insurance information.
   (F) Information or data collected through the use or operation of an automated license plate recognition system, as defined in Section 1798.90.5.
   (G) A user name or email address, in combination with a password or security question and answer that would permit access to an online account.
For purposes of this section, “personal information” does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

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

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

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

(1) Written notice.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(2) The security breach notification 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:

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

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

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

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

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

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

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

(1) An individual’s first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:
   (A) Social security number.
   (B) Driver’s license number or California identification card number.
   (C) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account.
   (D) Medical information.
   (E) Health insurance information.
   (F) Information or data collected through the use or operation of an automated license plate recognition system, as defined in Section 1798.90.5.

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

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

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

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

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

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

(1) Written notice.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(D) For a written notice described in paragraph (1) of subdivision (i), use of the model security breach notification form prescribed below or 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.

[NAME OF INSTITUTION / LOGO]  Date: [insert date]

NOTICE OF DATA BREACH

<table>
<thead>
<tr>
<th>What Happened?</th>
<th></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>What Information Was Involved?</th>
<th></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>What We Are Doing.</th>
<th></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>What You Can Do.</th>
<th></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Other Important Information.</th>
<th>[insert other important information]</th>
</tr>
</thead>
</table>
(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:
(A) Information about what the agency has done to protect individuals whose information has been breached.

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

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

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

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

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

(g) For purposes of this section, “personal information” means
either of the following:
(1) An individual’s first name or first initial and last name in
combination with any one or more of the following data elements,
when either the name or the data elements are not encrypted:
(A) Social security number.
(B) Driver’s license number or California identification card
number.
(C) Account number, credit or debit card number, in
combination with any required security code, access code, or
password that would permit access to an individual’s financial
account.
(D) Medical information.
(E) Health insurance information.
(F) Information or data collected through the use or operation
of an automated license plate recognition system, as defined in
Section 1798.90.5.
(2) A user name or email address, in combination with a
password or security question and answer that would permit access
to an online account.

(h) (1) For purposes of this section, “personal information”
does not include publicly available information that is lawfully
made available to the general public from federal, state, or local
government records.
(2) For purposes of this section, “medical information” means
any information regarding an individual’s medical history, mental
or physical condition, or medical treatment or diagnosis by a health
care professional.
(3) For purposes of this section, “health insurance information”
means an individual’s health insurance policy number or subscriber
identification number, any unique identifier used by a health insurer
to identify the individual, or any information in an individual’s
application and claims history, including any appeals records.
(4) For purposes of this section, “encrypted” means rendered
unsalable, unreadable, or indecipherable to an unauthorized person
through a security technology or methodology generally accepted
in the field of information security.
(i) For purposes of this section, “notice” may be provided by one of the following methods:

1. Written notice.
2. Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.
3. Substitute notice, if the agency demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the agency does not have sufficient contact information. Substitute notice shall consist of all of the following:
   (A) Email notice when the agency has an email address for the subject persons.
   (B) Conspicuous posting, for a minimum of 30 days, of the notice on the agency’s Internet Web site page, if the agency maintains one. For purposes of this subparagraph, conspicuous posting on the agency’s Internet Web site means providing a link to the notice on the home page or first significant page after entering the Internet Web site that is in larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size, or set off from the surrounding text of the same size by symbols or other marks that call attention to the link.
   (C) Notification to major statewide media and the Office of Information Security within the Department of Technology.
4. In the case of a breach of the security of the system involving personal information defined in paragraph (2) of subdivision (g) for an online account, and no other personal information defined in paragraph (1) of subdivision (g), the agency may comply with this section by providing the security breach notification in electronic or other form that directs the person whose personal information has been breached to promptly change his or her password and security question or answer, as applicable, or to take other steps appropriate to protect the online account with the agency and all other online accounts for which the person uses the same user name or email address or password or security question or answer.
5. In the case of a breach of the security of the system involving personal information defined in paragraph (2) of subdivision (g)
for login credentials of an email account furnished by the agency, the agency shall not comply with this section by providing the security breach notification to that email address, but may, instead, comply with this section by providing notice by another method described in this subdivision or by clear and conspicuous notice delivered to the resident online when the resident is connected to the online account from an Internet Protocol address or online location from which the agency knows the resident customarily accesses the account.

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

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

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

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

(b) A person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made promptly after the law enforcement agency determines that it will not compromise the investigation.

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

1. The security breach notification shall be written in plain language.
2. The security breach notification 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 cost to the affected person for not less than 12 months, along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed personal information defined in subparagraphs (A) and (B) of paragraph (1) of subdivision (h).
(3) At the discretion of the person or business, the security breach notification may also include any of the following:

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

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

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

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

(e) A covered entity under the federal Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. Sec. 1320d et seq.) will be deemed to have complied with the notice requirements in subdivision (d) if it has complied completely with Section 13402(f) of the federal Health Information Technology for Economic and Clinical Health Act (Public Law 111-5).

However, nothing in this subdivision shall be construed to exempt a covered entity from any other provision of this section.

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

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

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

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

(A) Social security number.
(B) Driver’s license number or California identification card number.
(C) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account.
(D) Medical information.
(E) Health insurance information.
(F) Information or data collected through the use or operation of an automated license plate recognition system, as defined in Section 1798.90.5.

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

(i) (1) For purposes of this section, “personal information” does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.
(2) For purposes of this section, “medical information” means any information regarding an individual’s medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

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

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

(1) Written notice.

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

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

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

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

(C) Notification to major statewide media.

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

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

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

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

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

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

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

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

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

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

   (D) For a written notice described in paragraph (1) of subdivision (j), use of the model security breach notification form prescribed below or 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.

<table>
<thead>
<tr>
<th>[NAME OF INSTITUTION / LOGO]</th>
<th>Date: [insert date]</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NOTICE OF DATA BREACH</strong></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>What Happened?</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>What Information Was Involved?</td>
<td></td>
</tr>
<tr>
<td>What We Are Doing.</td>
<td></td>
</tr>
<tr>
<td>What You Can Do.</td>
<td></td>
</tr>
<tr>
<td>Other Important Information.</td>
<td>[insert other important information]</td>
</tr>
</tbody>
</table>
For More Information.

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

(3) At the discretion of the person or business, the security
breach notification may also include any of the following:
(A) Information about what the person or business has done to
protect individuals whose information has been breached.
(B) Advice on steps that the person whose information has been
breached may take to protect himself or herself.

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

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

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

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

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

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

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

(A) Social security number.

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

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

(D) Medical information.

(E) Health insurance information.

(F) Information or data collected through the use or operation of an automated license plate recognition system, as defined in Section 1798.90.5.
(2) A user name or email address, in combination with a password or security question and answer that would permit access to an online account.

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

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

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

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

(1) Written notice.

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

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

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

(B) Conspicuous posting, for a minimum of 30 days, of the notice on the Internet Web site page of the person or business, if the person or business maintains one. For purposes of this subparagraph, conspicuous posting on the person’s or business’s Internet Web site means providing a link to the notice on the home page or first significant page after entering the Internet Web site that is in larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size, or set off from the surrounding text of the same size by symbols or other marks that call attention to the link.
(C) Notification to major statewide media.

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

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

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

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

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

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

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

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

1. The security breach notification shall be written in plain language.
2. The security breach notification 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 cost to the affected person for not less than 12 months, along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed personal information defined in subparagraphs (A) and (B) of paragraph (1) of subdivision (h).

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

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

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

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

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

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

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

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

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

1. An individual’s first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:
   (A) Social security number.
   (B) Driver’s license number or California identification card number.
   (C) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account.
   (D) Medical information.
(E) Health insurance information.

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

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

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

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

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

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

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

(1) Written notice.

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

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

(A) Email notice when the person or business has an email address for the subject persons.
(B) Conspicuous posting of the notice on the Internet Web site page of the person or business, if the person or business maintains one.

(C) Notification to major statewide media.

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

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

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

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

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

(d) A person or business that is required to issue a security breach notification pursuant to this section shall meet all of the following requirements:
(1) The security breach notification shall be written in plain language, shall be titled “Notice of Data Breach,” and shall present the information described in paragraph (2) under the following headings: “What Happened,” “What Information Was Involved,” “What We Are Doing,” “What You Can Do,” and “For More Information.” Additional information may be provided as a supplement to the notice.

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

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

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

(D) For a written notice described in paragraph (1) of subdivision (j), use of the model security breach notification form prescribed below or 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.

<table>
<thead>
<tr>
<th>[NAME OF INSTITUTION / LOGO]</th>
<th>Date: [insert date]</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>NOTICE OF DATA BREACH</td>
</tr>
<tr>
<td></td>
<td>What Happened?</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>What Information Was Involved?</td>
</tr>
</tbody>
</table>

95
<table>
<thead>
<tr>
<th>What We Are Doing.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>What You Can Do.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Other Important Information.</th>
</tr>
</thead>
<tbody>
<tr>
<td>[insert other important information]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Call [telephone number] or go to [Internet Web site]</th>
</tr>
</thead>
</table>

For More Information.

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

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

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

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

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

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

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

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

(g) For purposes of this section, “breach of the system” means unauthorized acquisition of computerized data that
compromises the security, confidentiality, or integrity of personal
information maintained by the person or business. Good faith
acquisition of personal information by an employee or agent of
the person or business for the purposes of the person or business
is not a breach of the security of the system, provided that the
personal information is not used or subject to further unauthorized
disclosure.
(h) For purposes of this section, “personal information” means either of the following:
(1) An individual’s first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:
(A) Social security number.
(B) Driver’s license number or California identification card number.
(C) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account.
(D) Medical information.
(E) Health insurance information.
(F) Information or data collected through the use or operation of an automated license plate recognition system, as defined in Section 1798.90.5.
(2) A user name or email address, in combination with a password or security question and answer that would permit access to an online account.
(i) (1) For purposes of this section, “personal information” does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.
(2) For purposes of this section, “medical information” means any information regarding an individual’s medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.
(3) For purposes of this section, “health insurance information” means an individual’s health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual’s application and claims history, including any appeals records.
(4) For purposes of this section, “encrypted” means rendered unusable, unreadable, or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security.
(j) For purposes of this section, “notice” may be provided by one of the following methods:
(1) Written notice.
(2) Electronic notice, if the notice provided is consistent with
the provisions regarding electronic records and signatures set forth
in Section 7001 of Title 15 of the United States Code.
(3) Substitute notice, if the person or business demonstrates that
the cost of providing notice would exceed two hundred fifty
thousand dollars ($250,000), or that the affected class of subject
persons to be notified exceeds 500,000, or the person or business
does not have sufficient contact information. Substitute notice
shall consist of all of the following:
(A) Email notice when the person or business has an email
address for the subject persons.
(B) Conspicuous posting, for a minimum of 30 days, of
the notice on the Internet Web site page of the person or business,
if the person or business maintains one. For purposes of this
subparagraph, conspicuous posting on the person’s or business’s
Internet Web site means providing a link to the notice on the home
page or first significant page after entering the Internet Web site
that is in larger type than the surrounding text, or in contrasting
type, font, or color to the surrounding text of the same size, or set
off from the surrounding text of the same size by symbols or other
marks that call attention to the link.
(C) Notification to major statewide media.
(4) In the case of a breach of the security of the system involving
personal information defined in paragraph (2) of subdivision (h)
for an online account, and no other personal information defined
in paragraph (1) of subdivision (h), the person or business may
comply with this section by providing the security breach
notification in electronic or other form that directs the person
whose personal information has been breached promptly to change
his or her password and security question or answer, as applicable,
or to take other steps appropriate to protect the online account
with the person or business and all other online accounts for which
the person whose personal information has been breached uses
the same user name or email address and password or security
question or answer.
(5) In the case of a breach of the security of the system involving
personal information defined in paragraph (2) of subdivision (h)
for login credentials of an email account furnished by the person
or business, the person or business shall not comply with this
section by providing the security breach notification to that email
address, but may, instead, comply with this section by providing notice by another method described in this subdivision or by clear and conspicuous notice delivered to the resident online when the resident is connected to the online account from an Internet Protocol address or online location from which the person or business knows the resident customarily accesses the account.

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

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

TITLE 1.81.23. COLLECTION OF LICENSE PLATE INFORMATION

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

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

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

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

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

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

(c) “Automated license plate recognition operator” or “ALPR operator” means a person that operates an ALPR system, but does
not include a transportation agency when subject to Section 31490
of the Streets and Highways Code.
(d) “Automated license plate recognition system” or “ALPR
system” means a searchable computerized database resulting from
the operation of one or more mobile or fixed cameras combined
with computer algorithms to read and convert images of registration
plates and the characters they contain into computer-readable data.
(e) “Person” means any natural person, public agency,
partnership, firm, association, corporation, limited liability
company, or other legal entity.
(f) “Public agency” means the state, any city, county, or city
and county, or any agency or political subdivision of the state or
a city, county, or city and county, including, but not limited to, a
law enforcement agency.
1798.90.51. An ALPR operator shall do all of the following:
(a) Maintain reasonable security procedures and practices,
including operational, administrative, technical, and physical
safeguards, to protect ALPR information from unauthorized access,
destruction, use, modification, or disclosure.
(b) (1) Implement a usage and privacy policy in order to ensure
that the collection, use, maintenance, sharing, and dissemination
of ALPR information is consistent with respect for individuals’
privacy and civil liberties. The usage and privacy policy shall be
available to the public in writing, and, if the ALPR operator has
an Internet Web site, the usage and privacy policy shall be posted
conspicuously on that Internet Web site.
(2) The usage and privacy policy shall, at a minimum, include
all of the following:
(A) The authorized purposes for using the ALPR system and
collecting ALPR information.
(B) A description of the job title or other designation of the
employees and independent contractors who are authorized to use
or access the ALPR system, or to collect ALPR information. The
policy shall identify the training requirements necessary for those
authorized employees and independent contractors.
(C) A description of how the ALPR system will be monitored
to ensure the security of the information and compliance with
applicable privacy laws.
(D) The purposes of, process for, and restrictions on, the sale,
sharing, or transfer of ALPR information to other persons.
(E) The title of the official custodian, or owner, of the ALPR
system responsible for implementing this section.
(F) A description of the reasonable measures that will be used
to ensure the accuracy of ALPR information and correct data errors.
(G) The length of time ALPR information will be retained, and
the process the ALPR operator will utilize to determine if and
when to destroy retained ALPR information.
1798.90.52. If an ALPR operator accesses or provides access
to ALPR information, the ALPR operator shall do both of the
following:
(a) Maintain a record of that access. At a minimum, the record
shall include all of the following:
(1) The date and time the information is accessed.
(2) The license plate number or other data elements used to
query the ALPR system.
(3) The username of the person who accesses the information,
and, as applicable, the organization or entity with whom the person
is affiliated.
(4) The purpose for accessing the information.
(b) Require that ALPR information only be used for the
authorized purposes described in the usage and privacy policy
required by subdivision (b) of Section 1798.90.51.
1798.90.53. An ALPR end-user shall do all of the following:
(a) Maintain reasonable security procedures and practices,
including operational, administrative, technical, and physical
safeguards, to protect ALPR information from unauthorized access,
destruction, use, modification, or disclosure.
(b) (1) Implement a usage and privacy policy in order to ensure
that the access, use, sharing, and dissemination of ALPR
information is consistent with respect for individuals’ privacy and
civil liberties. The usage and privacy policy shall be available to
the public in writing, and, if the ALPR end-user has an Internet
Web site, the usage and privacy policy shall be posted
conspicuously on that Internet Web site.
(2) The usage and privacy policy shall, at a minimum, include
all of the following:
(A) The authorized purposes for accessing and using ALPR
information.
(B) A description of the job title or other designation of the
employees and independent contractors who are authorized to
access and use ALPR information. The policy shall identify the
training requirements necessary for those authorized employees
and independent contractors.
(C) A description of how the ALPR system will be monitored
to ensure the security of the information accessed or used, and
compliance with all applicable privacy laws and a process for
periodic system audits.
(D) The purposes of, process for, and restrictions on, the sale,
sharing, or transfer of ALPR information to other persons.
(E) The title of the official custodian, or owner, of the ALPR
information responsible for implementing this section.
(F) A description of the reasonable measures that will be used
to ensure the accuracy of ALPR information and correct data errors.
(G) The length of time ALPR information will be retained, and
when to destroy retained ALPR information.
1798.90.54. (a) In addition to any other sanctions, penalties,
or remedies provided by law, an individual who has been harmed
by a violation of this title, including, but not limited to,
unauthorized access or use of ALPR information or a breach of
security of an ALPR system, may bring a civil action in any court
of competent jurisdiction against a person who knowingly caused
the harm.
(b) The court may award a combination of any one or more of
the following:
(1) Actual damages, but not less than liquidated damages in the
amount of two thousand five hundred dollars ($2,500).
(2) Punitive damages upon proof of willful or reckless disregard
of the law.
(3) Reasonable attorney’s fees and other litigation costs
reasonably incurred.
(4) Other preliminary and equitable relief as the court determines
to be appropriate.
1798.90.55. Notwithstanding any other law or regulation:
(a) A public agency that operates or intends to operate an ALPR
system shall provide an opportunity for public comment at a
regularly scheduled public meeting of the governing body of the
public agency before implementing the program.
(b) A public agency shall not sell, share, or transfer ALPR
information, except to another public agency, and only as otherwise
permitted by law. For purposes of this section, the provision of data hosting or towing services shall not be considered the sale, sharing, or transferring of ALPR information.

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

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

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

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

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

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