[2007 Cal AB 1298](#)

Enacted, October 14, 2007

CALIFORNIA ADVANCE LEGISLATIVE SERVICE > 2007 REGULAR SESSION > CHAPTER 699 > (Assembly Bill No. 1298)

Notice

Added: Text highlighted in green

Digest

Personal information: disclosure.

(1) The Confidentiality of Medical Information Act prohibits a provider of health care, a health care service plan, contractor, or corporation and its subsidiaries and affiliates from intentionally sharing, selling, using for marketing, or otherwise using any medical information, as defined, for any purpose not necessary to provide health care services to a patient, except as expressly authorized by the patient, enrollee, or subscriber, as specified, or as otherwise required or authorized by law. The act includes within the definition of "provider of health care," any corporation organized for the primary purpose of maintaining medical information for treatment or diagnosis, as specified.

Violations of those provisions are subject to a civil action for compensatory and punitive damages, and, if a violation results in economic loss or personal injury to a patient, it is punishable as a misdemeanor.

This bill would apply the prohibitions of the Confidentiality of Medical Information Act to any business organized for the purpose of maintaining medical information to allow an individual to manage his or her information, or for the treatment or diagnosis of the individual. By expanding an existing crime, this bill would impose a state-mandated local program.

(2) Existing state and federal law defines and regulates consumer credit reports. Existing state law permits a consumer to place a security freeze on his or her credit report by making a request in writing, which results in the placement of a notice in the consumer's credit report that, subject to certain exceptions, prohibits the consumer credit reporting agency from releasing the consumer's credit report or any information from it without the express authorization of the consumer.

This bill would, regardless of the existence of a security freeze, permit a consumer reporting agency to disclose public record information lawfully obtained from an open public record to the extent otherwise permitted by law. The bill would specify that these provisions do not prohibit the consumer reporting agency from electing to apply a valid security freeze to the entire contents of a credit report.

(3) Existing law requires any agency, and any person or business conducting business in California, that owns or licenses computerized data that includes personal information to disclose any breach of the security of the system, following discovery or notification of the security breach, to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Existing law defines "personal information," for the purposes of these provisions, to mean an individual's first name or first initial and last name in combination with specified data elements, when either the name or the data elements are not encrypted.

This bill would add medical information and health insurance information, as defined, to the data elements that, when combined with the individual's name as described above, would constitute personal information that would require disclosure when acquired, or believed to be acquired, by an unauthorized person due to a security breach. The bill would also repeal duplicative provisions of law.

(4) This bill would incorporate changes made by AB 779 that would become operative if both bills are enacted and this bill is enacted after AB 779.

(5) The California Constitution requires the state to reimburse local agencies and school districts for certain costs mandated by the state. Statutory provisions establish procedures for making that reimbursement.

This bill would provide that no reimbursement is required by this act for a specified reason.

Synopsis

An act to amend Sections 56.06 and 1785.11.2 of, and to repeal and amend *Sections 1798.29 and 1798.82 of, the Civil Code*, relating to personal information.

Text

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

SECTION 1.

Section 56.06 of the Civil Code is amended to read:

§ 56.06.

(a) Any * * * BUSINESS organized for the * * * purpose of maintaining medical information in order to make the information available to * * * AN INDIVIDUAL or to a provider of health care at the request of the * * * INDIVIDUAL or a provider of health care, for purposes of ALLOWING THE INDIVIDUAL TO MANAGE HIS OR HER INFORMATION, OR FOR THE diagnosis * * * AND treatment of the * * * INDIVIDUAL , shall be deemed to be a provider of health care subject to the requirements of this part. However, nothing in this section shall be construed to make a * * * BUSINESS specified in this subdivision a provider of health care for purposes of any law other than this part, including laws that specifically incorporate by reference the definitions of this part.

(b) Any * * * BUSINESS described in subdivision (a) shall maintain the same standards of confidentiality required of a provider of health care with respect to medical information disclosed to the * * * BUSINESS .

(c) Any * * * BUSINESS described in subdivision (a) shall be subject to the penalties for improper use and disclosure of medical information prescribed in this part.

SEC. 2.

Section 1785.11.2 of the Civil Code is amended to read:

§ 1785.11.2.

(a) A consumer may elect to place a security freeze on his or her credit report by making a request in writing by certified mail to a consumer credit reporting agency. "Security freeze" means a notice placed in a consumer's credit report, at the request of the consumer and subject to certain exceptions, that prohibits the consumer credit reporting agency from releasing the consumer's

credit report or any information from it without the express authorization of the consumer. If a security freeze is in place, information from a consumer's credit report may not be released to a third party without prior express authorization from the consumer. This subdivision does not prevent a consumer credit reporting agency from advising a third party that a security freeze is in effect with respect to the consumer's credit report.

(b) A consumer credit reporting agency shall place a security freeze on a consumer's credit report no later than five business days after receiving a written request from the consumer.

(c) The consumer credit reporting agency shall send a written confirmation of the security freeze to the consumer within 10 business days and shall provide the consumer with a unique personal identification number or password to be used by the consumer when providing authorization for the release of his or her credit for a specific party or period of time.

(d) If the consumer wishes to allow his or her credit report to be accessed for a specific party or period of time while a freeze is in place, he or she shall contact the consumer credit reporting agency, request that the freeze be temporarily lifted, and provide the following:

   (1) Proper identification, as defined in subdivision (c) of Section 1785.15.

   (2) The unique personal identification number or password provided by the credit reporting agency pursuant to subdivision (c).

   (3) The proper information regarding the third party who is to receive the credit report or the time period for which the report shall be available to users of the credit report.

(e) A consumer credit reporting agency that receives a request from a consumer to temporarily lift a freeze on a credit report pursuant to subdivision (d) * * * shall comply with the request no later than three business days after receiving the request.

(f) A consumer credit reporting agency may develop procedures involving the use of telephone, fax, the Internet, or other electronic media to receive and process a request from a consumer to temporarily lift a freeze on a credit report pursuant to subdivision (d) in an expedited manner.

(g) A consumer credit reporting agency shall remove or temporarily lift a freeze placed on a consumer's credit report only in the following cases:

   (1) Upon consumer request, pursuant to subdivision (d) or (j).

   (2) If the consumer's credit report was frozen due to a material misrepresentation of fact by the consumer. If a consumer credit reporting agency intends to remove a freeze upon a consumer's credit report pursuant to this paragraph, the consumer credit reporting agency shall notify the consumer in writing prior to removing the freeze on the consumer's credit report.

(h) If a third party requests access to a consumer credit report on which a security freeze is in effect, and this request is in connection with an application for credit or any other use, and the consumer does not allow his or her credit report to be accessed for that specific party or period of time, the third party may treat the application as incomplete.

(i) If a consumer requests a security freeze, the consumer credit reporting agency shall disclose the process of placing and temporarily lifting a freeze, and the process for allowing access to information from the consumer's credit report for a specific party or period of time while the freeze is in place.

(j) A security freeze shall remain in place until the consumer requests that the security freeze be removed. A consumer credit reporting agency shall remove a security freeze within three business days of receiving a request for removal from the consumer, who provides both of the following:

   (1) Proper identification, as defined in subdivision (c) of Section 1785.15.

(2) The unique personal identification number or password provided by the credit reporting agency pursuant to subdivision (c).

(k) A consumer credit reporting agency shall require proper identification, as defined in subdivision (c) of Section 1785.15, of the person making a request to place or remove a security freeze.

(l) The provisions of this section do not apply to the use of a consumer credit report by any of the following:

(1) A person or entity, or a subsidiary, affiliate, or agent of that person or entity, or an assignee of a financial obligation owing by the consumer to that person or entity, or a prospective assignee of a financial obligation owing by the consumer to that person or entity in conjunction with the proposed purchase of the financial obligation, with which the consumer has or had prior to assignment an account or contract, including a demand deposit account, or to whom the consumer issued a negotiable instrument, for the purposes of reviewing the account or collecting the financial obligation owing for the account, contract, or negotiable instrument. For purposes of this paragraph, "reviewing the account" includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements.

(2) A subsidiary, affiliate, agent, assignee, or prospective assignee of a person to whom access has been granted under subdivision (d) of Section 1785.11.2 for purposes of facilitating the extension of credit or other permissible use.

(3) Any state or local agency, law enforcement agency, trial court, or private collection agency acting pursuant to a court order, warrant, or subpoena.

(4) A child support agency acting pursuant to Chapter 2 of Division 17 of the Family Code or Title IV-D of the Social Security Act (42 U.S.C. et seq.).

(5) The State Department of Health Services or its agents or assigns acting to investigate Medi-Cal fraud.

(6) The Franchise Tax Board or its agents or assigns acting to investigate or collect delinquent taxes or unpaid court orders or to fulfill any of its other statutory responsibilities.

(7) The use of credit information for the purposes of prescreening as provided for by the federal Fair Credit Reporting Act.

(8) Any person or entity administering a credit file monitoring subscription service to which the consumer has subscribed.

(9) Any person or entity for the purpose of providing a consumer with a copy of his or her credit report upon the consumer's request.

(m)

This act does not prevent a consumer credit reporting agency from charging a fee of no more than ten dollars ($10) to a consumer for each freeze, removal of the freeze, or temporary lift of the freeze for a period of time, or a fee of no more than twelve dollars ($12) for a temporary lift of a freeze for a specific party, regarding access to a consumer credit report, except that a consumer credit reporting agency may not charge a fee to a victim of identity theft who has submitted a valid police report or valid Department of Motor Vehicles investigative report that alleges a violation of *Section 530.5 of the Penal Code*.

(N) REGARDLESS OF THE EXISTENCE OF A SECURITY FREEZE, A CONSUMER REPORTING AGENCY MAY DISCLOSE PUBLIC RECORD INFORMATION LAWFULLY OBTAINED BY, OR FOR, THE CONSUMER REPORTING AGENCY FROM AN OPEN PUBLIC RECORD TO THE EXTENT OTHERWISE PERMITTED BY LAW. THIS SUBDIVISION DOES NOT PROHIBIT A CONSUMER REPORTING AGENCY FROM ELECTING TO APPLY A VALID SECURITY FREEZE TO THE ENTIRE CONTENTS OF A CREDIT REPORT.

SEC. 3.

Section 1798.29 of the Civil Code, as added by Section 2 of Chapter 915 of the Statutes of 2002, is repealed.

SEC. 4.

Section 1798.29 of the Civil Code, as added by Section 2 of Chapter 1054 of the Statutes of 2002, 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) 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.

(e) For purposes of this section, "personal information" means 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:

(1) Social security number.

(2) Driver's license number or California Identification Card number.

(3)

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.

(4) MEDICAL INFORMATION.

(5) HEALTH INSURANCE INFORMATION.

(f) **(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.

(g) 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) E-mail notice when the agency has an e-mail address for the subject persons.

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

(C) Notification to major statewide media.

(h) Notwithstanding subdivision (g), 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.

SEC. 4.5.

Section 1798.29 of the Civil Code, as added by Section 2 of Chapter 1054 of the Statutes of 2002, 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) 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.

(e) For purposes of this section, "personal information" means 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:

(1) Social security number.

(2) Driver's license number or California identification card number.

(3) 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.

(4) Medical information.

(5) Health insurance information.

(f)

(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.

(g) 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) E-mail notice when the agency has an e-mail 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 Privacy Protection.

(h) Notwithstanding subdivision (g), 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.

SEC. 5.

Section 1798.82 of the Civil Code, as added by Section 4 of Chapter 915 of the Statutes of 2002, is repealed.

SEC. 6.

Section 1798.82 of the Civil Code, as added by Section 4 of Chapter 1054 of the Statutes of 2002, is amended to read:

§ 1798.82.

(a) Any person or business that conducts business in California, and 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 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 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) 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.

(e) For purposes of this section, "personal information" means 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:

(1) Social security number.

(2) Driver's license number or California Identification Card number.

(3)

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.

(4) MEDICAL INFORMATION.

(5) HEALTH INSURANCE INFORMATION.

(f) (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.

(g) 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) E-mail notice when the person or business has an e-mail address for the subject persons.

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

(C) Notification to major statewide media.

(h) Notwithstanding subdivision (g), 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. 6.5.

Section 1798.82 of the Civil Code, as added by Section 4 of Chapter 1054 of the Statutes of 2002, is amended to read:

§ 1798.82.

(a) Any person or business that conducts business in California, and 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 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 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) 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.

(e) For purposes of this section, "personal information" means an individual's first name or first initial and last name in combination with one or more of the following data elements, when either the name or the data elements are not encrypted:

(1) Social security number.

(2) Driver's license number or California identification card number.

(3) 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.

(4) Medical information.

(5) Health insurance information.

(f)

(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.

(g) 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) E-mail notice when the person or business has an e-mail 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 and the Office of Privacy Protection.

(h) Notwithstanding subdivision (g), 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. 6.7.

(a) Section 4.5 of this bill incorporates amendments to *Section 1798.29 of the Civil Code* proposed by both this bill and AB 779. It shall only become operative if (1) both bills are enacted and become effective on or before January 1, 2008, (2) each bill amends *Section 1798.29 of the Civil Code*, and (3) this bill is enacted after AB 779, in which case Section 4 of this bill shall not become operative.

(b) Section 6.5 of this bill incorporates amendments to *Section 1798.82 of the Civil Code* proposed by both this bill and AB 779. It shall only become operative if (1) both bills are enacted and become effective on or before January 1, 2008, (2) each bill amends *Section 1798.82 of the Civil Code*, and (3) this bill is enacted after AB 779, in which case Section 6 of this bill shall not become operative.

SEC. 7.

No reimbursement is required by this act pursuant to *Section 6 of Article XIII B of the California Constitution* because the only costs that may be incurred by a local agency or school district will be incurred because this act creates a new crime or infraction, eliminates a crime or infraction, or changes the penalty for a crime or infraction, within the meaning of *Section 17556 of the Government Code*, or changes the definition of a crime within the meaning of *Section 6 of Article XIII B of the California Constitution.*

History

Approved by Governor October 14, 2007

Filed with Secretary of State October 14, 2007

End of Document