

BILL NUMBER: SB 1386 CHAPTERED
BILL TEXT

CHAPTER 915

FILED WITH SECRETARY OF STATE SEPTEMBER 26, 2002
APPROVED BY GOVERNOR SEPTEMBER 25, 2002
PASSED THE SENATE AUGUST 30, 2002
PASSED THE ASSEMBLY AUGUST 26, 2002
AMENDED IN ASSEMBLY AUGUST 23, 2002
AMENDED IN ASSEMBLY AUGUST 5, 2002
AMENDED IN ASSEMBLY JULY 25, 2002
AMENDED IN ASSEMBLY JUNE 30, 2002
AMENDED IN ASSEMBLY JUNE 20, 2002
AMENDED IN ASSEMBLY JUNE 6, 2002
AMENDED IN SENATE MARCH 20, 2002

INTRODUCED BY Senator Peace
(Principal coauthor: Assembly Member Simitian)

FEBRUARY 12, 2002

An act to amend, renumber, and add Section 1798.82 of, and to add Section 1798.29 to, the Civil Code, relating to personal information.

LEGISLATIVE COUNSEL'S DIGEST

SB 1386, Peace. Personal information: privacy.

Existing law regulates the maintenance and dissemination of personal information by state agencies, as defined, and requires each agency to keep an accurate account of disclosures made pursuant to specified provisions. Existing law also requires a business, as defined, to take all reasonable steps to destroy a customer's records that contain personal information when the business will no longer retain those records. Existing law provides civil remedies for violations of these provisions.

This bill, operative July 1, 2003, would require a state agency, or a person or business that conducts 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 data, as defined, to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The bill would permit the notifications required by its provisions to be delayed if a law enforcement agency determines that it would impede a criminal investigation. The bill would require an agency, person, or business that maintains computerized data that includes personal information owned by another to notify the owner or licensee of the information of any breach of security of the data, as specified. The bill would state the intent of the Legislature to preempt all local regulation of the subject matter of the bill. This bill would also make a statement of legislative findings and declarations regarding privacy and financial security.

THE PEOPLE OF THE STATE OF CALIFORNIA DO ENACT AS FOLLOWS:

SECTION 1. (a) The privacy and financial security of individuals is increasingly at risk due to the ever more widespread collection of personal information by both the private and public sector.

(b) Credit card transactions, magazine subscriptions, telephone numbers, real estate records, automobile registrations, consumer surveys, warranty registrations, credit reports, and Internet Web sites are all sources of personal information and form the source material for identity thieves.

(c) Identity theft is one of the fastest growing crimes committed in California. Criminals who steal personal information such as social security numbers use the information to open credit card accounts, write bad checks, buy cars, and commit other financial crimes with other people's identities. The Los Angeles County Sheriff's Department reports that the 1,932 identity theft cases it received in the year 2000 represented a 108 percent increase over the previous year's caseload.

(d) Identity theft is costly to the marketplace and to consumers.

(e) According to the Attorney General, victims of identity theft must act quickly to minimize the damage; therefore expeditious notification of possible misuse of a person's personal information is imperative.

SEC. 2. Section 1798.29 is added to the Civil Code, 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.

(f) 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.

(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. 3. Section 1798.82 of the Civil Code is amended and renumbered to read:

1798.84. (a) Any customer injured by a violation of this title may institute a civil action to recover damages.

(b) Any business that violates, proposes to violate, or has violated this title may be enjoined.

(c) The rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under law.

SEC. 4. Section 1798.82 is added to the Civil Code, 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.

(f) 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.

(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. 5. This act shall become operative on July 1, 2003.

SEC. 6. This act deals with subject matter that is of statewide concern, and it is the intent of the Legislature that this act supersede and preempt all rules, regulations, codes, statutes, or ordinances of all cities, counties, cities and counties, municipalities, and other local agencies regarding the matters expressly set forth in this act.