

California SB 1386 – Personal Information: Privacy

SB 1386 goes into affect on July 1, 2003. Under the law, covered parties must disclose any breach of the security of personal data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

The law applies to state agencies, or a person or business that conducts business in California, that owns or licenses computerized data containing personal information.

The bill would permit the required notifications 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.

"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 organization.

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.

"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, if 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.

"Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

"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:
 - E-mail notice when the agency has an e-mail address for the subject persons.
 - Conspicuous posting of the notice on the agency's Web site page, if the agency maintains one.
 - Notification to major statewide media.

Note that existing laws regulate the maintenance and dissemination of personal information by state agencies, and require each agency to keep an accurate account of disclosures made pursuant to specified provisions. Existing laws also require a business, 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 laws provide civil remedies for violations of these provisions.

This article was summarized from the actual text of SB 1386, which is available online. Auxillium West assumes no liability for errors, omissions and/or misinterpretations arising from this summary of SB 1386.