

State of California

Franchise Tax Board-Legislative Services Bureau
PO Box 1468
Sacramento, CA 95812-1468

Telephone: (916)845-4326
ATSS: 468-4326
FAX: (916)845-5472

Legislative Change No.**02-33**Bill Number: AB 700Author: SimitianChapter Number: 02-1054Laws Affecting Franchise Tax Board: Civil Code Section 1798.29Date Filed with the Secretary of the State: September 29, 2002

SUBJECT: State Agencies Disclose Any Breach of Security of Computer Data Systems That Contain Personal Information

Assembly Bill 700 (Simitian), as enacted on September 29, 2002, made the following changes to California law:

Section 1798.29 of the Civil Code is added.

This act will require a state agency to notify a resident of California in the event their personal information has been acquired by an unauthorized person due to a breach of security of that agency's computer system.

This act defines "breach of the security of the system" as unauthorized acquisition of computerized data that will compromise the security, confidentiality, or integrity of personal information. However, it is not considered a breach of the security of the system if an employee or agent of an agency in good faith acquires personal information for purposes of the agency, provided that the information is not used or subject to further unauthorized disclosure.

This act defines "personal information" as a person'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: i) Social Security number; ii) driver's license number or California Identification Card number; or iii) account number, credit card number, or debit card number along with the required security code, access code, or password. Personal information does not include information that is legally made available to the general public from federal, state, or local government records.

This act states that notification will be made in the most expedient time possible and without unreasonable delay. If the agency maintains computerized data, but does not own the data, the agency must notify the owner or licensee of the information of the breach immediately following discovery.

This act states that notification can be delayed if a law enforcement agency determines it will impede a criminal investigation. However, notification must be made once it has been determined that it will not interfere with the investigation. Notification can also be delayed if consistent with agency measures to determine the scope of the breach and to restore the integrity of the data system.

Bureau Director

Roger Lackey

Date

October 24, 2002

This act allows notification to be made by any of the following methods: written, electronic, or substitute notice. A substitute notice can be made if the agency demonstrates that the costs to provide the notice will exceed \$250,000, or that the affected class of persons to be notified exceeds 500,000, or when the agency does not have sufficient contact information. The substitute notice will consist of all of the following: an e-mail notice when the agency has the e-mail addresses for the subject persons, the conspicuous posting of the notice on the agency's Web site, and notification to major statewide media.

This act states that any agency that maintains its own notification procedures as part of their own information security policy will be in compliance with this bill if persons are notified in accordance with those procedures and those procedures are consistent with the timing requirements of Part 4 of the Civil Code.

The provisions of this act will supersede and preempt all rules, regulations, codes, statutes, or ordinances of all cities, counties, cities and counties, municipalities, and other local agencies on the matters that are the subject of this act.

This act is effective January 1, 2003, and operative July 1, 2003.

This act will not require any reports by the department to the Legislature.