

California State Senate Bill 1386

Personal Information: Privacy Act

The "Personal Information: Privacy Act" was approved by the Governor September 25, 2002 and became effective July 1, 2003. It places new requirements on businesses that maintain computerized personal information on California residents.

The introduction to the Bill provides a concise description of the intent of the law.

"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 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 specific language of the law, contained in the California Civil Code, includes:

"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."

"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."

Certain terms are specifically defined in the law.

Breach of the Security of the System: Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business.

Personal Information: 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.

Notice: Defines acceptable forms of notice, including written, electronic, and acceptable substitute notice forms when certain financial or volume thresholds are reached.

Implications for businesses:

The provisions of this law apply to not only to businesses headquartered in California, but also to any business that conducts business in California. A fair assessment is that any business that maintains information as defined in the law is subject to the provisions of the law, whether or not the business has a physical presence in California.

Any information repository that is not protected to prevent unauthorized acquisition of the information presents a risk for the business maintaining the information. Simply building firewalls to protect against hacking does not eliminate the risks of unauthorized acquisition.

Unauthorized acquisition can occur in the following situations, among others:

1. Theft by employees with access to the information repository.
2. Inadvertent disclosure when the business does not have embedded safeguards in place to prevent accidental disclosure.
3. Secondary, unauthorized disclosure that can occur when data is removed from a supposed secure environment under legitimate circumstances but loses the security in the process of transfer.

Once an unauthorized disclosure occurs, the business is confronted with the notification provisions contained in the law. Additionally, the business could be liable for damages under the provisions of section 1798.84 quoted above.