

What is California Senate Bill 1386?

California was the first U.S. state to have an agency, the Office of Privacy Protection, dedicated to promoting and protecting the privacy rights of consumers. The State has a number of laws related to privacy and identity theft including Senate Bill 1386 (SB 1386). Since July 2003, businesses and individuals that maintain computerized data that includes specified personal information must disclose any breach of the security of that data. The legislation is designed to give companies the incentive to take proactive steps to ensure that their customers do not become victims of identity theft.

Who is affected?

Any “person or business that conducts business in California, and that owns or licenses computerized data that includes personal information.” Similar legislation exists for California government agencies. Since the legislation is designed to protect California residents, businesses outside California which conduct business in the state are also required to comply.

The law defines “personal information” as an individual’s unencrypted first and last name in combination with at least one other piece of information such as their Social Security number, driver’s license number, California ID card number; bank account number with PIN, security or other access code or credit or debit card number.

What does SB 1386 have to do with information management?

SB 1386 requires companies to disclose computer security breaches. The bill amends the California Civil Code as follows:

Section 1798.82 is added to the Civil Code, to read:

(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.

Companies with California-based customers are advised to adopt best practices for handling customer information. For example, a comprehensive privacy policy that addresses information-handling practices to take care of personal information throughout its entire life cycle, minimizing the risk of security breaches.

What do companies have to do to comply with SB 1386?

Companies can take a number of preemptive steps including familiarizing themselves with the law’s requirements should the company face a security breach, reviewing procedures for storing sensitive data to minimize the risk of a security breach, educating and training employees on proper handling of information, assessing and setting up appropriate recordkeeping systems. Companies may also wish to increase their encryption and data security systems.



If there is a security breach, companies must notify individuals immediately. The California Office of Privacy Protection suggests that notice within ten days of learning of the data security breach is sufficient. Companies should consult their legal counsel and, if necessary, local law enforcement, to ensure their notification is appropriate.

Under SB 1386, companies that fail to disclose computer security breaches become liable for civil damages and may face class action lawsuits:

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.

How can we help?

Consider Securit as your partner in information handling protocol. By ensuring that materials are safely stored and, when no longer needed, destroyed completely, onsite by Securit, companies limit the risk of a security breach. For peace of mind, contact Securit today at 1 800 697-4733.

For more information:

California Office of Privacy Protection – www.privacy.ca.gov

This document does not constitute a legal opinion or legal advice. Do not rely on any of the information in this document without first obtaining legal advice.

© Copyright 2005

