

CREDANT Solutions for SB 1386/SB 1136 Compliance

SB 1386 and SB 1136 can impact anyone doing business in California

REGULATORY OVERVIEW

SB 1386 is a California law regulating the privacy of personal information.

The law applies to an agency, person or business that conducts business in California and owns or licenses computerized "personal information." Compliance requires that these entities immediately notify any California resident if they believe the resident's unencrypted, personal information that they own or license has been disclosed.

THE COMPLIANCE CHALLENGE

Compliance with SB 1386 has become a major security issue over the past several years. Although mandated by California, the regulations apply to both California and out-of-state entities anywhere in the world that do business in California.

Adding to the law's impact is its relatively broad definition of personal information. This includes an individual's first and last name along with numbers from a Social Security account, debit or credit card, driver's license, California ID card, or bank account number. Almost anyone today has this sort of information stored in a multitude of company databases as well as PCs, laptops, handhelds, smartphones, USB drives and CD-DVDs.

At the same time, it is important to note that SB 1386 does not apply to encrypted information. Companies can avoid the reporting requirement by encrypting all personal information. They can also avoid reporting if data does not contain personal information relating to a California resident.

As a result, a significant part of compliance with SB 1386 involves encrypting and safeguarding this personal information, regardless of its location.

The recent Senate Bill 1136 will potentially modify and extend SB 1386 to establish standard content for data breach notification. This will include: A description of the incident (including date and time)—The type of information breached—The toll-free telephone number for the major credit reporting agencies for security breach notices in California.

Most significantly, SB 1136 also requires public agencies, businesses and people who are subject to California's security breach notification law to send an electronic copy of the notification to the Attorney General if more than 500 Californians are affected by a single breach. With the prospect of action by the state Attorney General facing organizations with a breach, it is even more important to ensure that information is well protected.

CREDANT SOLUTION

CREDANT encryption management solutions ensure that SB 1386 and SB 1136 encryption and security mandates are consistently and efficiently enforced – regardless of where the data resides.

ONLY CREDANT ENABLES ORGANIZATIONS TO:

- › Manage encryption and secure data across multiple endpoints from a common management platform
 - › Full Disk Encryption (FDE)
 - › Self-Encrypting Drives
 - › Policy-Based File/Folder Encryption
 - › Mobile Devices and Smartphones
 - › Removable Media
 - › Windows[®] BitLocker[™]
- › Create automatic audit trails that offer proof of end-to-end data security
- › Provide a transparent end-user interface that supports user productivity while keeping data safe
- › CREDANT provides you with a centrally-managed, highly scalable and architecturally flexible approach to manage all data endpoints. With CREDANT, organizations can:
 - › Help ensure data security, reducing the risk of insider or external attack
 - › Simplify and reduce the workload of maintaining compliance
 - › Provide confidentiality, privacy and auditing of data residing on any endpoint
 - › Integrate and manage multiple encryption solutions into a single management tool set