

# CREDANT Solutions for Compliance with the Texas Identity Theft Enforcement and Protection Act

Businesses must protect personal data and notify customers of security breaches

## CREDANT SOLUTION

*CREDANT Mobile Guardian (CMG) ensures that encryption and security requirements are consistently and efficiently enforced – regardless of where the data resides.*

### Only CMG enables organizations to:

- › Encrypt and secure data across multiple, diverse platforms from a single console.
- › 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.

*CMG provides centrally-managed, highly scalable and architecturally flexible security to manage all data endpoints. With CREDANT, organizations can:*

- › Ensure that all encryption keys are centrally generated and securely stored automatically on the server before anything is encrypted.
- › Protect data from leaving the organization unprotected on USB flash drives or other forms of removable media.
- › Safeguard data from unwarranted access, thus reducing risk of internal breaches.

## Regulatory overview

In almost every state today, statutes are now in place to help protect personal information stored and processed by computers. The Texas Identity Theft Enforcement and Protection Act is one of the strongest and most comprehensive of these laws, and new amendments have been passed recently to increase its scope and effectiveness.

As of April 1st, 2009, businesses in Texas are now required to protect all email transmissions and personal identifying information. Businesses are defined as “any person who conducts business in [the] state and owns or licenses computerized data that includes sensitive personal information.” The definition of personal identifying information is fairly broad, including name, social security number, date of birth, government-issued identification numbers, address, bank routing codes and account numbers.

The law stipulates that “a business shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect and safeguard from unlawful use or disclosure any sensitive personal information collected or maintained by the business in the regular course of business...” This includes data stored and managed on desktops, as well as laptops, note-pads, USB drives and other mobile devices.

## The compliance challenge

Breach notification is a key part of the Texas law. After discovering or receiving notification of a security breach involving personal data, businesses must “disclose any breach of system security to any resident of [the] state whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person.”

Even with proper breach notification, a court can order the defendant to make restitution to the victim for lost income and other expenses that result from the theft of personal data. Civil penalties for each security breach per individual can range from a minimum of \$2,000 to \$50,000.

## CREDANT

More than 700 enterprises and government agencies -- including 50 of the Global 500 – rely on CREDANT to ensure security compliance, protect their brand and enhance IT and end-user productivity.