

CREDANT Solutions for Compliance with FSS 817.5681

Breach of unencrypted private data requires notification within 45 days.



CREDANT SOLUTION

CREDANT Mobile Guardian (CMG) provides unique levels of trust, control and transparency to demonstrate compliance for FSS 817.5681 – but without disrupting operational processes or the user experience.

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.
- › Provide all the necessary audit reports required by FSS 817.5681 policies.
- › Protect data from leaving the organization unprotected on USB flash drives or other forms of removable media.
- › Protect data from unwarranted access, thus reducing risk of internal breaches.

Regulatory overview

In line with breach notification laws recently passed in other U.S. states, Florida State Statute 817.5681 requires notification by companies doing business in Florida if “personal information was, or is reasonably believed to have been, acquired by an unauthorized person.”

Personal information includes items such as a social security number and driver’s license number, as well as a credit card number or debit card number, in combination with any codes or passwords that would permit access to an individual’s financial account.”

The law applies to anyone doing business in the state. Notification must be made no later than 45 days.

The compliance challenge

The statute applies to any “computerized data in a system that includes personal information.” Along with desktops, this would include laptops, notepads, USB drives and other mobile devices.

Failure of notification results in rigorous and rapidly escalating fines: “\$1,000 for each day the breach goes undisclosed for up to 30 days and, thereafter, \$50,000 for each 30-day period or portion thereof for up to 180 days.”

Significantly, though, the statute applies only to unencrypted data. Under the Florida statute, a company is not required to report a data breach if the compromised information is encrypted. Therefore, the challenge for companies is to develop proper encryption for private data on endpoint devices, backed by the ability to prove encryption if any devices are lost, stolen or compromised.

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.