

CREDANT Solutions for Compliance with the Utah Code § 13-44-101

Requires Investigation and Notification of Unencrypted Personal Information

REGULATORY OVERVIEW

Similar to other state's security breach legislation, the code's purpose is to address the integrity of consumer credit data and impart the obligation to protect the data upon any person that conducts business in the state of Utah and maintains personal information on its residents.

The law mandates that once aware of a breach, the person who owns or licenses the computerized data must a) "conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused for identity theft or fraud purposes," and b) "if an investigation under previous section (a) reveals that the misuse of personal information for identity theft or fraud purposes has occurred, or is reasonably likely to occur, the person shall provide notification to each affected Utah resident."

Through the above processes, if the investigation reveals misuse, or potential misuse, of personal information for personal identity theft or fraud purposes that have occurred or are likely to occur, the person that conducts business will need to provide victims a notification in the most expedient time possible without unreasonable delay via written, electronic or telephonic media, or a publication in a newspaper of general circulation.

A person that conducts business in Utah who violates the 'Protection of Personal Information Act' provisions is subject to a civil fine of no greater than \$2,500 for violations concerning one specific consumer, and no greater than \$100,000 in the aggregate for related violations concerning more than one consumer. However exemptions to Utah Code § 13-44-101 do exist if the personal data that was lost, stolen or accessed by an unauthorized individual is:

- › Encrypted data or rendered unreadable
- › Publicly available (i.e. Government data)
- › Deemed immaterial

THE COMPLIANCE CHALLENGE

The statute applies to any person conducting business and who owns or licenses computerized data that contains personal information of Utah residents, including desktops, laptops, USB drives and other removable media. However, the statute only applies to unencrypted data. Under the Utah Code § 13-44-101, if data is encrypted, it's not required to report data breach. Therefore, the real compliance challenge is really about ensuring proper encryption of computerized personal information.

CREDANT SOLUTION

CREDANT encryption management solutions ensure that Utah Code § 13-44-101 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