

CREDANT Solutions for Compliance with the New York State Information Security Breach and Notification Act

Updated Act More Clearly Defines Compliant Data Encryption



REGULATORY OVERVIEW

The New York State Information Security Breach and Notification Act, passed in 2009, amended the State Technology Law (Section 208) and the General Business Law (Section 899-aa) to more clearly define the parameters of what constitutes a data breach. Most state information security laws grant organizations exemption from breach notification requirements if they are able to prove that the breached information was encrypted.

However, the updated version of the New York Act now more clearly defines what constitutes “encrypted” data, making it more difficult for organizations to claim notification exemption. The Act defines encryption as private information, in storage or in transit, protected by encryption technology that is generally recognized in the IT industry, including:

- › The National Institute of Standards and Technology
- › The International Standards Organization
- › The Payment Card Industry Security Standards Council

One caveat is that if private information is acquired along with the key needed for decryption, the acquired data is not considered to have been “encrypted,” and the organization involved is subject to notification requirements.

Under the new Act, a data breach is defined as unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of private information maintained by a state entity. A violation happens when the information breached includes private information (a person’s name, symbol or mark) in combination with any one or more of the following unencrypted items:

- › Social Security number
- › Driver’s license number or non-driver identification card number
- › Account number, credit or debit card number

Exemptions include data that is:

- › Legally available to the general public from federal, state or local government records
- › Acquired in “good faith” on behalf of the state agency and is not used for unauthorized disclosure

The judiciary and municipalities are not considered to be state entities.

CREDANT SOLUTION

CREDANT encryption management solutions ensure that New York State Information Security Breach and Notification Act 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

CREDANT Solutions for Compliance with the New York State Information Security Breach and Notification Act

Updated Act More Clearly Defines Compliant Data Encryption



THE COMPLIANCE CHALLENGE

The Act requires state entities, individuals and businesses conducting business in NY that own or license computerized private information to disclose any breach to New York state residents, as well as:

- › The New York State Attorney General
- › The NYS Office of Cyber Security & Critical Infrastructure Coordination
- › The Consumer Protection Board

In addition to the above, state entities must also notify non-residents, and they must notify consumer reporting agencies if more than 5,000 residents are affected.

CREDANT

CREDANT is the Trusted Expert in Data Protection. Founded in 2001, CREDANT enables organizations to control, manage and protect data on vulnerable laptops, desktops, PCs, Macs, smartphones and removable media devices. Protecting sensitive information on more than 7 million endpoints at over 1,000 global customers, CREDANT provides the most comprehensive mobile data protection and management platform.

For more information, visit www.credant.com.