MORRISON | FOERSTER

Legal Updates & News

Bulletins

New Massachusetts Regulation Requires Encryption of Portable Devices and Comprehensive Data Security Programs

September 2008
by Miriam Wugmeister, Charles H. Kennedy

Related Practices:

- Financial Services Law
- Privacy and Data Security

Privacy and Data Security Update, September 23, 2008

As of January 1, 2009, all companies that own, license, store or maintain personal information concerning any Massachusetts resident must take comprehensive measures to protect that information from unauthorized access, disclosure or misuse.

Although the new regulations impose a broad range of requirements, the most pressing compliance issue for many organizations will be the new obligation to encrypt all personal information of Massachusetts residents that is stored on any portable device which includes laptops, flashdrives, Blackberries or cell phones (to the extent feasible) that is transmitted over the Internet or by wireless connections.

Although laptop encryption is becoming more common, frequent reports of losses of laptops containing unencrypted personal data demonstrate that many organizations have not completed the transition to encrypted storage on their portable devices. Similarly, some of the best publicized losses of personal data, including those that resulted in massive identity theft, have occurred because of exploitation of insecure wireless connections.

Even organizations that have no facilities or personnel in Massachusetts should anticipate that they will be subject to the regulations if they maintain personal information of any Massachusetts residents. Personal information is defined as: first name and last name or first initial and last name in combination with Social Security number; driver's license number or state-issued identification card number; and financial account or credit or debit card number with or without any required security code, access code, personal identification number or password that would permit access to an individual's financial account.

Besides the new encryption obligation, the regulations require entities that maintain personal information of Massachusetts residents to:

- designate an employee to maintain security program;
- identify paper, electronic and other storage media (including laptops) that contain personal information;
- conduct risk assessments;
- develop and implement, according to the results of those risk assessments, a program that ensures the security of all records – whether maintained in paper or electronic form – that contain personal information of Massachusetts residents;
- document the security program;
- include in the security program:
    - processes for granting and withdrawing access privileges,
    - ensuring proper authentication of users,
    - appropriate access controls,
    - methods of assigning passwords,
    - maintaining up to date firewalls and malware protections,
    - training all affected employees and
    - disciplining employees for violations of the security program;
- implement physical access controls and develop a written procedure;
- limit the amount of personal information to that which is reasonably necessary to accomplish the

purpose for which the personal information was collected;
- limit the amount of time that personal information can be retained to only the time necessary to accomplish the purpose for which personal information was collected;
- limit access to only those individuals who need access in order to accomplish their job duties;
- regularly monitor compliance with the security program;
- conduct at least annual reviews of the security program and measures; and
- document response taken in connection with any security breach.

The new regulations also will require all affected organizations to review their relationships with service providers that have access to personal information of Massachusetts residents. Specifically, organizations must:

- conduct due diligence of service providers to ensure that they have the capacity to protect personal information;
- enter into contracts that require service providers to protect personal information; and
- obtain a certification from each service provider that it has a written, comprehensive information security program that complies with the new Massachusetts regulations.

Also, a Nevada statute, scheduled to take effect on October 1, 2008, will require encryption by entities doing business in that state of all personal information leaving an organization's system and transmitted over electronic networks. Taken together, the Nevada and Massachusetts enactments go a long way toward moving encryption from a best practice to a nationwide legal obligation. Moreover, the Massachusetts regulations go significantly further than any other state law or regulation by codifying many additional elements which have been best practice with respect to data security up until now.