

NEW DATA & IDENTIFY THEFT REGULATIONS CONDOMINIUM MANAGERS MUST COMPLY

Moira Casey

Identity theft can happen to anyone. The phone rings and a collection agency demands that you pay past-due accounts for goods you never ordered. The supermarket refuses your checks because you have a history of bouncing them. But you have always paid bills on time. What has happened? Identity Theft.

Massachusetts has become one of the most aggressive states in the country regarding protecting personal data. In November 2008, The Massachusetts Office of Consumer Affairs & Business Regulations (“OCABR”) adopted a new Massachusetts data-security law, Mass.Gen.L. ch. 93H and its implementing regulations, 201CMR 17.00. The purpose of the regulations are to (1) ensure the security and confidentiality of personal information; (2) protect personal information against threats or hazards and (3) protect personal information against unauthorized access or use that could create a substantial risk of identity theft or fraud. The new regulations were designed to combat a recent epidemic of corporate data breaches and identity theft in the state. There are massive and well publicized incidents of data loss at area companies including the 2006 theft of some 45 million credit card numbers from Framingham, MA based TJX and the revelation that intruders had placed credit and debit card scooping malware on hundreds of servers owned by Hannaford Bros. Supermarket chain.

OCABR established March 1, 2010, as the new deadline, by which businesses must fully comply with the new regulations. OCABR extended the prior compliance deadline of January 1, 2010 because of the challenges caused by the current economic climate and businesses needing additional time to better understand what is required to protect customer data.

Management Companies Subject to the New Regulations

The Massachusetts regulations are extremely broad and no industry sector or business size that has personal information, as defined, is exempted from these regulations. Personal information is defined as the name of a Massachusetts resident in combination with any of the following: (1) Social Security Number; (2) driver’s license number or state-issued identification number; or (3) a financial account number, or credit or debit card number, with or without any required security code, access code, or PIN that would allow account access. Many property management companies offer the convenience of a direct payment program. A management company’s receipt of a unit owner’s name, together with bank account information, subjects the property manager to the new regulations. Furthermore, if the management company employs one person, they are required to keep W-4 and I-9 forms and these forms also subject the company to the new regulations.

A company's obligation under Chapter 93H is triggered by a "breach of security". This is an unauthorized acquisition for use of personal information regarding a Massachusetts resident that creates a substantial risk of identity theft or fraud. Upon learning of a breach of security, the Company must promptly notify each affected Massachusetts resident, the Attorney General and OCABR. The notice must contain specific information, including how the affected residents can request a security freeze with respect to his or her consumer reports, and what steps the Company has taken or plans to take in response to the security breach. The new regulations are intended to reduce the risks of data-security breaches.

Serious Consequences for Failure to Comply

If you do not comply with the new regulations and a breach occurs, the state will most certainly view you as negligent. Fines start at \$5,000 and treble damages can apply. Potential fines for failure to report a breach or for improper disposal of records such as old computers and paper can be \$50,000 plus legislative and investigative costs. Failure to comply with the new regulations may have serious consequences.

Chapter 93H authorizes the Massachusetts Attorney General to remedy a violation of the statute by bringing an action under Mass.Gen.L.ch.93A ("Chapter 93A"), which prohibits unfair and deceptive acts and practices. Chapter 93A provides for civil penalties, awards of multiple damages and attorneys' fees.

Further, although Chapter 93H does not refer to a private right of action, Massachusetts courts might interpret the statute to confer such a right, either by allowing a resident to sue directly under Chapter 93H or by allowing a private lawsuit under Chapter 93A based on a company's failure to comply with Chapter 93H.

Steps and Costs to Compliance

With the March 1st deadline looming, companies are scrambling to make sense of just what needs to be done and where the security controls they installed for previous regulatory requirements may or may not fit into the new regulations. Many experts are reasonably confident that most companies will survive these new regulations unscathed. Many of the provisions are basic best practices and industry standards that have been required for years. However, this does not mean that you can ignore the new regulations and companies need to take the following steps by March 1, 2010:

- Have in place a comprehensive written information security program ("WISP") that reflects (1) the size, scope and type of business; (2) the amount of resources available to the business; (3) the amount of stored information maintained by the business; and (4) the sensitivity of the information.
- Ensure that the WISP protects personal information in both paper and electronic forms.

- Have in place protocols to evaluate the WISP, to discipline employees who violate the WISP and to ensure that terminated employees are prevented from accessing personal information.
- Take reasonable steps to ensure that third party vendors are protecting personal information.

After understanding the scope of each Company's individual security plan, each business should designate an employee to implement, supervise and maintain the plan. This designated employee shall be responsible for initial implementation of the plan, training employees, and regular testing of the plan's safeguards, and evaluating the ability of service providers to implement their own security plan.

The new regulations make Massachusetts one of only two states including Nevada that require all companies to encrypt data sent over the internet or saved on laptops or flash drives, and encrypt wirelessly transmitted data. Only 20 to 30 percent of companies already own the software needed to protect the data on laptop hard drives and wireless networks. OCABR has estimated that average small business with 10 employees will need to spend about \$3,000 up front on the required software and up to \$500 a month for ongoing administration while bigger organizations could end up spending hundreds of thousands of dollars. Companies will also be required to deploy up-to-date firewalls to create "an electronic gatekeeper" between the data and the outside world that only allows authorized users to access or transmit data.

OCABR announced on August 17th adjustments to the regulations that maintain protections and also reinforce flexibility in compliance by small businesses. The updated regulations make clear that their approach to data security is a risk-based approach that is especially important to small businesses that may not handle a lot of personal information about customers. Under a risk-based approach, a business, in developing a written security program, should take into account its size, nature of its business, the kinds of records it maintains, and the risk of identity theft posed by its operations. A public hearing on the regulations will be held on Tuesday, September 22, 2009 at 10:00 a.m. at the Transportation Building, 10 Park Plaza, Boston, MA.

The new adjustments do not change the fact that Property Managers need to start preparations to ensure compliance with the regulations.

Moira Casey, Esq. is Director of Human Resources with the law firm of Marcus, Errico, Emmer & Brooks, PC in Braintree, MA.