NEWSSTAND

March 1, 2010: Massachusetts Security Regulation Affecting All Companies with Personal Information of Massachusetts Residents

Winter 2010
Mark E. Schreiber, Theodore P. Augustinos, Socheth Sor

Under the Massachusetts Security Regulation (201 CMR 17.00) (the Regulation) promulgated by the Massachusetts Office of Consumer Affairs and Business Regulation (OCABR), every person or company that owns or licenses certain personal information about a Massachusetts resident must develop, implement, maintain and monitor a comprehensive written information security program (WISP).

The applicability of the Regulation extends to any company that has personal information of Massachusetts residents, whether or not the company is doing business in Massachusetts. The Regulation does not exempt any industry, sector or out-of-state business, and does not exempt a de-minimus number of Massachusetts customers, employees or other residents.

The Regulation protects the personal information of Massachusetts residents, which means the first name and last name or first initial and last name in combination with any one or more of the following of a Massachusetts resident: Social Security number; driver's license number or state-issued identification card number; or financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, which would permit access to a resident's financial account.

Standards for the Protection of Personal Information
The WISP must be reasonably consistent with industry standards and is required to contain administrative, technical and physical safeguards to ensure the security and confidentiality of records containing personal information. The provisions of the Regulation concerning WISPs are both broad and very granular at the same time and effectively demand an entire systems review as well as policy and other reconfigurations where necessary. In its WISP, a person or company must, among other things, do the following:

- Identify and evaluate internal and external risks;
- Regularly monitor employees' access to personal information;
- Block terminated employees' access to documents, devices and other records that contain personal information;
- Take all reasonable steps to ensure third-party service providers' compliance with the regulations;
- Review security measures annually, and update the WISP when there is a material change in the business operations;

- Develop and maintain a procedure for actions taken in response to any breach of security;
- Train employees about and discipline employees for violation of the policy; and
- Designate one or more employees to maintain, supervise and implement the WISP.

Computer Security Requirements
The WISP must also address the establishment and maintenance of a detailed computer security program, which includes the following as they pertain to personal information of Massachusetts residents:

- Encryption of all transmitted records and files, to the extent technically feasible, containing personal information that is stored on laptops and other portable devices and/or will travel across public networks or wirelessly;
- Secure user-authentication protocols and access-control measures, including control over user identifiers, passwords and access;
- A system for monitoring unauthorized use; and
- Up-to-date firewalls, anti-virus definitions and anti-malware programs.

Ensuring Vendor Compliance
The issue of third party vendor compliance is an equally important one. As noted above, companies must take all reasonable steps to select and retain third party service providers with access to the personal information of Massachusetts residents that are capable of complying with the Regulation. Companies with contracts already in place before March 1, 2010 have a two-year grace period to March 1, 2012 to amend their contracts with third party service providers to require them to implement and maintain security measures for personal information in accordance with the Regulation. The two-year grace period applies only to contracts that have been entered into before March 1, 2010. Contracts entered into after March 1, 2010 must contain a provision requiring the third party vendor to maintain appropriate security measures for personal information. Given that many contracts renew automatically, many companies are beginning the process of adding security provisions to existing contracts now.

Enforcement
In an effort to ease the burden on small businesses, the OCABR stresses the notion that there is no one-size-fits-all WISP. Compliance with the Regulation will be judged on a case-by-case basis to take into account the following factors: (i) the size, scope and type of business handling the information; (ii) the amount of resources available to the business; (iii) the amount of stored data; and (iv) the need for security and confidentiality of both consumer and employee information. This risk-based approach brings the Regulation in line with both the enabling legislation and applicable federal law, including two rules promulgated by the Federal Trade Commission: the Red Flags Rule, effective June 1, 2010, which require creditors and financial institutions to have a written Identity Theft Prevention Program to detect warning signs of identity theft and fraud, and the Gramm-Leach-Bliley Safeguards Rule (16 CFR Part 314), which requires financial institutions to have a security plan to protect personal consumer information.

As compliance is evaluated on a case-by-case basis, a WISP must be customized for each business. Deficiencies in compliance after March 1, 2010, especially in the event of a data

breach, are sure to draw attention by regulators and perhaps by civil litigants, although no enforcement guidelines have yet been issued.