Massachusetts' Data Security Regulation: Important Deadline Approaching

The deadline for compliance with a key requirement of the Massachusetts Data Security Regulation, 201 CMR 17.00 *et seq.* (the "Regulation") is less than a month away. The Regulation requires that by March 1, 2012, all entities subject to the Regulation must require their respective "service providers" (as defined below) to implement and maintain appropriate security measures to protect personal information that are consistent with the Regulation and applicable federal regulations.

Who is subject to the Regulation?

Regardless of whether an entity maintains a place of business in Massachusetts, it must comply with the Regulation if it receives, stores, maintains, processes, or otherwise has access to personal information of Massachusetts residents in connection with the provision of goods or services or in connection with employment. The term "personal information" is defined to mean a person's name in combination with certain sensitive information, such as a Social Security number, driver's license number or other state-issued ID number, financial account number, or debit or credit card number. A full discussion of the Regulation can be found in our previous alert, which can be accessed here.

Requirements for overseeing services providers

The Regulation requires that subject entities oversee service providers by taking reasonable steps to select and retain service providers that are capable of maintaining appropriate security measures to protect personal information. In addition, those service providers must contractually agree to implement and maintain appropriate security measures to protect personal information consistent with the Regulation and applicable federal regulations. Note that such oversight responsibilities apply only to "service providers," defined as "any person that receives, stores, maintains, processes, or otherwise is permitted access to personal information through its provision of services directly to a person that is subject to this regulation."

The approaching deadline

The Regulation provides that contracts with service providers entered into on or after March 10, 2010 must include provisions requiring the service provider to implement and maintain security measures for personal information consistent with the Regulation. The Regulation contains a two-year grace period for contracts entered into prior to March 1, 2010, which expires as of March 1, 2012.

The penalties for non-compliance with the Regulation are enforced through the Massachusetts Consumer Protection Statute (M.G.L. c. 93A), and violators may face the risk of a civil penalty of up to $5,000 for each violation, plus reasonable costs of investigation and litigation of such violation (including reasonable attorney's fees). Furthermore, entities that fail to comply with the Regulation may be subject to additional liability and penalties under the Massachusetts Consumer Protection Statute (M.G.L. c. 93A), which prohibits unfair and deceptive trade practices.

If you would like to learn more about the issues raised by this update, please contact your usual Ropes & Gray attorney or a member of our privacy and data security practice group, including: David M. McIntosh, Mark P. Szpak, Michele M. Garvin, Timothy M. McCrystal, Deborah L. Gersh, Peter C. Erichsen, and Adinna A. Smith.