

## Massachusetts' Data Protection Regulations to Have Nationwide Impact on Financial Services Employers

Like the changes to courts' interpretations of the New York anti-discrimination laws, Massachusetts' amendments to its data privacy laws could have far-reaching impact for employers. In August 2009, the Massachusetts Office of Consumer Affairs and Business Regulation issued a new version of its proposed regulations on data security of personal information. After several iterations of proposed regulations, it is the August 2009 version of the regulations that took effect on March 1, 2010. Notably, the regulations govern any employer that "receives, stores, maintains, processes, or otherwise has access to personal information" of any Massachusetts resident, regardless of whether the employer has any other ties to the state. Moreover, "personal information" is broadly defined to include the retention of a Massachusetts resident's name in connection with any of the following other information: social security number, driver's license, or financial account number or credit or debit card number. Given the breadth of the definitions in the regulations, any employer who employs Massachusetts residents, and thus retains personal information about those residents, is obliged to meet the standards of protection set forth in the regulations.

The regulations require employers to create a written comprehensive information security program, which focuses on the specific data security risks of its company and the type of information it stores and maintains. Specifically, the regulations require employers to do the following: designate an employee to maintain the security program; conduct risk assessments as to the company's safeguards in protecting personal information; develop security policies for the storage, access, and transportation of personal

information; impose disciplinary measures for violations of the program rules; prevent terminated employees from accessing records containing personal information; take reasonable steps to ensure that third-party vendors can protect personal information; restrict physical access to records containing personal information; and routinely monitor and adapt the program to limit risks of improper use of personal information.

Additional comprehensive requirements exist if the personal information is electronically stored or transmitted. For employers who electronically store information deemed personal under the regulations, the employer must do the following: ensure that there are security protocols in place that govern access to electronically stored information, including control of user ID's and the selection and distribution of passwords; restrict access to private records to those who need that information and issue unique identification and passwords to those employees; encrypt any electronically stored personal information; monitor the systems for unauthorized access or use of personal information; routinely update security agent software so that the software is reasonably up to date; and educate and train employees as to the proper use of the computer security system.

Even if an employer has only a few Massachusetts employees, employers are arguably required to develop company-wide policies that comply with the new regulations. Employers who retain Massachusetts residents should immediately consider whether their information security and electronic security protocols are up to date and comply with the extensive requirements listed in Massachusetts new regulations. While it is unclear how the courts will ultimately decide what constitutes a "violation" of these regulations, it is clear that a court can impose a \$5,000 civil penalty for each violation, however that term is ultimately defined. Accordingly, it is imperative that employers ensure that they have examined their policies and update them as necessary to satisfy the substantial Massachusetts requirements.