MASSACHUSETTS DATA SECURITY REGULATIONS EFFECTIVE ON MARCH 1, 2010

The new Massachusetts data security regulations (the "Regulations") became effective on March 1, 2010.[1] While the Regulations have been modified several times since their initial release in 2008, our previous client memoranda[2] detail most of its current requirements. The Regulations are arguably the most detailed and onerous state or federal data security regime in the United States.

Who Must Comply?

The Regulations apply to any business that receives, stores or maintains a combination of certain personally identifying information of Massachusetts residents that is not publicly available ("Personal Information").[3] Among other types of businesses, pooled investment vehicles, investment managers, and broker-dealers are subject to the Regulations if they receive Personal Information of investors, customers or employees who are Massachusetts residents.

What Are the Requirements?

A business subject to the Regulations must develop, implement and maintain a written comprehensive information security policy that is tailored to the size, scope and resources of the business, and to the amount of Personal Information to be safeguarded. Among other requirements, the comprehensive information security policy must (i) designate one or more employees to maintain the policy; (ii) specify that there will be ongoing employee training about the policy and discipline of employees who violate the policy; (iii) include procedures to reasonably monitor employees and computer systems; (iv) require the oversight of service providers through contract provision requirements and due diligence in selecting service providers; (v) specify that computer systems must employ password protection and/or two-factor authentication; (vi) require encryption of Personal Information that is transmitted over public networks or wirelessly; (vii) require encryption of Personal Information stored on laptops and other portable devices to the extant technically feasible; and (viii) require the use of software that employs malware protection and reasonably up-to-date patches and virus definitions, and institute procedures for staying current on security updates.

---

1 201 CMR 17.00 et seq.

2 http://www.willkie.com/files/tbl_s29Publications%5CFileUpload5686%5C2732%5CRecent_State_Data Privacy_Laws.pdf; http://www.willkie.com/files/tbl_s29Publications%255CFileUpload5686%255C3090%255CMassachusetts%2520Again%2520Revises%2520Its%2520Data%2520Security%2520Regulations.pdf

3 The Regulations' definition of "personal information" includes a Massachusetts resident's first and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (1) Social Security number; (2) driver's license number or state-issued identification card number; or (3) financial account number, 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 the resident's financial account.

How to Comply?

A business should first determine if it has Personal Information of Massachusetts investors, customers or employees. If so, the business should have a comprehensive written information security program that includes each of the required elements, including those described above; implement that program; and should periodically review how the firm is meeting its obligations under the Regulations.

An important part of that process includes conducting a sufficient level of due diligence with respect to whether service providers with access to Personal Information of the firm's Massachusetts customers, investors or employees are complying with the Regulations, and adding the required data security compliance language to contracts with service providers executed after March 1, 2010. Existing contracts executed with service providers prior to March 1, 2010 will have to be modified to include the required data security compliance language by March 1, 2012.

* * * * * * * * * * * * * * *

If you have any questions regarding this memorandum, please contact Martin R. Miller (212-728-8690, mmiller@willkie.com) or Marc J. Lederer (212-728-8624, mlederer@willkie.com), or the Willkie attorney with whom you regularly work.

Willkie Farr & Gallagher LLP is headquartered at 787 Seventh Avenue, New York, NY 10019-6099. Our telephone number is 212-728-8000 and our facsimile number is 212-728-8111. Our website is located at www.willkie.com.

March 15, 2010