Compliance Corner

Data Security Requirements under Massachusetts Law

*— By: Julia B. Jacobson and James G. Snell, Bingham LLP**

In 2009, Massachusetts adopted a new data security breach law (M.G.L. c. 93H) and regulations thereunder (201 CMR 17) (together, the "Massachusetts Law") which are designed to protect the personal information of Massachusetts residents. The Massachusetts Law, which went into effect on March 1, 2010, applies to any business that receives, stores, maintains, processes or otherwise has access to personal information about a Massachusetts resident. Following is a brief overview of how the Massachusetts Law applies to investment advisers.

Although they have some points of overlap, the Massachusetts Law is much more specific than the two primary federal data security regulations applicable to investment advisers: *i.e.,* Securities and Exchange Commission's (SEC) Regulation S-P (17 CFR 248) applicable to SEC-registered investment advisers and the Federal Trade Commission's (FTC) "Safeguards Rule" (16 CFR 314), which covers investment advisers not registered with the SEC. Some of the more prominent differences between the Massachusetts Law and Regulation S-P and/or the FTC's Safeguards Rule are highlighted below.

Scope of the Massachusetts Law

An investment adviser does not need to be located in Massachusetts or to have an ongoing customer relationship with a Massachusetts resident for the Massachusetts Law to apply; if the investment adviser has any personal information, whether in paper or electronic form, about a client, investor, employee, or other person residing in Massachusetts, it is required to comply with the Massachusetts Law.

Personal Information

The Massachusetts Law requires an investment adviser to protect personal information, which is defined as a Massachusetts resident's "first name and last name or first initial and last name" combined with (a) social security number, (b) driver's license or state-issued identification number, or (c) "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 a resident's financial account" (201 CMR 17.02).

Regulation S-P and the Safeguards Rule each cover a different set of information about individual clients that potentially overlaps with the personal information covered by the Massachusetts Law:

- Regulation S-P's 'safeguard rule' requires a registered investment adviser to safeguard *"customer records and information"* from unauthorized use or disclosure (17 CFR 248.30(a)). A customer is someone to whom an investment adviser provides financial products or services primarily for "personal, family or household purposes" and with whom an investment adviser has a "continuing relationship" (*e.g.,* enters into an advisory contract with customer, acts as custodian of customer securities or IRA) (17 CFR § 248.3(j)-(k)). (In 2008, the SEC released proposed amendments to Regulation S-P (the "Proposed Amendments") that, among other changes, expand the scope of information protected and how it must be protected (SEC Release No. 34-57427). Although the Proposed Amendments have not yet been finalized, they offer some indication of the SEC's intentions with respect to the protection of personal information. Accordingly, while this article will focus on Regulation S-P as now in effect, requirements of the Proposed Amendments are highlighted as appropriate and readers should keep in mind that Regulation S-P may change because of the Proposed Amendments.)
- The FTC's Safeguards Rule covers *"customer information,"* which is defined as "personally identifiable financial information" provided by "an individual who obtains or has obtained a financial product or service from [the adviser] that is to be

Continued on page 13

used primarily for personal, family, or household purposes." (16 CFR 313.3(n)).

Personal information for purposes of the Massachusetts Law, as well as the SEC and FTC regulations, does not include publicly-available information or information lawfully obtained from a federal, state, or local government record.

Comprehensive Information Security Program

The data security obligations under Regulation S-P are somewhat vague: a registered investment adviser is required to "adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information" (17 CFR 248.30). For unregistered investment advisers, the FTC's Safeguards Rule is more robust, requiring a written information security plan that must include assessment of safeguards in place to protect personaly identifiable financial information, risk assessment and implementation of new safeguards as needed to minimize risk, employee training, testing and monitoring of data security systems and contractual requirements for service providers to maintain systems that protect personally identifiable financial information. The Proposed Amendments also require that an investment adviser implement an "information security program."

Like the FTC's Safeguards Rule and Proposed Amendments, the Massachusetts Law requires a written information security plan but is more specific about what the plan must include, particularly with respect to electronic storage and transmittal of personal information.

The Massachusetts Law requires a "comprehensive information security program" ("CISP") that is "appropriate" to: the size and type of business, resources available to devote to data security, the type and amount of personal information that the business has stored, and the "need for security, and confidentiality of consumer and employee information" (201 CMR 17.03). A CISP must be based on analyses of internal and external security and confidentiality risks for electronic, paper, or other records containing personal information about a Massachusetts resident.

Specific requirements for a CISP include:

- designating the employee(s) responsible for maintaining the CISP, monitoring (at least annually) its effectiveness in protecting personal information and upgrading the security practices as needed to address "reasonably foreseeable internal and external risks" to the security of personal information;
- establishing and enforcing security policies for employees' storage, access and transportation of records containing personal information outside of the business premises and for preventing terminated employees from accessing such records;
- restricting physical access to records containing personal information and storing such records in locked facilities, storage areas, or containers;
- training employees (including temporary and contract employees) on how to protect personal information;
- restricting employee access to personal information to those who need it for performance of their job duties;
- describing disciplinary measures for employee violations of the CISP's policies and procedures; and
- documenting responses to any security breach and conducting "mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information."

The Massachusetts Office of Consumer Affairs and Business Regulation ("OCABR", the state agency charged with enforcing the Massachusetts Law), published special guidance for "small businesses" about how to implement a CISP, which is available at http://www.mass.gov/ocabr/docs/idtheft/sec-plan-smallbiz-guide.pdf.

Electronic Storage and Transmittal: With respect to computer security *(i.e.,* the electronic storage and transmittal) of personal information, the Massachusetts Law is quite detailed and its requirements are more robust than any provision of Regulation S-P, the Proposed Amendments, or the FTC's Safeguards Rule.

A CISP must include at least the following components with respect to computer security:

- user authentication (*e.g.,* user IDs, secure passwords and "unique identifier technologies" to create them, blocking users after multiple failed access attempts);
- access control protocols (*e.g.,* restrict access to personal information to employees);
- encryption of all wirelessly transmitted personal information (data is encrypted if it undergoes a "transformation … into a form in which meaning cannot be assigned" (201 CMR 17.02));
- encryption of personal information sent over the Internet (*e.g.*, via email);
- regular monitoring of systems to identify unauthorized use of or access to personal information;
- encryption of data and documents saved on laptops, flash drives and other portable devices (*e.g.,* for employees who travel or telecommute);

Continued on page 14

continued from page 13

- "up-to-date" firewall and malware/virus protection; and
- employee training on electronic storage and transmittal of personal information.

In guidance from OCABR, all of these computer security requirements apply to a business if they are "technically feasible" through a reasonably available technological means (see *Frequently Asked Question Regarding 201 CMR 17.00* at http://www.mass.gov/ocabr/docs/idtheft/201cmr17faqs.pdf).

Use of Third-Party Service Providers: Consistent with the FTC's Safeguards Rule, the Massachusetts Law requires an investment adviser to (i) take "reasonable steps" to evaluate and select third-party service providers (*e.g.,* pricing agent, proxy voting agent, and/or tax/accounting services) that have or can implement systems for safeguarding personal information, and (ii) contractually require third-party service providers to maintain or implement and update data security systems as appropriate. While Regulation S-P does not contain a similar requirement, the Proposed Amendments do.

Responding to Data Security Breach

The Massachusetts Law specifies how an investment adviser must respond to a "breach of security," which is defined as "the unauthorized acquisition or unauthorized use of …data … that creates a substantial risk of identity theft or fraud against a [Massachusetts] resident…" The response must be documented and a "post-incident review of events and actions taken, if any to make changes in business practices relating to protection of personal information" is mandated (201 CMR 17.03(j)).

An investment adviser that has experienced a data security breach also must "as soon as practicable and without unreasonable delay" provide written notice to the Massachusetts Attorney General and the Director of OCABR that details the date of the breach, actions taken to address the breach and how many people were affected by the breach. (A sample notice is available at http://www.mass.gov/ago/docs/consumer/93h-sampleletter-ago.pdf). Each affected Massachusetts resident also must receive written notice of his/her right to obtain a police report, how he/she can request a security freeze on his/her credit reports and the information needed to request a security freeze. (The Attorney General's sample notice to individuals is available at http://www.mass.gov/ago/docs/consumer/93h-sampleletter-residents.pdf.)

The FTC's Safeguards Rule is less specific about how to respond to a data security breach—it requires that an investment adviser respond to "attacks, intrusions, or other systems failures" (16 CMR 314.4(b)(3))—and does not require notification to regulatory authorities or affected individuals. Regulation S-P does not provide any direction on responding to a data security breach but the Proposed Amendments require that an investment adviser notify the SEC if an affected individual is likely to experience "substantial harm or inconvenience" (Proposed Regulations, §248.30a(4)(v)).

As described above, the Massachusetts Law imposes some of the most stringent data security requirements among state and federal laws. Massachusetts is not, however, the only state with detailed data security requirements; for example, California and Nevada also have enacted fulsome data security laws. Given the recent focus on and increase in enforcement of data privacy and security laws by the SEC, FTC and state regulators, as well as the direction taken by the SEC in the Proposed Amendments, all investment advisers—whether or not they have personal information about Massachusetts residents—would be well served to consider implementing policies and procedures that address the data security issues that the Massachusetts Law is designed to address.

James Snell, partner Bingham McCutchen LLP

**Julia B. Jacobson is Counsel in the Boston office of Bingham McCutchen LLP, and James G. Snell is Partner & Co-chair of the Privacy and Security Group in the Palo Alto office of Bingham McCutchen. Ms. Jacobson may be reached at (617) 951-8017 or julia.jacobson@bingham.com, and Mr. Snell may be reached at (650) 849-4882 or james.snell@bingham.com.*