New Massachusetts Data Security Law and Regulations

Written by Catherine M. Anderson, Jeffrey D. Collins

February 3, 2010

Comprehensive Information Security Plan required before March 1, 2010

As many of you are aware, The Commonwealth of Massachusetts has adopted a new data security law, and regulations thereunder (the "Regulations"), intended to protect its residents from identity theft. While the new law primarily addresses the required response by a company which is subject to an identity theft (prompted by the TJX data breach), the Regulations also set forth measures that businesses, including investment advisers and private fund managers, located in Massachusetts or elsewhere must take to safeguard the personal information of Massachusetts residents.

Such measures include the adoption of a comprehensive information security program. While many other states have adopted information security regulations, the requirements set forth in the Regulations have been recognized as some of the most detailed and comprehensive requirements in the country. Final regulations were filed by the Massachusetts Office of Consumer Affairs and Business ("OCABR") on November 4, 2009 and the Regulations principally become effective on March 1, 2010. A full text of the Regulations may be found at the Massachusetts OCABR's website. This memorandum is intended to inform investment advisers and private fund managers of how the Regulations will impact them and what they need to do to comply.

To whom do the Regulations apply?

The Regulations apply to **any** person or business that owns or licenses "personal information" of a Massachusetts resident, including registered and unregistered investment advisers and private fund managers with Massachusetts clients, investors or employees. If you are an SEC registered investment adviser with Massachusetts clients, investors or employees, then you must also comply with these Regulations even though you are already complying with Regulation S-P.

The investment adviser/fund manager does not have to be located in Massachusetts in order to be required to comply with the Regulations. If you are an investment adviser (either registered or unregistered) or fund manager located outside of Massachusetts then you must comply with these Regulations if you have investors or clients located in Massachusetts. The Regulations define "personal information" as a person's first name and last name or first initial and last name in combination with that person's social security number, driver's license number (or other state-issued identification number), or financial account number (or credit or debit card number with or without any required password, PIN etc.) and includes personal information of both your investors/clients and employees. As a practical matter, every investment adviser and fund manager is in possession of "personal information." Personal information does not include information that is lawfully obtained from publicly available information or from federal, state or local government records lawfully made available to the general public.

What do the Regulations require?

The Regulations require that every person or business that has the "personal information" of a Massachusetts resident develop, implement and maintain a "comprehensive information security program ("CISP") that is written in one or more readily accessible parts" by March 1, 2010.

In practice, this will mean that you will need to review and update your existing privacy and data protection policies to be compliant with the Regulations and adopt in writing a CISP. You also need to train your employees with respect to such policies.

The information security program must be reasonably consistent with industry standards and must contain administrative, technical, and physical safeguards to protect the personal information of Massachusetts residents.

The Regulations require a program that is tailored to your business. The Regulations set forth a list of elements that every CISP must include.

Some elements of your CISP can be included in your compliance manual but matters pertaining to your computer system security requirements or which would otherwise assist a potential violator should be kept confidential to those employees who are required to know the information to carry out their roles. We also recommend that you have a summary of your CISP available as a stand alone document that may be provided to your investors and clients (upon request) during any due diligence processes, or to regulators in an exam.

How do I develop a comprehensive information security program?

Developing an information security program requires a careful assessment of your business's needs and may not necessitate a complete overhaul of your current security methods. We recommend you first review the elements required to be included in the program as set forth in the Appendix (see below). We have also developed a guidebook to developing a CISP which you can download here. Once you have developed your draft CISP, please send it to us and we would be happy to review it for compliance with the Regulations.

What are my obligations to verify that any third-party service providers I retain are also protecting the personal information of Massachusetts residents?

In many cases, you may be providing certain third-party service providers (for example, fund administrators or banks), the personal information of Massachusetts residents. The Regulations require that you take reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect such personal information in a manner that complies with the Regulations and any applicable federal regulations.

This would likely require you to engage in some level of due diligence with respect to service providers who have access to "personal information" to determine what data security measures they have in place, and to obtain representations with respect to such measures. You should also check that your third-party service provider has in place adequate insurance in the event of a data/security breach. You should review their "general liability" policy to ensure that it does not have an exception for liability due to data breach, and whether a separate "cyber and data security" policy needs to be in place.

Under the Regulations, you must also require such third-party service providers by contract to implement and maintain appropriate security measures for personal information. There is a grandfather provision that deems any contract with a service provider entered into before March 1, 2010 to be in compliance even if it makes no reference to data protection. The grandfather provision expires March 1, 2012, however, so any contract regardless of when signed must be brought into compliance by such date. Although not required by the Regulations, we recommend that you receive an initial certification from your third-party service provider as to compliance with the Regulations which you would then require such provider to update on a regular (at least annual) basis.

What are the Computer System Security Requirements in the Regulations?

Your CISP will need to include the establishment and maintenance of a security system covering your computers (including any wireless system).

The most burdensome requirement is likely to be the requirement of encryption of all personal information stored on laptops or other portable devices and the encryption of all transmitted records and files containing personal information that will travel across public networks and encryption of all data containing personal information to be transmitted wirelessly.

You should review the means of delivery of your subscription agreements or other documents containing “personal information” to your administrators (and vice versa). In addition, the security system needs to include “secure user authentication protocols” including control of user IDs, a reasonably secure method of assigning passwords, control of data security passwords, restricting access to active users, and blocking access to user identification after multiple unsuccessful attempts. You also need to ensure that you have “secure access control measures” in place that restrict access to records and files containing personal information to those who need such information to

perform their jobs. You will need to monitor your systems for unauthorized use or access to personal information and ensure that you have up-to-date firewall protection and operating system security patches together with reasonably up-to-date malware protection, patches and virus definitions.

It is likely that for many investment advisers and fund managers these computer system security requirements will already be in place, but they should be memorialized in the CISP. The CISP also needs to include education and training of employees on the proper use of the computer security system and the importance of personal information security.

How must I manage a breach of data security in light of Regulations?

The Regulations, in summary, define a "breach of security" as an unauthorized acquisition or unauthorized use of (i) unencrypted data or (ii) encrypted electronic data and the confidential process or key needed to defeat the encryption. To be a “breach of security” the acquisition or use must also create a substantial risk of identity theft or fraud concerning a Massachusetts resident.

A breach of data security can occur in several ways, the most common being the theft or loss of computer hardware, the misuse of company information by an employee, or inadvertent disclosure by an employee (for example, sending an email with the wrong attachment).

Under the Regulations, a business must document responsive actions taken in connection with any incident involving a breach of security and conduct a mandatory post-incident review of events and actions taken, if any, with a view to making any needed changes in business practices relating to protection of personal information. Further, under recently enacted laws in Massachusetts, the business is subject to a notification obligation that it must fulfill "as soon as practicable and without unreasonable delay." Specifically, it must notify the affected individuals of the date of the breach, the steps that have been taken or will be taken to deal with the breach, the individual’s right to obtain a police report, and instructions for the individuals to request a credit report security freeze. It must also notify the Massachusetts Attorney General and the Director of the Consumer Affairs and Business Regulation of the date of the breach, the plans to deal with the breach, and the number of people affected by the breach.

Other states have data security regulations that have different notification requirements. You should consult with us to determine the correct course of action if a data breach occurs and you have clients/investors in multiple states.

Do the Red Flags Rules apply to investment advisers?

The FTC, FDIC and other federal regulatory authorities adopted the Red Flags Rules in January 2008 in response to the enactment of the Fair and Accurate Credit Transactions Act, 15 U.S.C. § 1681. The Rules requires many businesses and organizations to implement a written Identity Theft Prevention Program designed to detect the warning signs (i.e., “red flags") of identity theft in their day-to-day operation and to mitigate the potential harm caused to consumers. The Rules have been in effect for banks, credit card companies and traditional financial institutions since November 1, 2008. However, there have been delays in enforcement of the broadest of the Red Flags Rules, as set forth in 16 C.F.R. Part 681, which apply to "creditors." In 2008, the FTC caused considerable controversy by construing the term "creditor" to apply to any business that sells goods or services now and bills its customers later. Based on this reasoning, conceivably it is possible that the Red Flags Rules could be deemed to apply to investment advisers or private fund managers who charge their management fees in arrears. It should be noted that attempts have been by professional groups to limit this broad interpretation of the definition of "creditor." The American Bar Association, for example, was successful in obtaining a judgment that lawyers were exempt from the Red Flags Rule and the American Institute of Certified Public Accountants is also currently seeking summary judgment on this issue (before the same judge that decided the ABA case). At this time, however, we are recommending that investment advisers and fund managers take a conservative approach and comply with the Red Flags Rules because the requirements are not onerous and investment advisers and fund managers could integrate a program into the adoption of a CISP.

The FTC has repeatedly postponed the original November 1, 2008 deadline for businesses swept into the broad FTC definition of "creditor," most recently until June 1, 2010.

The FTC has released a "do-it-yourself prevention program" for businesses that have a low risk of identity theft, "such as businesses that know their customers personally," which may be the case with many investment advisers and fund managers.

According to the FTC, the June 1, 2010 deadline should give "low-risk" businesses an opportunity to use the FTC prevention program to develop a compliant program containing the elements set forth below. The basic elements of a compliant identity theft prevention program include:

- The appointment of an identity theft / information security coordinator
- Procedures to identify Red Flags and warning signs of identity theft and security risks
- Procedures for responding to Red Flags that have been detected
- An effective training program to educate staff on how to recognize and respond to Red Flags
- Ongoing oversight and monitoring of the identity theft prevention program.

We will continue to monitor the application of the Red Flags Rules to investment advisers and private fund managers and provide you with any updates.

APPENDIX 1

Summary of Minimum Standards of Comprehensive Information Security Program

The following is an excerpt from the Regulations stating the minimum standards which every information security program must meet. For updated information, please refer to the Regulations (201 CMR 17.00) which may be found at the Massachusetts Office of Consumer Affairs and Business Regulation's website.

17.03 Duty to Protect and Standards for Protecting Personal Information

Every comprehensive information security program shall include, but shall not be limited to:

- Designating one or more employees to maintain the comprehensive information security program.
- Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information; and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting identified risks, including but not limited to: (i) ongoing employee (including temporary and contract employee) training; (ii) employee compliance with policies and procedures; and (iii) means for detecting and preventing security system failures.
- Developing security policies for employees relating to the storage, access and transportation of records containing personal information outside of business premises.
- Imposing disciplinary measures for violations of the comprehensive information security program rules.
- Preventing terminated employees from accessing records containing personal information.
- Taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect such personal information consistent with these regulations and any applicable federal regulations;
- Requiring such third-party service providers by contract to implement and maintain such appropriate security measures for personal information; provided, however, that until March 1, 2012, a contract a person has entered into with a third party service provider to perform services for said person or functions on said person's behalf satisfies the provisions of 17.03(2)(f)(2) even if the contract does not include a requirement that the third party service provider maintain such appropriate safeguards, as long as said person entered into the contract no later than March 1, 2010.
- Reasonable restrictions upon physical access to records containing personal information, and storage of such records and data in locked facilities, storage areas or containers.
- Regular monitoring to ensure that the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information; and upgrading information safeguards as necessary to limit risks.
- Reviewing the scope of the security measures at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information.

RELATED INDUSTRIES

- Investment Advisers & Private Funds

- Professional Services

RELATED PRACTICES

- Business Counseling
- SBIC
