HARBOR LAW GROUP

The Massachusetts Data Security Regulations – Prepare to Comply

BY SHEHZAD RAJWANI

On August 17, 2009, the Office of Consumer Affairs and Business Regulation ("OCABR") revised the Massachusetts Data Security Regulations (the "Regulations") for a second time since their issuance in September 2008. The Regulations can be found at 201 C.M.R. 17.00, *et. seq.*, and the OCABR has extended the deadline for compliance to March 1, 2010.

The OCABR indicates that the August 2009 version of the Regulations contains the following important differences from the previous version: (i) a risk-based approach to information security consistent with applicable federal law; (ii) removal of certain specific provisions required to be included in a business's written information security program; (iii) the encryption requirement being tailored to be technology neutral and technical feasibility being applied to all computer security requirements; and (iv) the third party vendor requirements being changed to be consistent with federal law. Though the revisions appear to increase flexibility to reduce burdens on smaller and mid-sized business, the Regulations contain minimum requirements to be met by all companies who own or license "Personal Information" about Massachusetts residents.

The word finally seems to be spreading about the Regulations. Many people I talk with, however, still do not have a good idea about what the purpose of the Regulations and related laws is. They are also confused about what actions they need to take in order to comply with the Regulations.

The Purpose of the Regulations and Related Laws.

In the wake of well-publicized data breaches, including the TJX data breach, the Massachusetts legislature enacted two laws towards the end of 2007 and beginning of 2008. By way of background, TJX is the parent company of T.J. Maxx and Marshalls stores and disclosed in January 2007 that hackers had captured customer data from its computerized customer transaction systems. This exposed at least 45.7 million credit and debit cards to possible fraud and has cost TJX millions of dollars to date in settling lawsuits from banks, customers and attorney generals from forty-one states related to this massive data breach.[1]

The first law enacted by the legislature became effective October 31, 2007, and can be found at Chapter 93H of the Massachusetts General Laws. It requires notification of unauthorized acquisition or use of Massachusetts' residents' "Personal Information" to the Attorney General, the OCABR and, under most circumstances, the resident(s) affected.

The second law governs the manner in which this Personal Information must be disposed of or destroyed and can be found at Chapter 93I of the Massachusetts General Laws. It became effective February 3, 2008.

The OCABR subsequently promulgated a comprehensive set of regulations, which have recently been revised and are set to go into effect on March 1, 2010. The Regulations affect companies large and small and are designed to protect Massachusetts residents' Personal Information from identity theft and fraud. They require that every person and business that owns or licenses Personal Information about Massachusetts residents develop, implement and maintain a comprehensive written data security program.[2] The laws and regulations, therefore, mandate that all employers of Massachusetts' residents have a program to safeguard Personal Information, as that term is defined in the statute, require a procedure for disposal of Personal Information, and call for certain actions in the event of a data security breach.

Continued on next page >>

1 Fairly recently the United States Attorney in New Jersey announced indictments against three defendants related to the Heartland Payment Systems Inc. data breach. According to the indictment, the defendants stole more than 130 million credit and debit card numbers from late 2006 to early 2008, making this the largest data breach to date. The mastermind of the Heartland Payment Systems breach, Albert Gonzalez, was also involved in the TJX data breach (among others) and is awaiting trial in Massachusetts with regard to the TJX breach.

2 The Regulations exclude from the definition of "person" any "agency, executive office, department, board, commission, bureau, division or authority of the Commonwealth, or any of its branches, or any political subdivision thereof."

Harbor Law Group
Phone (508) 393-9244 | www.harborlaw.com
300 West Main Street, Building A, Unit 1 | Northborough, MA 01532

>> *From page one*

What is Personal Information?

Personal information consists of a Massachusetts resident's first name and last name or first initial and last name *in combination with* any one or more of the following: (a) social security number; (b) driver's license number or state-issued identification; or (c) financial account number, or credit or debit card number. Personal Information, however, does not include information lawfully obtained from publicly available information or government records lawfully made available to the public.

There is a good deal of confusion regarding Personal Information, and some people I have spoken with mistakenly think that the law does not apply to their companies because they do not maintain any Personal Information regarding Massachusetts residents. In fact, every employer should have Personal Information regarding its employees, including employment applications and employment eligibility verification forms, payroll and direct-deposit information and health benefit forms. In addition, many companies collect Personal Information regarding their customers for credit card transactions.

On the other hand, I have spoken with individuals who think that all confidential, proprietary or company sensitive data is subject to the Regulations. For example, the computer system security requirements in the regulations require "[t]o the extent technically feasible, encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data to be transmitted wirelessly." 201 C.M.R. 17.04(3). I have been asked what steps I have taken, or intend to take, with regard to confidential and privileged communications with clients that travel across the public networks or wirelessly. My answer is that, though I may be sending confidential and privileged information, I am not transmitting Personal Information regarding Massachusetts residents by email. Thus, the regulations do not speak to these communications and do not have to be encrypted. In the unlikely event that opposing counsel improperly attempts to obtain privileged email communications, there are other laws and ethical rules which can address this situation.

Our law firm, however, maintains Personal Information regarding Massachusetts residents. For example, the firm has information regarding its employees which constitutes Personal Information under the laws and regulations. We are, therefore, required to comply with the Regulations.

It is thus important to understand the purpose of the Regulations and related laws. Once you understand what documents and files contain Personal Information, your company can take the steps required by the Regulations to safeguard this information from unauthorized access or use.

Chapter 93H – Notification of Security Breaches

As discussed above, Chapter 93H is in effect now and contains, among other things, a duty to report known security breaches or unauthorized use of Personal Information. The statute provides for notification "as soon as practicable and without unreasonable delay" to the attorney general, OCABR and the resident(s) affected. The notice to the affected resident(s) may be delayed if law enforcement thinks it may impede a criminal investigation.

The statute provides that the notice to the attorney general and OCABR must include, but not be limited to: (i) the nature of the breach of security or unauthorized acquisition or use; (ii) the number of residents of the Commonwealth affected by such incident at the time of notification; and (iii) any steps the person or agency has taken or plans to take relating to the incident.[3]

With regard to the resident(s) affected, the notice must include, but not be limited to: (i) the resident's right to obtain a police report; (ii) how the resident requests a security freeze and the necessary information to be provided when requesting the security freeze; and (iii) any fees to be paid to any of the consumer reporting agencies. The notification, however, should NOT include: (i) the nature of the breach or unauthorized acquisition or use of the resident's Personal Information; and (ii) the number of Massachusetts residents affected by the breach or unauthorized access or use.[4]

Information regarding security freezes, along with additional helpful information related to identity theft, can be found on the OCABR's website. A security freeze prohibits, with certain specific exceptions, a credit reporting agency from releasing the consumer's credit report or any information from it without the express authorization of the consumer. To place a security freeze on your credit report, you must send a written request to all three credit reporting agencies, Equifax, Experian and TransUnion. These companies' websites provide instructions regarding requesting a security freeze and the necessary information to be provided by the consumer.

Continued on next page >>

3 The Attorney General's website contains a page, which provides guidance for businesses on security breaches. Sample breach notification letters to the Attorney General and OCABR, and to the Massachusetts residents affected, can be found on this page of the website.

4 At this time 45 states, the District of Columbia, Puerto Rico and the Virgin Islands have enacted breach notification laws. Therefore, companies reporting breaches affecting residents of multiple states should check the different notice requirements for each state.

>> *From page two*

An advisory from the OCABR informs that "[i]f you are a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, temporarily lift, or remove a security freeze. In all other cases, a credit reporting agency may charge you a fee of up to $5 to place, lift, or remove a security freeze."

Because information about a security breach must be provided by companies "as soon as practicable and without unreasonable delay," your company should develop procedures for responding to a potential breach. I recommend you involve counsel early in the event that your company discovers a breach of security, finds that Personal Information has been acquired or used by an unauthorized person, or learns that Personal Information was used for an unauthorized purpose.

Chapter 93I – Disposition and Destruction of Records

When businesses dispose of records containing Personal Information, they must meet the following minimum standard:

> (a) Paper documents containing personal information shall be either redacted, burned, pulverized or shredded so that personal data cannot practicably be read or reconstructed;
>
> (b) Electronic media and other non-paper media containing personal information shall be destroyed or erased so that personal information cannot be read or reconstructed.

Companies may contract with third parties to dispose of Personal Information so long as the third party complies with Chapter 93I.

201 C.M.R. 17.00 – The Regulations

The Regulations require that "[e]very person that owns or licenses personal information about a resident of the Commonwealth shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to (a) the size, scope and type of business of the person obligated to safeguard the personal information under such comprehensive information security program; (b) the amount of resources available to such person; (c) the amount of stored data; and (d) the need for security and confidentiality of both consumer and employee information." They further provide that "[t]he safeguards contained in such program must be consistent with the safeguards for protection of personal information and information of a similar character set forth in any state or federal regulations by which the person who owns or licenses such information may be regulated."

Depending on its size, your company should assemble a team of employees to learn about the details of the laws and Regulations. They can begin to identify paper, electronic and other records, computing systems, and storage media, including laptops and portable devices, which contain Personal Information. Once your company identifies where it stores documents containing Personal Information, it must identify internal and external risks to such information and evaluate current safeguards that are in place. In coming up with a comprehensive written information security program, companies must meet specific minimum requirements in the Regulations. These include, in abbreviated terms, the following:

- Designate one or more employees to maintain the program;
- Conduct ongoing employee training (including temporary and contract employees);
- Ensure employee compliance and impose disciplinary measures upon those who violate polices in the program;
- Have means for detecting and preventing security failures;
- Develop a policy for transporting records containing Personal Information outside of business premises so as to safeguard this information;
- Prevent terminated employees from accessing records containing Personal Information;
- Take reasonable steps to select and retain third-party service providers who can protect Personal Information and require such third-party service providers by contract to implement and maintain appropriate security measures (but the Regulations provide a potential two-year window regarding the contract requirement depending on when the agreement was entered into between the parties);
- Restrict access to paper documents containing Personal Information and keep them under lock and key;
- Restrict access to electronic documents containing Personal Information through firewalls, encryption and other electronic safeguards;
- Provide for restrictions upon physical access to records containing Personal Information;
- Document breaches of security, take appropriate actions regarding notifications required under Chapter 93H and conduct a post-incident review;
- Comply with various computer system security requirements to the extent technically feasible, including using strong passwords, encrypting Personal Information traveling across public networks, encrypting Personal Information on laptop computers and other portable

Continued on next page >>

Harbor Law Group
Phone (508) 393-9244 | www.harborlaw.com
300 West Main Street, Building A, Unit 1 | Northborough, MA 01532

>> *From page three*

devices, using a firewall, using up-to-date virus protections and educating and training of employees on computer system security.

The OCABR's website contains additional guidance regarding the Regulations, and both the OCABR and Attorney General provide information regarding notification of security breaches on their websites. In addition, the Federal Trade Commission's website has a good deal of useful information regarding identity theft and steps for businesses to take to comply with various federal laws. It is important for companies to analyze how they safeguard Personal Information. In so doing, the above-mentioned agencies want businesses not only to develop and implement programs designed to protect Personal information from identity theft, but also to maintain a "culture of security" through a regular schedule of employee training going forward.

How Much Effort Will It Take to Comply?

As discussed, not all companies will be judged by the same standard under the Regulations. Thus, Joe the Plumber (or any small plumbing business) will not be held to the same standards as Wal-Mart or Bank of America. All businesses that employ Massachusetts residents, however, will have to take some necessary steps to comply with the Regulations.

With regard to complying with the computer system security requirements, your company will probably need to consult with an Information Technology ("IT") company. The Frequently Asked Questions Regarding 201 CMR 17.00, which are posted on the OCABR website, state the following: "All of the computer security provisions apply to a business if they are technically feasible. The standard of technical feasibility takes reasonableness into account. The computer security provisions in 17.04 should be construed in accordance with the risk-based approach of the regulation." The FAQ's further provide that "[t]echnically feasible' means that if there is a reasonable means through technology to accomplish a required result, then that reasonable means must be used." Therefore, most companies will likely need IT assistance in determining technical feasibility and ensuring compliance with the computer system security requirements in the Regulations.

What If My Company Already Has To Comply With Other Federal Laws?

The regulations in 201 CMR 17.00 apply to companies who already have to comply with overlapping federal laws such as Graham-Leach-Bliley ("GLB"), HIPAA or the Federal Trade Commission's Red Flag Rules (which the FTC intends to implement beginning November 1, 2009). If your company has taken steps to comply with federal regulations in order to protect customer and patient privacy, it likely has many of the required measures in place to protect Personal Information. However, the OCABR's website specifically provides that you must comply with the Regulations even if you already comply with other federal regulations.

What Happens If I Do Not Comply?

The Attorney General has enforcement powers under the statutes and violations can subject noncompliant persons to civil penalties and costs of the investigation and litigation, including attorney's fees. The Attorney General will likely look for elements of deceptiveness and unfairness in deciding whether her office should pursue an enforcement action against a company. These include, for example, situations where a company knew of a breach of security and failed to notify the Massachusetts residents affected or where there are no adequate policies in place to protect Massachusetts residents' Personal Information.

In addition, resourceful trial attorneys may try and portray the regulations as establishing a standard of care in pursuit of negligence claims in data breach litigation. Businesses, therefore, would be well advised to begin taking steps to bring them into compliance by the March 1, 2010 deadline.

Shehzad Rajwani

Mr. Rajwani practices in the areas of employment law and business litigation. He counsels management and employees on federal and state employment law and represents both in related litigation. He also represents clients in litigation and arbitration proceedings regarding breaches of contracts and business torts.

Mr. Rajwani graduated from Baylor Law School, where he served as President of the Baylor University Minority Law Student Association and was a member of the Order of Barristers. He is licensed to practice in Massachusetts and Texas and has authored several articles regarding issues in his field.

Harbor Law Group
Phone (508) 393-9244 | www.harborlaw.com
300 West Main Street, Building A, Unit 1 | Northborough, MA 01532