

101 Arch Street
Boston, Massachusetts 02110
Telephone (617) 951-2800
Facsimile (617) 951-2819
www.lgllp.com

ARE YOU PREPARED FOR THE NEW IDENTITY THEFT REGULATIONS IMPACTING ALL MASSACHUSETTS BUSINESSES AND RESIDENTS?

By: Richard J. Grahn, Esq.



Richard J. Grahn, Esq.
rgrahn@lgllp.com

January 2010

The March 1, 2010 compliance date is rapidly approaching, but it's not too late.

Massachusetts will soon require all businesses to comply with a stringent set of identity theft regulations. The Massachusetts Office of Consumer Affairs and Business Regulation has established March 1, 2010 as the effective date. These detailed regulations, the first of their kind in the nation, establish the procedures that businesses must adopt to increase the level of security of personal information they hold. The regulations may be found at <http://www.mass.gov/Eoca/docs/idtheft/201CMR17amended.pdf>.

Under these regulations, referred to as 201 CMR 17, if you or your business own, license, receive, store, maintain, process or otherwise have access to information containing the first name or initial and last name of a Massachusetts resident, combined with a Social Security number, state issued identification number, financial account, credit, or debit card number ("Personal Information"), you are required to comply with 201 CMR 17 and protect that information from disclosure.

As many clients are unsure of what precisely needs to be done before March 1, 2010, we address the five critical steps you must take to limit your risk, ensure compliance, and protect your data.

Where do you stand?

201 CMR 17.00 requires that you take five specific steps to prevent identity theft. All persons in Massachusetts who possess Personal Information must take these steps. In addition, all organizations outside of Massachusetts that use Personal Information about a Massachusetts resident likewise are subject to these regulations. The procedures required to implement these regulations are "risk based," in that they are dependent on an assessment of the likelihood, extent, and

Looney & Grossman

Practice Areas:

Bankruptcy & Insolvency
Business
Family Law
Litigation
Professional Liability Defense
& Insurance
Real Estate
Transportation & Maritime

101 Arch Street
Boston, Massachusetts 02110
Telephone (617) 951-2800
Facsimile (617) 951-2819
www.lgllp.com

If your business handles detailed financial information or processes credit card transactions, the requirements will be far more onerous. If your industry has information security standards, you should become aware of them, as they will serve as a measure against which your security program will be considered.

nature of the harm that might be caused by a breach of security.

The regulations provide some latitude to businesses in framing their respective security programs by giving consideration to the size of the organization, the amount of Personal Information it handles and the resources available. Even if you access little Personal Information, you still must take these steps. If your business handles detailed financial information or processes credit card transactions, the requirements will be far more onerous. If your industry has information security standards, you should become aware of them, as they will serve as a measure against which your security program will be considered.

What you need to do:

1. Appoint a **Personal Information Security Manager**.
2. **Conduct a Risk Analysis** regarding the Personal Information you receive or transmit.
3. Draft and approve a written **Comprehensive Information Security Program**.
4. **Train your staff** to understand and follow the Comprehensive Information Security Program.
5. **Audit compliance** regularly.

Step One: Appoint a Personal Information Security Manager.

This is the first, and may well be the most essential, step in implementing 201 CMR 17, and it is the one upon which the success of your program likely depends. Your Personal Information Security Manager (PISM) must be diligent, computer literate, and have an understanding of office procedures and the capacity of your business to secure the confidentiality of Personal Information. This task requires the ability to identify Personal Information, consider how it is used in your business, determine how best to secure it (both in hard copy and electronic formats), and assess how best to train employees in securing that Personal Information.

You should choose someone as PISM who has been with your organization long enough to understand how your business operates and how its encryption system functions. Encryption is the process of

Looney & Grossman

Practice Areas:

Bankruptcy & Insolvency
Business
Family Law
Litigation
Professional Liability Defense
& Insurance
Real Estate
Transportation & Maritime

101 Arch Street
Boston, Massachusetts 02110
Telephone (617) 951-2800
Facsimile (617) 951-2819
www.lgllp.com

transforming information into a form unrecognizable to all except those possessing a key to decipher the content. Encryption is widely used to protect data being transmitted over the Internet by computers, mobile phones, PDAs, and Bluetooth devices.

Equally as important is the commitment of management. The PISM will likely face impediments whether as a result of inertia or due to outright resistance. Management must be prepared to support the efforts of the PISM if the implementation of the program is to be successful.

Step Two: Conduct a Risk Analysis Regarding the Personal Information You Receive or Transmit.

While recent amendments to the regulations deleted the requirement for a formal risk assessment, the drafting of the comprehensive written information security program necessarily entails a consideration of what Personal Information your business receives, how it is stored, how it is used, whether it is transmitted, and when and how it is destroyed. A typical approach to risk assessment involves the establishment of a process to identify foreseeable internal and external risks to the security, confidentiality and integrity of the Personal Information. The PISM should take the lead in developing the process to conduct the risk analysis and to obtain the results.

Step Three: Draft and Approve a Comprehensive Information Security Policy.

Your PISM should also be responsible for drafting a written Comprehensive Information Security Program (CISP) that is understandable and adequate to address the needs of your business and the concerns for the security of its Personal Information. Management of the organization should approve and support it.

The CISP should enforce basic standards for keeping Personal Information out of the hands of hackers, third parties, visitors, and unauthorized employees. If laptops, flash drives, and other storage devices contain Personal Information, encryption is required. If Personal Information is transmitted or removed from your business premises, it must be secured. These means of transmission include facsimile transmittal and internet delivery, as well as through wireless networks, if your employees have remote access to your business computers.

Looney & Grossman

Practice Areas:

Bankruptcy & Insolvency
Business
Family Law
Litigation
Professional Liability Defense
& Insurance
Real Estate
Transportation & Maritime

101 Arch Street
Boston, Massachusetts 02110
Telephone (617) 951-2800
Facsimile (617) 951-2819
www.lgllp.com

March 1, 2010 is but two months away. Based upon our discussions with business leaders and IT professionals, it is apparent that many businesses underestimated the amount of time, effort and cost required to comply with 201 CMR 17.

Looney & Grossman

Practice Areas:

Bankruptcy & Insolvency
Business
Family Law
Litigation
Professional Liability Defense
& Insurance
Real Estate
Transportation & Maritime

The CISP should also consider the terms under which your business receives or supplies Personal Information to or from third party vendors with whom you contract (e.g. payroll services, employee benefits providers, or accountants). The amended regulations defer until March 1, 2012 the requirement that third party vendors certify that they maintain procedures required to comply with 201 CMR 17 for all contracts entered into on or before March 1, 2010. For contracts entered into after March 1, 2010, vendors must make those certifications.

Step Four: Train Your Staff to Understand and Follow the Comprehensive Information Security Program.

Drafting your CISP is an important, but not last step. You must train your staff to understand what you are requiring of them, and then enforce those requirements. The PISM should be directly involved in this process. Any breaches must be detected, analyzed and reported as may be required under the regulations.

Step Five: Audit Compliance Regularly.

Once you have drafted and implemented the CISP, you must monitor its effectiveness. You must review the CISP and its implementation at least annually, or when a significant change in your business operation occurs that could affect the CISP, such as personnel changes, change in your office location, change in industry security standards, or change in the way you implement security.

A Final Thought.

March 1, 2010 is fewer than two months away. Based upon our discussions with business leaders and IT professionals, it is apparent that many businesses underestimated the amount of time, effort and cost required to comply with 201 CMR 17. We routinely see clients surprised by the sheer volume of data in their businesses which falls within the definition of Personal Information. However, if you follow the steps as outlined above, you will be much better prepared to comply with the requirements of the regulations and protect your business and the Personal Information of your customers and employees. It is not too late to complete this process, but timing is critical.

Looney & Grossman is available to suggest appropriate risk assessment techniques and guidelines for drafting comprehensive information security programs. Should you have questions, please contact Richard J. Grahn.