

Looney & Grossman LLP

Attorneys at Law

BUSINESSES MUST PAY ATTENTION TO NEW REGULATIONS REQUIRING PROTECTION OF THE PERSONAL INFORMATION OF MASSACHUSETTS RESIDENTS

Effective Date Extended to May 1, 2009

By: **Richard J. Grahn, Esq.**

Without much fanfare or publicity, the Massachusetts Office of Consumer Affairs and Business Regulation (the “OCABR”) recently issued comprehensive regulations (see www.mass.gov/oca) designed to reduce incidents of identity theft, and imposing significant obligations upon businesses to safeguard personal information. When first promulgated, the new regulations were to take effect on January 1, 2009. However, in the face of a firestorm of complaints and the economic downturn, the effective date has been postponed to **May 1, 2009**.

The regulations require all persons and entities that “own, license, store or maintain” personal information of a Massachusetts resident to adopt written policies and procedures to protect that information. The regulations apply to businesses or employers outside of Massachusetts which have personal information regarding Massachusetts residents. Personal information is defined to include names of Massachusetts residents “in combination with” social security numbers, driver’s license numbers or financial account numbers. The regulations are not limited to financial institutions and companies which store customer credit card information that have received publicity for their massive data thefts. They expressly refer to employee information as well, and accordingly, every business employing a Massachusetts resident will be impacted by the comprehensive requirements imposed by these new regulations.

Assessing the Scope of Responsibility

The regulations require that every person or entity which owns, licenses, stores or maintains personal information of Massachusetts residents must have a comprehensive, written information security program (“WISP”) applicable to all records containing such personal information. The WISP must be reasonably consistent with industry standards and include administrative, technical, and physical safeguards to ensure the security and confidentiality of these records. It must also satisfy the requirements of any other federal or state mandated security requirements applicable to the particular business (HIPAA, Gramm-Leach-Bliley, SEC requirements). While it is clear that a failure to meet HIPAA, GLB or SEC information security requirements will also result in a violation of the OCABR regulations, compliance with these other requirements may not necessarily satisfy the OCABR regulations.

New Regulations

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



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

November 2008

Looney & Grossman

Practice Groups:

Bankruptcy

Business

Litigation

Transportation

Family Law

The regulations are not limited to financial institutions and companies which store customer credit card information that have received publicity for their massive data thefts. They expressly refer to employee information, and accordingly, ...every business that employs Massachusetts residents will be impacted by the comprehensive requirements imposed by these new regulations.

Visit www.lgllp.com to read client alerts and articles, which may be beneficial to you or your business. Also view attorney profiles and descriptions of Looney & Grossman's Bankruptcy, Business, Litigation, Transportation, and Family Law Practice Groups.

The regulations acknowledge the burden on smaller businesses by providing that evaluation of compliance with these regulations will take into account (i) the size, scope and type of business, (ii) the resources available to the business, (iii) the volume of stored data, and (iv) the need for security and confidentiality of both consumer and employee information. However, at this point there is no express guidance to assure that a company's information security plan and procedures satisfy the regulations. Enforcement will be undertaken through the Office of the Attorney General, which has yet to issue enforcement guidelines.

In general terms, the regulations provide that every WISP must, at a minimum, include the following:

- Designation of one or more employees to maintain the information security program;
- Identification and assessment of reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of all electronic, paper or other records containing personal information.
- Provisions for ongoing employee (including temporary and contract employee) training; monitor employee compliance with policies and procedures; and development of a means for detecting and preventing security system failures.
- Security policies for employees that take into account whether and how employees should be allowed to keep, access and transport records containing personal information outside of business premises.
- Disciplinary measures for violations of the information security programs and provisions preventing terminated employees from accessing records containing personal information.
- Reasonable steps to verify that third-party service providers (outside payroll services, benefits providers, storage facilities and the like) with access to personal information have the capacity to protect personal information, by (i) selecting and retaining service providers capable of maintaining safeguards for personal information; and (ii) contractually requiring service providers to maintain these safeguards. The regulations specifically mandate that prior to permitting third-party service providers access to personal information, the person permitting access is required to obtain from the third-party service provider a written certification that the service provider also has a written, comprehensive information security program that is in compliance with the provisions of these regulations.
- Limit the amount of personal information collected to that reasonably necessary to accomplish the legitimate purpose for which it is collected; limit the time this information is retained to that reasonably necessary to accomplish the desired purpose; and limit access only to those persons who are reasonably required to have this information in order to accomplish such responsibilities or to comply with state or federal record retention requirements.

This material may be considered advertising under the rules of the Supreme Judicial Court of Massachusetts. Do not act or rely upon this information without seeking professional legal advice.

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

- Identification of paper, electronic and other records, computing systems, and storage media, including laptops and portable devices used to store personal information, to determine which records contain personal information and how that information can be secured.
- Restrict physical access to records containing personal information, including a written procedure that sets forth the manner in which physical access to these records is restricted; and storage of the records and data in locked facilities, storage areas or containers.
- Provisions for regular monitoring to ensure that the information security program is operating in a manner reasonably calculated to prevent unauthorized access or unauthorized use.
- Annual review of the scope of the security measures or more frequent reviews whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information.
- Documentation of responsive actions taken in connection with any incident involving a breach of security, and mandatory post-incident review of events and actions taken.

Electronic System Security Requirements

In addition to the foregoing, the regulations contain detailed requirements for encryption of data for all persons and entities that maintain or transmit employee or other personal information in electronic format over public networks, and by use of laptop computers, PDA's and other wireless devices.

The deadline to ensure encryption for laptops was extended to May 1, 2009, and for other portable devices to January 1, 2010.

Conclusion

Many of the requirements set forth in the regulations are new to businesses and employers, particularly out-of-state employers of Massachusetts residents. The regulations do not specify the precise or approved methods for compliance. However, a good faith attempt to satisfy the requirements of these regulations will be important to avoid sanctions in the event of personal information maintained by covered businesses is compromised or if the office of the Attorney General inquires. Given the broad reach of the requirements imposed by these regulations and the numerous complaints received about them, more guidance may be forthcoming. We will attempt to keep clients advised as more information becomes available.

Richard J. Grahn is Managing Partner at Looney & Grossman LLP. His practice involves primarily litigation related to governmental enforcement actions and related claims in both civil and criminal proceedings. He represents companies, other organizations, and individuals in a broad range of investigations, including transportation, accounting, maritime security, insurance, securities and other regulatory compliance matters.

If you have any questions about or need legal assistance, you may contact Richard Grahn at 617-951-2800 or rgrahn@lgllp.com
New Regulations

Visit www.lgllp.com to read client alerts and articles, which may be beneficial to you or your business. Also view attorney profiles and descriptions of Looney & Grossman's Bankruptcy, Business, Litigation, Transportation, and Family Law Practice Groups.

This material may be considered advertising under the rules of the Supreme Judicial Court of Massachusetts. Do not act or rely upon this information without seeking professional legal advice.