jackson|lewis
Preventive strategies.
Positive solutions.

Massachusetts Identity Theft/ Data Security Regulations

Effective March 1, 2010
Are You Ready?

SPECIAL REPORT

All We Do Is Work.
Workplace Law. In four time zones and 45 major locations coast to coast.

www.jacksonlewis.com

JACKSON LEWIS

SERVING THE DIVERSE NEEDS OF MANAGEMENT

Jackson Lewis is one of the largest law firms in the country dedicated exclusively to representing management on workplace issues. The Firm has successfully handled cases in every state and is admitted to practice in all Circuit Courts of Appeal and in the United States Supreme Court. With 45 offices and more than 600 attorneys, the Firm has a national perspective and sensitivity to the nuances of regional business environments.

Since 1958 we have represented a wide range of public and private businesses and non-profit institutions in a vast array of industries. When issues arise, we devise optimal solutions that minimize costs and maximize results. Whether we are counseling on legal compliance or litigating a complex case, we assist our clients in achieving their business goals.

In addition, we help employers create policies and procedures promoting positive employee relations. We have built our practice and earned our national reputation over the years by helping companies reduce workplace-related litigation by educating management on legal trends, judicial developments, and statutory and regulatory compliance in the rapidly evolving area of workplace law. Our state-of-the-art preventive law programs utilize the Firm's expertise and unmatched experience to evaluate employment trends and related litigation, minimizing the risk of exposure in future lawsuits.

JACKSON LEWIS
BOSTON OFFICE
75 Park Plaza, 4th Floor
Boston, Massachusetts 02116
(617) 367-0025
www.jacksonlewis.com

Massachusetts Identity Theft/Data Security Regulations Effective March 1, 2010 – Are You Ready?

Joseph J. Lazzarotti | Partner
lazzaroj@jacksonlewis.com

Introduction

The Massachusetts Office of Consumer Affairs and Business Regulations (OCABR) announced on November 4, 2009, the filing of final identity theft/data security regulations with the Secretary of State's office, the final step before the regulations take effect on March 1, 2010. Many businesses are now beginning to think about what they need to do to comply. **This Special Report, with checklists, and our companion webinar will help businesses prepare for the new regulations.** More information about data privacy and security developments and resources can be found at www.workplaceprivacyreport.com.

The regulations apply to any business or individual that owns or licenses personal information (PI) about a Massachusetts resident, and establish minimum standards for protecting and storing such information. One owns or licenses PI when one "receives, stores, maintains, processes, or otherwise has access to personal information in connection with the provision of goods or services or in connection with employment."

PI is an individual's first name (or first initial) and last name in combination with: (i) social security number, (ii) driver's license number, (iii) state identification number, or (iv) financial account, debit or credit card number contained in paper **or** electronic format.

The regulations require covered entities develop, implement and maintain a comprehensive information security program to protect personal information. The program must be written (WISP). In evaluating compliance, the following items should be taken into account:

- the size, scope and type of business,
- the amount of resources available,
- the amount of stored data, and
- the need for security and confidentiality of both consumer and employee information.

Compliance Checklists

The following checklist outlines the items required to achieve compliance with the final data security regulations issued in Massachusetts.

Massachusetts Data Security Compliance Checklist: Minimum "Written Information Security Program" (WISP) Requirements	
Requirements for Every WISP	***Status***
In General: ▪ Program must be in writing. ▪ Program must be developed, implemented, maintained **and** monitored. ▪ Program must have administrative, technical, and physical safeguards and be reasonably consistent with safeguards for protection of personal information and information of a similar character set forth in any applicable state or federal regulations.	
Appoint Key Person: Designate one or more employees to maintain the program.	
Risk Assessment: ▪ Identify and assess reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of personal information. ▪ Evaluate and improve current safeguards for addressing identified risks through such steps as: o ongoing employee (including temporary and contract employee) training; o ensuring employee compliance with policies and procedures; o detecting and preventing security system failures.	
External Employee Access: Develop security policies addressing whether and how employees may keep, access **and** transport records containing personal information outside of the Company's business premises.	
Discipline: Impose discipline when the Company's program is violated.	
Protocols for Termination of Employment: Establish procedures to immediately stop access by terminated employees to personal information by physical or electronic access, such as deactivating their passwords and user names, changing locks, retrieving IDs, and so on.	
Oversee Service Providers. A service provider is any person that receives, stores, maintains, processes, or otherwise is permitted access to personal information through its provision of services directly to a person that is subject to the regulations. To adequately oversee service providers, the regulations require that covered entities: 1. Take reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect personal information consistent with the regulations and any applicable federal regulations; and 2. Require such service providers by contract to implement and maintain such appropriate security measures for personal information; provided, however, that until March 1, 2012, a contract in place prior to March 1, 2010, will be deemed to satisfy this requirement even if	

the contract does not require the service provider to maintain the appropriate safeguards. However, these contracts should be amended to include similar provisions as soon as possible, as there may be similar requirements under federal or other states' laws (such as HIPAA or data security laws in Maryland, Oregon or Nevada). Contracts entered into on or after March 1, 2010, must contain appropriate language.	
Physical Access and Storage: Impose reasonable restrictions upon physical access to records containing personal information, and storage of such records and data in locked facilities, storage areas or containers.	
Monitor Security Program Performance: Establish procedure for regular monitoring to ensure the program is operated in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information, and upgrade information safeguards as necessary.	
Annual Assessment of Scope of Security Program: At least once per year (or whenever there is a material change in business practices that reasonably affects the security or integrity of records containing personal information), review the scope of the program's security measures for adequacy.	
Document Breach Response: Document steps to respond to breach of security and post-breach review of events and actions taken, if any, to make changes in program.	

The following checklist outlines additional items for electronically stored or transmitted personal information.

Additional Requirements if Personal Information is Electronically Stored or Transmitted	***Status***
The additional elements below apply at a minimum, *and to the extent feasible*: ▪ to every person that owns or licenses personal information about a resident of the Commonwealth and electronically stores or transmits such information, and ▪ be part of a security system established and maintained by such person that covers the person's computers, including any wireless system.	
Implement Secure User Authentication Protocols that: ▪ control user IDs and other identifiers; ▪ reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices; ▪ control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect; ▪ restrict access to active users/user accounts only; and ▪ block access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system.	

Implement Secure Access Control Measures that: ▪ restrict access to personal information to those who need such information to perform their job duties; and ▪ assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls.	
Encryption: Encrypt all transmitted records and files containing personal information that will travel across public networks and transmit wirelessly.	
Mandatory Encryption for Portable Devices: Encrypt all laptops or other portable devices that store personal information.	
Monitor IT System Use and Access: Perform reasonable monitoring for unauthorized use of or access to personal information.	
Firewall/Malware/Virus Protection: Implement reasonably up-to-date firewall, system security agent software, malware and reasonably up-to-date patches and virus definitions that are reasonably designed to maintain the integrity of the personal information on a system connected to Internet. System also should be designed to receive current security updates on a regular basis.	
Training: Train and educate employees on the proper use of the computer security system and the importance of personal information security.	