

## Summary of New Massachusetts Privacy Law

*If you have any questions regarding the matters discussed in this memorandum, please contact the following attorneys or call your regular Skadden contact.*

**Stuart D. Levi**  
New York  
212.735.2750  
stuart.levi@skadden.com

**Scott Brown**  
Boston  
617.573.4874  
scott.brown@skadden.com

**James R. Carroll**  
Boston  
617.573.4801  
james.carroll@skadden.com

\* \* \*

*This memorandum is provided by Skadden, Arps, Slate, Meagher & Flom LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This memorandum is considered advertising under applicable state laws.*

On March 1, 2010, new regulations governing the handling of personal information about Massachusetts residents will go into effect. *The regulations are widely applicable to all persons (including corporations, partnerships and other legal entities) that receive, store, maintain, process or otherwise have access to personal information about any Massachusetts resident (in paper or electronic format), even if that information is comingled with information about residents of other states.* Known as The Standards for the Protection of Personal Information of Residents of the Commonwealth, these regulations were promulgated pursuant to Massachusetts' security breach notification law (Mass. Gen. L. ch. 93H). The regulations are memorialized at 201 C.M.R. 17.00.

The regulations have three stated objectives:

- Ensure the security and confidentiality of customer information in a manner fully consistent with industry standards;
- Protect against anticipated threats or hazards to the security or integrity of such information; and
- Protect against unauthorized access to or use of such information that may result in substantial harm or inconvenience to any consumer.

A summary of the regulations are set forth below.

### **"Personal Information" Covered by the Regulation**

"Personal information" is broadly defined as a person's name combined with private information, such as a Social Security number, driver's license number or any information that would permit access to a financial account (e.g., credit card number). Personal information does not include information that is lawfully made available to the general public.

### **Requirements for an Information Security Program**

The regulations create a duty to develop, implement and maintain a comprehensive, written information security program applicable to any records containing personal information about a resident of Massachusetts. The program must contain administrative, technical and physical safeguards to ensure the security and confidentiality of such personal information.

Whether the comprehensive information security program complies with the regulations will be evaluated taking into account the following four factors:

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

The regulations provide the following baseline list of criteria for a comprehensive information security program:

- (1) Designating one or more employees to maintain the comprehensive information security program;
- (2) Identifying and assessing reasonably foreseeable internal and external risks to the security and integrity of personal information records, and evaluating and improving, where necessary, the effectiveness of current safeguards for limiting such risks. This should include:
  - ongoing employee (including temporary and contract employee) training;
  - employee compliance with policies and procedures; and
  - means for detecting and preventing security system failures;
- (3) Developing security policies for employees relating to the storage, access and transportation of records outside of business premises;
- (4) Imposing disciplinary measures for violations of the program;
- (5) Preventing terminated employees from accessing records containing personal information;
- (6) Imposing reasonable restrictions on physical access to records, and storing such records and data in locked facilities, storage areas or containers;
- (7) Undertaking regular monitoring to ensure that the program is operating in a manner reasonably calculated to prevent unauthorized access or use of personal information; and upgrading information safeguards as necessary to limit risks;
- (8) 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; and
- (9) Reviewing any security breach incident and documenting the review and responsive actions taken as well as any changes made to business practices relating to the protection of personal information. A security breach is defined as the unauthorized acquisition or use of unencrypted data (or of encrypted data where the “key” has also been compromised) that creates a substantial risk of identity theft or fraud.

### **Use of Third-Party Service Providers**

The baseline criteria for a comprehensive information security program also includes required actions for dealing with any third party that receives, stores, maintains, processes or otherwise is permitted to access personal information through its provision of services. An entity that is subject to the Massachusetts regulation must 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 regulation as well as any applicable federal regulation.

In addition, such third-party service providers must be required by contract to implement and maintain “appropriate” security measures. Note that if a contract was entered into before March 1,

2010, this requirement only goes into effect on March 1, 2012. Therefore, existing contracts do not need to be amended at this time. However, companies may want to start the process of reviewing and, where necessary, amending their contracts now instead of waiting until 2012.

### **Computer System Security Requirements**

The regulations also impose specific – although technology neutral – requirements for the establishment and maintenance of a security system for computers, including wireless systems. These requirements are:

- (1) Securing user authentication protocols including:
  - (a) control of user IDs and other identifiers;
  - (b) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;
  - (c) 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;
  - (d) restricting access to active users and active user accounts only; and
  - (e) blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system;
- (2) Securing access control measures that:
  - (a) restrict access to records and files containing personal information to those who need such information to perform their job duties; and
  - (b) 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;
- (3) Encrypting all transmitted records and files containing personal information that will travel across public networks, and encrypting all data containing personal information to be transmitted wirelessly;
- (4) Reasonable monitoring of systems for unauthorized use of or access to personal information;
- (5) Encrypting of all personal information stored on laptops or other portable devices;
- (6) For files containing personal information on a system that is connected to the Internet, there must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information;
- (7) Reasonably up-to-date versions of system security agent software, which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis; and

- (8) Educating and training of employees on the proper use of the computer security system and the importance of personal information security.

### **Enforcement**

The Massachusetts attorney general is authorized to remedy violations of these regulations through an enforcement action pursuant to the “Little FTC Act” (Mass. Gen. L. ch. 93A, sect. 4), which is modeled after federal law and prohibits unfair business practices.

The attorney general may consider the following mitigating factors in determining whether a company’s information security program complies with the new regulations:

- (1) the size, scope and type of business charged with safeguarding the personal information at issue;
- (2) the resources available to such person or company;
- (3) the amount of personal information stored; and
- (4) the need for the confidentiality of such information.