



Client Alert

January 1, 2009

MASSACHUSETTS ISSUES REGULATIONS GOVERNING THE PROTECTION OF CONSUMER PERSONAL INFORMATION:

The Massachusetts Department of Consumer Affairs and Business Regulation has issued final regulations, codified as *201 CMR 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth*, which require all businesses and individuals that maintain personal information about Massachusetts residents to take certain steps to assure the security of that information. These regulations are the result of a law approved last year to combat identity theft. Although originally scheduled to take effect on January 1, 2009, the time period with which to comply with these Regulations has been extended to **May 1, 2009**.

Who is covered?

The Regulations apply to individuals, corporations, associations, partnerships, and other legal entities that own, license, store, or maintain “personal information” about a resident of Massachusetts.

What information must be protected?

The law and regulations define “personal information” to mean a Massachusetts resident’s first name, or first initial, and last name, combined with his or her social security number, driver’s license number, or any financial account, debit account number, or credit card number, with or without any required security code, access code, personal ID number or password, that would permit access to a resident’s financial account.

What is required?

Under the regulations, any person or business that owns, licenses, stores or maintains a Massachusetts resident’s personal information must develop and maintain a comprehensive written “Information Security Program” that is consistent with industry standards and contains safeguards to ensure the security and confidentiality of such personal information. All written security plans must address the following minimum requirements:

- Designating an employee who is responsible for maintaining the Information Security Program;
- Identifying and assessing reasonably foreseeable risks to the security of electronic and paper records that contain personal information. The program should address minimizing such risks by (i) implementing employee training programs; (ii) monitoring employee compliance with security program rules; (iii) improving means for detecting and preventing security systems failures;
- Training employees on information security, including how employees should be allowed to keep, access and transport records containing personal information

outside business premises, and disciplining them for violations of the security program;

- Limiting the amount of personal information collected, the duration for which such information is retained, and restricting employee access to such personal information to those individuals who are reasonably required to know such information;
- Monitoring regularly the compliance with, and the adequacy of, the Security Program and reviewing security measures on at least an annual basis or whenever there is material change in the business practice that might impact the security of records;
- Vetting and supervising service providers, which includes acquiring written certification from each service provider that it has a written information security program that meets the requirements of the Regulations;
- Documenting all information security breaches and responses in accordance with a written incidence response plan that includes mandatory post-incident review of events and describes any modification of information security practices;
- **Using encryption to protect electronic records (i) to the extent technically feasible, for all transmitted records and files containing personal information that will travel across public networks, and encryption of all data to be transmitted wirelessly and (ii) for all personal information on laptops and other portable devices.**

To review a copy of the Regulations and to obtain additional information and guidance on how to establish an Information Security Program, including a model program for small businesses, a compliance checklist and answers to frequently asked questions, please see the OCABR website at www.mass.gov/ocabr.