CAIN HIBBARD

Cain Hibbard & Myers PC | Counselors at Law

CLIENT ALERT

MAY 2011

REGULATIONS IMPOSE NEW OBLIGATIONS IN HANDLING PERSONAL INFORMATION AND PREVENTING IDENTITY CRIMES

Both the Commonwealth of Massachusetts and the federal government have issued new regulations designed to help safeguard the personal information of consumers. The federal regulations, known as the "Red Flag Rules," were promulgated by the Federal Trade Commission ("FTC") in conjunction with several other agencies. The Red Flag Rules became effective January 1, 2008, but the FTC delayed enforcement thereof until January 1, 2011 while Congress finalized legislation limiting the scope of businesses covered by the Rules. The Red Flag Rules require financial institutions and creditors who maintain certain types of customer accounts to develop and implement programs designed to detect, prevent and mitigate identity theft. Each program must include policies and procedures to identify and detect account activity that may signal identity theft ("Red Flags") and to respond appropriately to these Red Flags when they are detected. The term "creditor", as defined in the Red Flag Program Clarification Act of 2010, means a creditor that (a) obtains or uses consumer reports in connection with a credit transaction, (b) furnishes information to consumer reporting agencies in connection with a credit transaction or (c) advances funds to or on behalf of a person, based on an obligation of the person to repay the funds, except for advances of expenses incidental to a service provided by the creditor.

The regulations promulgated by the Massachusetts Office of Consumer Affairs and Business Regulation became effective March 1, 2010 and apply to "all persons that own or license personal information about a resident of the Commonwealth." The phrase "personal information" refers to the first and last name, or first initial and last name, of a Massachusetts resident together with the resident's Social Security number, driver's license (or other state issued ID) number, financial account number, or credit or debit card number. Any person or business that owns or licenses personal information must develop, implement, and maintain a comprehensive security program to protect those records.

Among other requirements, the security program must identify and assess internal and external risks to the security of personal information, provide security policies relating to records located off premises, impose discipline upon employees who violate program policies, establish reasonable procedures to verify that third-party service providers have the capacity to protect personal information, monitor, document, and update program policies, and restrict physical and electronic access to personal information. For electronically stored records, the security program must incorporate passwords, encryption, firewall protection, security patches and employee education. The administrative, technical and physical safeguards contained in the security program must be appropriate to (a) the size, scope and type of the business, (b) the amount of resources available to the business, (c) the amount of data stored by the business and (d) the need for security and confidentiality of both consumer and employee information.

Because substantial penalties could result from violation of either the federal or the state regulations, we are advising our clients to carefully review and evaluate their current policies and the ways in which they handle personal information about their employees, customers, clients or patients.

If you would like to speak with someone about these new requirements, please contact Lucy Prashker of our Technology and Internet Law Group.

Cain Hibbard & Myers PC
ww.cainhibbard.com
66 West Street
Pittsfield, MA 01201
Phone: (413) 443-4771

309 Main Street
Great Barrington, MA 01230
Phone: (413) 528-4771

377 Main Street
Williamstown, MA 01267
Phone: 413-884-0006