INTELLECTUAL PROPERTY ALERT

ROBINSON BRADSHAW & HINSON

FEBRUARY 2010

Massachusetts Privacy Regulation Will Finally Take Effect on March 1; Regulators Send Mixed Messages

By Robert M. Bryan and John M. Conley

Barring further surprises, the long-delayed Massachusetts "Standards for the Protection of Personal Information of Residents of the Commonwealth" (201 CMR 17) will finally take effect on March 1, 2010. As we reported in August 2009, the regulation requires that (a) "every person that owns or licenses personal information about" a Massachusetts resident must implement a written information security program that contains administrative, technical, and physical safeguards; (b) effective two years from now, third-party service providers must give contractual guarantees of information security; and (c) all personal information that is stored on portable devices like laptops or that will travel across networks or via wireless transmission must be encrypted. The law also has a strong data security breach notification requirement.

FAQs issued in August 2009 by the state's Office of Consumer Affairs and Business Regulation stress that the regulation is intended to encourage a "risk-based" approach to compliance rather than mandate a one-size-fits-all solution. The FAQs also emphasize that the state is trying to make its approach consistent with that of the Federal Trade Commission's Safeguards Rule (FTC's Business Guide). Specifically, the written policy should take into account "the particular business' size, scope of business, amount of resources, nature and quality of data collected and stored, and the need for security." The encryption requirement -- probably the most controversial aspect of the entire regulation -- is said to be applicable only "where it is reasonable and technically feasible." This is not the same as saying that it is optional, however, since the definition of "technically feasible" states that "if there is a reasonable means through technology to accomplish a required result, then that reasonable means must be used."

Beyond these vague statements in the FAQs, the state has given little guidance on how the new regulation will be enforced. In a pair of late-January public presentations about prospective enforcement, representatives of the Office of Consumer Affairs and Business Regulation and the Office of the Attorney General focused primarily

on the data security breach notification issue. Both said that they will be more lenient with businesses that promptly notify the affected individuals and the state, cooperate in any state investigation, and show a commitment to following industry best practices. The few comments on the rest of the regulation encouraged businesses to seek out and follow best privacy practices for their respective industries. Small business advocates continue to complain about the prohibitive cost of compliance for their constituents.

As we approach the implementation date, the key issue remains how the state enforcement authorities will construe such generalities as "risk-based," "reasonable," and "technically feasible." Unfortunately, those who have to comply have been given very few clues.