Massachusetts Forces Businesses to Implement Sweeping Information Security Measures by January 1, 2009

October 14, 2008

The Commonwealth of Massachusetts recently adopted regulations requiring all businesses that own, license, store or maintain personal information about a resident of Massachusetts to adopt a comprehensive, written information security program. The security program must include a computer security system that encrypts all records and files containing personal information, including all employee and consumer information.

Information Security Program

The new regulations apply to any person or entity that owns, licenses, stores or maintains any personal information of a Massachusetts resident. The regulations define "personal information" as any combination of a resident's name with a Social Security number, driver's license number, bank account number or credit card number.

The written information security program must be reasonably consistent with industry standards, but may take into account the size, type and resources of a particular business as well as the amount of data stored and the need for confidentiality of consumer and employee information. The regulations provide detailed requirements for any such program, including identification of risks, development of security policies for employees, verification of the security of third-party providers and regular monitoring of the program.

Computer System Security Requirements

The new regulations also require the establishment and maintenance of a security system covering a business' computers, including any wireless networks connecting its computers. The security system must include secure user authentication protocols and access measures as well as reasonably up-to-date firewall protection, operating system security patches and system security agent software. In addition, the regulations require the encryption of (1) to the extent technically feasible, all transmitted records and files that contain personal information and will be transmitted over public networks or transmitted wirelessly and (2) all personal information stored on laptops or other portable devices.

Compliance

All businesses must comply with these regulations by January 1, 2009. If a business fails to comply with the regulations, the Massachusetts Attorney General may bring an action for injunctive relief, and a court may impose a fine of up to $5,000 for each violation of the regulations plus the reasonable costs of such investigation and litigation, including reasonable attorneys' fees.

Open Questions

These regulations raise many questions for interpretation, particularly with respect to the computer system security requirements. For example:

- What is meant by "reasonably up-to-date" with respect to firewall protection, operating system security patches and system security agent software?
- Does the requirement for encryption on all records and files that contain personal information transmitted wirelessly include internal wireless networks within a business?
- What devices are considered "portable devices"?
- Does the $5,000 fine apply to each resident whose records are not properly secured or only on a per security incident basis?

For Further Information

If you have any questions regarding these regulations, including how they may affect your company, please contact one of the members of the Information Technologies and Telecom Practice Group or the lawyer in the firm with whom you are regularly in contact.