

## New Massachusetts Data Security Requirements Go Into Effect In January 2009

*The Massachusetts Office of Consumer Affairs and Business Regulation recently released a new data security regulation,<sup>1</sup> which goes into effect January 1, 2009, requiring businesses that handle personal information of Massachusetts residents to institute various new and burdensome security controls.*

These controls include adopting a written, comprehensive information security program that contains administrative, technical, and physical safeguards consistent with industry standards, and, perhaps most significantly (and novel among states), requires that businesses encrypt certain highly sensitive personal data that is stored on mobile devices. This advisory provides an overview of the new requirements under the Regulation.

### APPLICABILITY

The Regulation requires any person that owns, licenses, stores, or maintains certain sensitive “personal information” about a Massachusetts resident to develop, implement, maintain, and monitor a comprehensive, written information security program applicable to records containing such personal information. Thus, if a business outside of Massachusetts collects Massachusetts residents’ personal information (whether customer, employee, or other personal data), under the terms of the Regulation, the business would be subject to its requirements. It remains to be seen whether the Massachusetts Attorney General or private litigants will attempt to enforce the Regulation against businesses with no operations in Massachusetts, but if they do (and succeed), businesses could be subject to civil penalties, as detailed below.

Under the Regulation, “personal information” is defined as a person’s first and last name or first initial and last name *in combination with one or more of the following elements*: Social Security number, driver’s license or state identification card number, financial account number, credit card number, or debit card number (and excluding publicly available information). Thus, unlike many safeguard laws in other states, such as California, Texas, Connecticut, and Michigan, among others, the Massachusetts regulation’s requirements focus on *sensitive personal information*, rather than *any type of data* that potentially identifies an individual.

### REQUIREMENTS

The Regulation requires business to have a written, comprehensive security program that:

- Designates one or more employees to maintain the program;
- Identifies reasonably foreseeable internal and external risks to the personal information (note that this will require periodic updates as the foreseeability of risks changes over time), and assesses and improves the effectiveness of safeguards in limiting these risks, such as through employee training, employee compliance with policies and procedures, and controls for detecting and preventing security system failures;
- Includes security policies to address employee retention, access, and transport of personal information outside of the business premises, and disciplining employees who do not comply with such policies;
- Prevents terminated employees from accessing personal information by immediately terminating

<sup>1</sup> Mass. Regs. Code tit. 201, § 17.00 (2008).

- their physical and electronic access (e.g., terminating user names and passwords);
- Takes reasonable steps to verify that third-party service providers with access to personal information can protect the information, including by obtaining written certification from the third-party that it has a written, comprehensive information security program in compliance with the Regulation;
- Limits the amount of personal information collected, retained, and accessed to that reasonably necessary to accomplish a legitimate business or legal purpose;
- Identifies the paper, electronic, and other records, computing systems, mobile devices, and storage media that contain personal information (i.e., personal information mapping within the business) (another element that will require periodic updating of the policy);
- Implements reasonable restrictions for physical access to personal information within the business; and
- Provides for regular monitoring of the business's security program, including documentation of incidents involving a breach of security and post-incident reviews.

How these requirements are applied will depend on the (1) size, scope, and type of business, (2) the amount of resources available to the business, (3) the amount of data stored by the business, and (4) the need for security and confidentiality of both consumer and employee information. In addition, the security program must be reviewed at least annually or when there is a material change in business practices that may affect the security or integrity of personal information.

The Regulation also requires that the written, comprehensive information security program address technical security provisions, which must cover, at a minimum:

- Encryption of all personal information stored on laptops or other portable devices;
- Encryption of all transmitted records and files with personal information over public networks or transmitted wirelessly, to the extent feasible;
- Secure user authentication protocols (e.g., control user IDs, securely assign user IDs and selecting passwords, restrict access to active users, locking users out after multiple failed sign-in attempts, etc.);
- Restrict access to personal information to those who need such information to perform job requirements;
- Monitor electronic systems for unauthorized access;
- Up-to-date firewall protection and system security agent software, including malware protection; and
- Employee education and training on information security and the proper use of the computer security system.

**The encryption requirement as applied to personal information on mobile devices is the first of its kind among federal and state laws applicable to general businesses.** Given the approaching compliance time frame of January 2009, and the prevalence of storing such information on mobile devices for business purposes – from a laptop to a PDA – it is likely that many businesses will need to devise a reasonable strategy to ensure compliance with this requirement, among the others identified in the Regulation.

## PENALTIES

Violations of the Regulation are subject to enforcement under the Massachusetts Unfair Competition Statute.<sup>2</sup>The Massachusetts attorney general may seek a temporary restraining order or a preliminary or permanent injunction against a business that it believes is in violation of the Regulation. If found to be in violation of the law, a court may require that the business pay a civil penalty of up to \$5,000 per violation, as well as the costs of the investigation and attorneys' fees. It remains to be seen what counts as a single violation

<sup>2</sup> Mass. Gen. Laws, ch. 93A.

under the Regulation, but it is likely the enforcers will assert that each aspect of non-compliance with the Regulation, and/or each day of non-compliance, should be considered a separate violation.

### **CIVIL REMEDIES**

Businesses also face the potential of a private action for noncompliance of the Regulation. Massachusetts residents potentially can bring a claim for unfair or deceptive practices under Chapter 93A of the Massachusetts Laws, or a negligence claim using the Regulation (or the statute under which it was issued) to prove that the business had a duty that was breached. Under Massachusetts law, a violation of a statute may constitute per se negligence. If such a case is successfully brought, the exposure is the amount of actual damages or twenty-five dollars, whichever is greater. Additionally, if the court finds that the practice was a willful or knowing violation, the court may order treble damages.

### **CONCLUSION**

Following the trend set by a number of other states, Massachusetts has imposed a rigorous data security standard that will require significant effort and resources from many businesses over the next few months to ensure compliance. While some aspects of this Regulation are novel (e.g., required encryption of personal data on mobile devices, greater specificity on the types of security controls, etc.), most of the requirements in the Massachusetts regulation parallel similar safeguards required by the Federal Trade Commission, and in a host of states, such as California, Texas, Michigan, and Connecticut, among others.

As the number of security breach incidents continues to grow, along with complaints about identity theft, more states are likely to adopt similar or more rigorous information security requirements. The trend continues to be that new state laws carry at least some provisions found in few, if any, other state laws, making compliance an increasing challenge for national

(not to mention global) businesses. Accordingly, businesses that collect or handle personal information would be wise to focus attention on implementing or updating their existing data security programs regularly. Given the regulatory changes over the last few years, and corresponding enforcement by regulators and litigants, such efforts are a critical component of a risk management strategy.

### **For more information about this Client Advisory, please contact:**

**ALYSA Z. HUTNIK**

**(202) 342-8603**

**ahutnik@KelleyDrye.com**

**D. REED FREEMAN**

**(202) 342-8880**

**rfreeman@KelleyDrye.com**