Bloomberg Law Reports® Privacy & Information

New Massachusetts Privacy Regulations Affect Companies Across the Country

By Mary J. Hildebrand, Elaine M. Hughes, and Matthew Savare, Lowenstein Sandler PC

Massachusetts Enacts Strict Privacy Regulations

In response to numerous, high-profile data breaches, 44 states – including New York, New Jersey, California, Delaware, Connecticut, Massachusetts; as well as the District of Columbia, Puerto Rico, and the Virgin Islands – have enacted data security breach notification laws. In February 2009, the Massachusetts Office of Consumer Affairs and Business Regulation issued amended data privacy regulations which are the most comprehensive and restrictive in the nation. These regulations, which become effective on January 1, 2010, apply to all "persons who own, license, store or maintain personal information about a resident of the Commonwealth of Massachusetts." Thus, the broad-based regulations transcend particular industries, and ostensibly apply to all businesses in the financial and investment sectors, including mutual funds, hedge funds, broker-dealers, investment advisers, and banks.

Unlike the privacy laws of other states, which typically require notification *after* a data breach, the revised Massachusetts regulations impose several compliance obligations to *prevent* data breaches.

Requirements Under the New Regulations

Significantly, the new regulations are not restricted to companies that are located or operate in Massachusetts. Instead, they apply to businesses located anywhere in the United States that store or maintain "personal information" about a Massachusetts resident. The law defines "personal information" as a person's name in combination with any one or more of the following: Social Security number, driver's license number, state-issued identification card, financial account number, and credit or debit card number.

There are two primary compliance provisions in the new regulations. First, businesses must develop, implement, maintain, and monitor a comprehensive, written information security program. Second, companies must establish and maintain a security system, which, among other things, encrypts personal information stored on portable devices, or transmitted wirelessly or on public networks.

Security Program Requirements

The law requires the security program to be "reasonably consistent with industry standards," and to contain "administrative, technical, and physical safeguards" to protect the security and confidentiality of personal information. In addition, the program must contain the safeguards set forth in any other state or federal law to which the company may be subject, such as the federal law known as Gramm-Leach Bliley.

Recognizing that such programs could be prohibitively expensive or complicated to implement, the regulations permit businesses to tailor their programs based on their size, scope and type of business; the amount of resources available to the company; the amount of data stored by the

business; and the need for security and confidentiality of both consumer and employee information.

In its security program, a company must address, at a minimum, the following:

1. Designate one or more employees to maintain the program;
2. Identify and assess reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of the personal information;
3. Develop comprehensive security policies for employees;
4. Impose disciplinary measures for violations of the program;
5. Prevent terminated employees from accessing personal information by immediately prohibiting physical or electronic access to such data;
6. Take "all reasonable steps" to verify that any third-party service provider with access to personal information has the ability to protect such data in accordance with the regulations;
7. Limit the amount of personal information collected to only that which is required for the legitimate business purpose for which it was collected; limit the time within which the data is kept; and limit access to such information to only those who are reasonably required to have it;
8. Create a comprehensive inventory of paper and electronic records; computers, including laptops and portable devices; and storage media that contain personal information;
9. Impose reasonable restrictions and safeguards upon the physical access to records containing personal information
10. Monitor and upgrade the program regularly to ensure compliance;
11. Audit the scope of the security system described below at least once a year or whenever there is a material change in business practices that may affect the security of personal information; and
12. Document actions taken in response to any breach of security.

Security System Requirements

In addition to the written security program, companies covered by the regulations must also establish and maintain a security system addressing its computers, including any wireless systems, which must contain, at a minimum, the following elements:

1. Create secure user authentication protocols, including strict control of user IDs and passwords;
2. Develop secure access control measures that restrict access to personal information to only those who need the information to perform their obligations;
3. Encrypt, to the maximum extent technically possible, all data containing personal information that will travel across public networks such as the Internet, and encrypt *all* such data that will be transmitted wirelessly or that is stored on laptops or other portable devices;
4. Monitor systems for unauthorized use of or access to personal information;
5. Utilize reasonably current firewalls and security patches on all systems connected to the Internet that contain personal information;
6. Use reasonably current security software, which must include malware protection and current patches and virus definitions; and
7. Educate and train company employees on the proper use of the security system and the importance of the security of personal information.

Best Practices

The Massachusetts regulations are likely the start of a legislative trend requiring companies to *proactively* protect personal information rather than simply dictating how businesses are to

respond to data breaches. For example, there is a pending bill in Michigan to require companies to encrypt stored personal data in accordance with accepted industry standards.

Given that privacy laws are a patchwork of myriad federal and state statutes, there is no single compliance checklist for companies. Notwithstanding, the following principles are practical ways to mitigate risks.

First, as required in the Massachusetts regulations, companies should collect only data that is actually necessary to conduct their businesses and retain data for only as long as it is needed.

Second, companies should adopt, implement, and periodically audit a comprehensive security program like the one required under Massachusetts law. This includes utilizing robust electronic and physical safeguards to protect and monitor their consumers' and employees' personal information.

Third, companies should create strict internal procedures dictating how they will address security breaches. Fourth, companies engaging outside vendors to store, process, transmit, or destroy data containing personal information should thoroughly investigate the company and determine whether its privacy practices are adequate.

Finally, companies that process or store personal information should consider obtaining cyber-insurance, which covers a broader range of privacy and identity theft claims than general liability policies.

Mary J. Hildebrand is a Member of the law firm Lowenstein Sandler, PC. She focuses on strategic planning, commercialization, protection, and management of intellectual property and technology assets in the United States and many foreign jurisdictions.

Elaine Hughes is a Member of the law firm Lowenstein Sandler, PC. She focuses on private equity, venture capital and hedge fund formation, compliance and investment.

Matthew Savare is an Associate with the law firm Lowenstein Sandler, PC. He focuses on copyright and trademark law matters, information privacy issues, cybersquatting, domain name disputes and technology licensing.