# Massachusetts Adopts Strict Security Regulations Governing Personal Information

LISA M. ROPPLE, KEVIN V. JONES, AND CHRISTINE M. SANTARIGA

*Establishing itself as a leader in the data security area, Massachusetts recently promulgated the "Standards for the Protection of Personal Information of Residents of the Commonwealth" pursuant to the state's security breach notification law enacted in 2007. According to the authors, the new regulations may present a daunting compliance challenge for companies handling personal information about Massachusetts residents.*

As security breaches at major businesses continue to generate frequent headlines, the Massachusetts Office of Consumer Affairs and Business Regulation (the "OCA") has issued groundbreaking new regulations imposing significant duties on companies and organizations that have personal information about Massachusetts residents.[1]

Effective January 1, 2010, the regulations require companies to develop a comprehensive written information security program to safeguard any electronic or paper record that contains such information. The program must include minimum features identified in the regulations, some of

---

Lisa M. Ropple is a partner and Kevin V. Jones is an associate in the Litigation Department of Ropes & Gray LLP; both have expertise in complex data breach litigation and governmental investigations. Christine M. Santariga is an associate in the Corporate Department of Ropes & Gray LLP who advises companies on technology and data security and privacy compliance matters. All are members of the firm's Privacy Group.



Published in the April 2009 issue of Privacy & Data Security Law Journal.

which are familiar from other data security guidance, but some of which are novel and demanding. In addition, companies that electronically store or transmit personal information about Massachusetts residents must ensure that their computer systems meet a number of specific technical requirements and must provide training to employees on the computer system and the importance of data security.

In announcing these regulations, Massachusetts has established itself as a leader in the data security area. The latest in an emerging trend of increased state regulation of how companies protect personal information, Massachusetts's new rules are the most far reaching and technically specific of any existing state data security laws and exceed federal data security regulations and guidance.

This article highlights key features of the Massachusetts regulations. With the regulations scheduled to become effective in only nine months and advance time necessary to effectively implement the new measures, companies need to assess their security programs and computer systems and take action promptly to ensure compliance.

## SCOPE OF MASSACHUSETTS REGULATIONS

The "Standards for the Protection of Personal Information of Residents of the Commonwealth" were promulgated pursuant to the security breach notification law that Massachusetts enacted in 2007.[2] That law, in turn, was enacted under the state's general consumer protection laws prohibiting unfair and deceptive trade practices.[3]

The regulations impose "minimum standards" for safeguarding personal information of Massachusetts residents, to (1) ensure the security and confidentiality of such information in a manner consistent with industry standards; (2) protect against threats or hazards to the security of such information; and (3) protect against unauthorized access to or misuse of such information in a manner that creates a substantial risk of identity theft or fraud against such residents.

### Who Is Subject to the Regulations?

The regulations apply to all persons (defined broadly to include corpo-

rations, associations, and other legal entities) that "own, license, store, or maintain" personal information about Massachusetts residents. The regulations purport to apply both inside and outside Massachusetts, reaching any entity, wherever located, that has information about a Massachusetts resident. The regulations exempt from their broad reach only state governmental agencies; they provide no size limitation or other exemption.

### What Information Is Subject to the Regulations?

The regulations extend to paper and electronic records that contain "personal information" about a Massachusetts resident. "Personal information" is defined as a resident's first name or initial and last name *in combination with* certain sensitive items, such as a Social Security number, driver's license number, financial account number, or debit or credit card number.

This definition of "personal information" is consistent with the definition used in the data breach notification laws that most states have enacted.[4] As in the notification laws, the definition appears designed to circumscribe the regulations' application only to information that, if lost or stolen, would give rise to a substantial risk of misuse by an unauthorized person to commit identity theft or fraud.[5] Where this risk is not present — for example, in the case of an e-mail address or credit card number standing alone — such information properly does not fall within the definition of "personal information" and is not subject to the regulations.

Even with these limitations, however, the definition of "personal information" reaches a wide range of records commonly kept by organizations in many different industries, such as records containing customer information, investor information, patient information, or student information. Because employee and payroll records are highly likely to contain "personal information," virtually any employer of a Massachusetts resident will be subject to the regulations.

## INFORMATION SECURITY PROGRAM

The Massachusetts regulations require companies to implement and maintain a "comprehensive, written information security program" to protect the security and confidentiality of personal information. Under

this information security program, a company must engage in an ongoing process of assessing reasonably foreseeable risks to personal information it handles and addressing those risks through the use of administrative, physical, and technical safeguards. This concept of an information security program is not new, as it is the cornerstone of federal data security guidance applicable to financial institutions under the Gramm-Leach-Bliley Act[6] and numerous consent orders issued by the Federal Trade Commission ("FTC")[7] and has been mandated by at least one other state.[8]

The Massachusetts regulations, however, go further than these pre-existing authorities in defining the elements of such a program. Unlike federal or state precursors, the regulations provide specific direction with respect to the content of a sufficient information security program. First, the regulations provide four factors against which the sufficiency of a company's information security program shall be evaluated:

1. The company's size, scope, and type of business;
2. The company's resources;
3. The amount of stored data; and
4. The need for security and confidentiality of the information.

Second, they mandate minimum requirements for a compliant information security program. Under the regulations, every information security program (regardless of the four factors enumerated above) must contain the following elements:

- *Program Oversight*: Companies must designate an employee or group of employees to oversee the information security program.
- *Security Policies*: Companies must develop security policies for their employees, particularly with respect to off-site use of personal information. They also must impose disciplinary measures for security violations.
- *Need-to-Know Access*: Companies must limit access to personal information on a need-to-know basis and must terminate immediately the access of employees who leave the company.

- *Physical Security*: Companies must place reasonable restrictions on physical access as documented in a written procedure and must lock areas or containers that include personal information.
- *Service Providers*: Companies must take reasonable steps to verify and ensure that outside service providers, if given access to personal information, have the capacity to protect it in the manner provided for in the regulations and that any such service provider applies protective security measures at least as stringent as those required for personal information under the Massachusetts regulations.
- *Data Minimization*: Companies must limit the amount of personal information that they collect and the length of time they retain it to only that which is reasonably necessary.
- *Data Inventory*: Companies must conduct a data inventory to identify where they are storing personal information, both in electronic and paper form, unless they treat all records as if they contain personal information.
- *Monitoring and Evaluation*: Companies must evaluate and monitor the information security program and underlying safeguards on an ongoing basis to ensure its continued effectiveness.
- *Security Incidents*: Companies must document responsive actions taken in connection with any incident involving a security breach, including any changes in their business practices.

The regulations also expressly address their interrelationship with other data security standards. They direct that the information security program must be "reasonably consistent with industry standards" and consistent with safeguards for the protection of such data set forth in any other state or federal regulation that applies to the company.

## COMPUTER SYSTEM SECURITY REQUIREMENTS

In addition to the obligations addressed above, for companies that electronically store or transmit personal information, the Massachusetts regulations impose a host of technical security requirements that the com-

pany's computer systems must meet. These requirements include:

- *Access Controls*: Companies must implement secure user authentication protocols and secure access control measures, including unique user identification, non-default passwords, and secure password storage, among other requirements.
- *Encryption*: Companies must encrypt personal information when it is stored on laptops or other portable devices, when it is transmitted over wireless systems, and (to the extent feasible) when it travels across public networks. The OCA has stressed the importance of these encryption requirements, noting that most breaches involve portable devices and that encryption would help neutralize the risk to consumers.
- *Monitoring*: Companies must reasonably monitor their systems for unauthorized access to or use of personal information.
- *Segmentation*: Companies must have "reasonably up-to-date" firewall protection for systems connected to the Internet that contain personal information.
- *Antivirus and Patching*: Companies also must have "reasonably up-to-date" antivirus software and security patches.
- *Employee Training*: Companies must educate and train their employees on the proper use of the computer security system and the importance of personal information security.

## COMPLIANCE CHALLENGE

When the regulations were first issued on September 19, 2008, they carried an effective date of January 1, 2009, which would have given companies only a few months to achieve compliance with all of the requirements. Business groups warned that this aggressive deadline would be overly burdensome or even impossible to meet, given the unprecedented scope and technical specificity of the regulations. In response to this public outcry and in light of deteriorating economic conditions, the OCA announced on November 14, 2008 that it had extended the deadline to May 1, 2009 for most of the requirements and to January 1, 2010 for some of

the most challenging requirements, including the encryption of personal information on certain portable devices.

Despite this deadline extension, the outcry continued. At a public hearing on January 16, 2009, the room could not accommodate the number of attendees from business groups and companies there to ask questions and voice concerns about the regulations. On February 12, 2009, the OCA responded to such concerns by extending the compliance deadline for all of the requirements to January 1, 2010. In addition, the OCA clarified a number of requirements that had caused confusion and eliminated a controversial requirement that companies obtain written compliance certifications from their service providers before allowing them to access personal information.

Even with the extended deadlines, complying with the Massachusetts regulations will present a challenge for many companies. Designing and implementing a comprehensive information security program and complying with the technical computer systems requirements will require considerable time and resources, careful planning, and oversight. Even with a substantial investment, there are significant questions about whether compliance with some of the new rules realistically can be achieved or is fair to expect. Given the lead time necessary to plan for and implement some of these significant requirements, companies handling personal information of Massachusetts residents will need to take action as soon as possible.

## ENFORCEMENT

The statute under which the Massachusetts regulations were issued[9] authorizes the state Attorney General to remedy violations by bringing an action alleging unfair or deceptive business practices under the state's consumer protection statute.[10] Violations could result in injunctive relief and, in some circumstances, civil penalties. The Attorney General's Office has stated publicly that it is in the process of developing enforcement guidelines.

## EMERGING TREND AMONG STATES

Massachusetts is not alone among states in enhancing its regulation of information security. During the past five years, states have become

increasingly active in the data security area. Their efforts have resulted in a variety of legislative and regulatory initiatives, including:

- *Breach Notification Laws*. Almost every state has passed a security breach notification law requiring companies to notify consumers and/or regulators when personal information is subject to unauthorized access or acquisition.[11] Most of these laws follow the same basic format, which is based on the first such law passed by California in 2003.[12] But some states, including Massachusetts, have incorporated their own unique requirements, which, in some respects, conflict with other states' breach laws. For example, the Massachusetts law prohibits companies from disclosing the nature of the security breach in its notification to residents,[13] while other states expressly require companies to include such information in their notices.[14]
- *Reasonable Security Laws*. About one-fifth of the states have passed laws requiring companies to maintain reasonable security procedures and practices to protect personal information from unauthorized access or acquisition.[15] These laws require generally that companies implement reasonable security measures, rather than directing companies to implement any specific security measures as the Massachusetts regulations do. Oregon, however, specifically requires companies to maintain reasonable security by adopting an information security program similar to the one mandated by the Massachusetts regulations.[16]
- *Data Disposal Laws*. About half of the states have passed laws requiring the secure disposal or destruction of records containing personal information when retention is no longer necessary for business purposes.[17] These laws typically provide that companies must take reasonable steps to shred, burn, or pulverize paper records and to destroy, erase, or otherwise modify electronic records such that the personal information contained in them is rendered unreadable or undecipherable through any means.
- *Data Encryption Laws*. Nevada passed a law, effective October 2008, that requires companies doing business in that state to encrypt any customer personal information that is transmitted electronically to a

person outside the company's secure system, with the exception of facsimiles.[18] This law is similar to one of the technical requirements in the Massachusetts regulations, except that the Massachusetts requirement is limited to transmissions over public networks and does not require encryption if it is technically infeasible.

- *Social Security Number Laws*. More than half of the states have passed laws regulating the security of Social Security numbers.[19] These laws typically prohibit companies from requiring a person to transmit his or her Social Security number over the Internet, unless the connection is secure or the number is encrypted. They also typically prohibit companies from requiring a person to use his or her Social Security number to access a web site, unless another authentication device is also required. In a few instances, these laws require companies to limit employee access to Social Security numbers[20] or to develop and make publicly available a written privacy policy that describes how they protect Social Security numbers.[21]
- *Payment Card Information Laws*. State legislative efforts also have been directed at securing credit card information in particular. Minnesota, for example, passed a law, effective August 2007, that generally prohibits a company doing business in Minnesota from retaining full magnetic-stripe data, PIN verification data, or card security code data past the authorization of a transaction.[22]

While not exhaustive, these laws demonstrate the states' increasing regulation of personal information security.

## CONCLUSION

The new Massachusetts regulations, with their sweeping scope and unprecedented technical specificity, push the advancing front of state data security regulation to a new frontier. Massachusetts has positioned itself at the leading edge of personal information security regulation, in much the same way that California did when it became the first state to pass a security breach notification law in 2003.[23] Whether other states will fol-

low Massachusetts's lead, as they did California's, remains to be seen. For now, the Massachusetts regulations present a daunting compliance challenge for companies handling personal information about Massachusetts residents.

## NOTES

[1] 201 MASS. CODE REGS. § 17.00 (issued pursuant to Mass. Gen. Laws ch. 93H).

[2] MASS. GEN. LAWS ch. 93H.

[3] MASS. GEN. LAWS ch. 93H, § 6 (authorizing enforcement under Mass. Gen. Laws ch. 93A).

[4] These states include Alaska (ALASKA STAT. 45.48.010 *et seq.*), Arizona (ARIZ. REV. STAT. § 44-7501), Arkansas (ARK. CODE § 4-110-101 *et seq.*), California (CAL. CIV. CODE § 1798.82), Colorado (COLO. REV. STAT. § 6-1-716), Connecticut (CONN. GEN. STAT. § 36a-701b), Delaware (DEL. CODE ANN. tit. 6, § 12B-101 *et seq.*), District of Columbia (D.C. CODE § 28-3851 *et seq.*), Florida (FLA. STAT. § 817.5681), Georgia (GA. CODE § 10-1-910 *et seq.*), Hawaii (HAW. REV. STAT. § 487N-2), Idaho (IDAHO CODE § 28-51-104 *et seq.*), Illinois (ILL. COMP. STAT. ch. 815, § 530/1 *et seq.*), Indiana (IND. CODE § 4-1-11), Iowa (IOWA CODE § 715C.1), Kansas (KAN. STAT. § 50-7a01 *et seq.*), Louisiana (LA. REV. STAT. § 51:3071 *et seq.*), Maine (ME. REV. STAT. tit. 10, § 1347 *et seq.*), Maryland (MD. CODE, COM. LAW § 14-3501 *et seq.*), Massachusetts (MASS. GEN. LAWS ch. 93H), Michigan (MICH. COMP. LAWS § 445.72), Minnesota (MINN. STAT. §§ 325E.61, 325E.64), Montana (MONT. CODE 30-14-1701 *et seq.*), Nebraska (NEB. REV. STAT. § 87-801 *et seq.*), Nevada (NEV. REV. STAT. § 603A.010 *et seq.*), New Hampshire (N.H. REV. STAT. § 359-C:19 *et seq.*), New Jersey (N.J. STAT. § 56:8-163), New York (N.Y. GEN. BUS. LAW § 899-aa), North Carolina (N.C. GEN. STAT. § 75-65), North Dakota (N.D. CENT. CODE § 51-30-01 *et seq.*), Ohio (OHIO REV. CODE § 1349.19 *et seq.*), Oklahoma (OKLA. STAT. § 74-3113.1), Oregon (OR. REV. STAT. 646A.600 *et seq.*), Pennsylvania (73 PA. STAT. § 2303), Rhode Island (R.I. GEN. LAWS § 11-49.2-1 *et seq.*), South Carolina (S.C. CODE § 39-1-90), Tennessee (TENN. STAT. § 47-18-2107), Texas (TEX. BUS. & COM. CODE § 48.103), Utah (UTAH CODE § 13-44-101 *et seq.*), Vermont (VT. STAT. tit. 9, 2430 *et seq.*), Virginia (VA. CODE ANN. § 18.02-186.6), Washington (WASH. REV. CODE § 19.255.010), West Virginia (W.V. CODE § 46A-2A-101 *et seq.*), Wisconsin (WIS. STAT. § 134.98 *et seq.*),



Published in the April 2009 issue of Privacy & Data Security Law Journal.

and Wyoming (Wyo. Stat. § 40-12-501).

[5] *See* Mass. Gen. Laws ch. 93H, § 1(a) (defining "breach of security" as the unauthorized acquisition or use of data that "creates a substantial risk of identity theft or fraud against a resident of the commonwealth").

[6] 15 U.S.C. § 6801 *et seq.*, enforced under FTC "Safeguards Rule," 16 C.F.R. § 314.

[7] A list of recent FTC enforcement actions relating to data security and privacy is available at http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html.

[8] *See* Or. Rev. Stat. § 646A.622.

[9] Mass. Gen. Laws ch. 93H.

[10] Mass. Gen. Laws ch. 93A, § 4.

[11] *See supra* note 4.

[12] Cal. Civ. Code § 1798.82.

[13] Mass. Gen. Laws 93H § 3.

[14] *See, e.g.*, Iowa Code § 715C.2; N.H. Rev. Stat. § 359-C:20; Or. Rev. Stat. § 646A.604.

[15] These states include Arkansas (Ark. Code § 4-110-104), California (Cal. Civ. Code § 1798.81.5), Connecticut (Conn. Pub. Acts No. 08-167), Maryland (Md. Code, Comm. Law § 14-3501), Nevada (Nev. Rev. Stat. § 603A.210), Rhode Island (R.I. Gen. Laws § 11-49.2), Texas (Tex. Bus. & Com. Code § 48.102), and Utah (Utah Code § 13-44-201).

[16] Or. Rev. Stat. § 646A.622.

[17] These states include Arizona (Ariz. Rev. Stat. § 44-7601), Arkansas (Ark. Code § 4-110-104), California (Cal. Civ. Code § 1798.81), Colorado (Colo. Rev. Stat. § 6-1-713), Connecticut (Conn. Pub. Acts No. 08-167), Georgia (Ga. Laws § 10-15-2), Hawaii (Haw. Rev. Stat. § 487R-2), Indiana (Ind. Code § 24-4-14), Kansas (Kans. Stat. § 50-7a03), Kentucky (Ky. Rev. Stat. § 365.725), Maryland (Md. Code, Com. Law § 14-3501), Massachusetts (Mass. Gen. L. ch. 93I, § 2), Michigan (Mich. Comp. Laws § 445.72a), Montana (Mont. Code § 30-14-1702-3), Nevada (Nev. Rev. Stat. § 603A.200), New Jersey (N.J. Stat. § 56:8-162), New York (N.Y. Gen. Bus. Law § 399-h), North Carolina (N.C. Gen. Stat. § 75-60), Oregon (Or. Rev. Stat. § 646A.622), Tennessee (Tenn. Code § 39-14-150), Texas (Tex. Bus. & Com. Code §§ 35.48, 48.102, 72.001-4), Utah (Utah Code § 13-44-201), and Vermont (Vt. Stat. tit. 9, § 2445).

[18] Nev. Rev. Stat. § 597.970.

[19] These states include Alaska (ALASKA STAT. § 45.58.400) Arizona (ARIZ. REV. STAT. § 44-1373), Arkansas (ARK. CODE § 4-56-107), Colorado (COLO. REV. STAT. § 6-1-715), Connecticut (CONN. GEN. STAT. § 42-470), Georgia (GA. LAWS § 10-1-393.8), Hawaii (HAW. REV. STAT. § 487J-2), Kansas (KANS. STAT. § 75-3520), Maine (ME. REV. STAT. tit. 10, § 1271-3), Maryland (MD. CODE, COM. LAW § 14-3401-3), Michigan (MICH. COMP. LAWS § 445.81-87), Minnesota (MINN. STAT. § 325E.59), Missouri (MO. STAT. § 407-1355), Nebraska (NEB. REV. STAT. § 48-237), New Jersey (N.J. STAT. § 56:8-164), New Mexico (N.M. STAT. § 57-12B-1-4), New York (N.Y. GEN. BUS. LAW § 399-dd, N.Y. LABOR LAW § 203-d), North Carolina (N.C. GEN. STAT. § 75-62), Oklahoma (OKLA. STAT. tit. 40, § 173.1), Oregon (OR. REV. STAT. § 646A.620), Pennsylvania (74 PA. STAT. § 201), Rhode Island (R.I. GEN. LAWS § 6-48-8), South Carolina (S.C. CODE § 37-20-180), Tennessee (TENN. CODE § 47-18-2110), Texas (TEX. BUS. & COM. CODE § 35.58), Utah (UTAH CODE § 13-45-301), Vermont (VT. STAT. tit. 9, § 2440), and Virginia (VA. CODE § 59.1-443.2).

[20] *See, e.g.*, MINN. STAT. § 325E.59.

[21] *See, e.g.*, CONN. PUB. ACTS No. 08-167.

[22] MINN. STAT. § 325E.64.

[23] CAL. CIV. CODE § 1798.82.