



# PRIVACY & SECURITY LAW



## REPORT

Reproduced with permission from Privacy & Security Law Report, Vol. 07, No. 41, 10/20/2008, pp. 1518-1521. Copyright © 2008 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>

### Corporate Data Security

#### State Requirements

## New State Regulations Signal Significant Expansion Of Corporate Data Security Obligations

By THOMAS J. SMEDINGHOFF  
AND LAURA E. HAMADY

**S**weeping new security regulations issued by the Commonwealth of Massachusetts are the latest evidence of the accelerating development of two key legal trends. The first is the expanding scope of the duty imposed on companies to provide reasonable security for their data. The second is the growing reliance on requirements for the use of encryption in certain cases.

On Sept. 22, 2008, the Massachusetts Office of Consumer Affairs and Business Regulation released its “Standards for Protection of Personal Information of

Residents of the Commonwealth”<sup>1</sup> as required by the 2007 Massachusetts security breach and data destruction law.<sup>2</sup> They are effective Jan. 1, 2009, and apply to “all persons that own, license, store or maintain personal information about a resident”<sup>3</sup> of Massachusetts. As such, they are likely to have a broad and significant nationwide impact similar to that of California’s pioneering breach notification law, S.B. 1386 enacted in 2003, and may inspire other states to adopt similar legislation using the regulations as a template.

The Regulations, together with the security breach and data destruction provisions of Massachusetts law, constitute one of the most comprehensive sets of general security regulation yet seen at the state level. At the same time, however, these Regulations are clearly modeled after aspects of developing data security law at the federal level, making them perhaps a logical next step in the continuing expansion of corporate security obligations.

Like the law in at least nine other states—Arkansas, California, Connecticut, Maryland, Nevada, Rhode Is-

*Thomas J. Smedinghoff is a partner and Laura E. Hamady is an associate in the Privacy & Data Security Law Practice at the law firm of Wildman Harrold, in Chicago. Mr. Smedinghoff recently authored INFORMATION SECURITY LAW: THE EMERGING STANDARD FOR CORPORATE COMPLIANCE (IT Governance Publishing, 2008). They can be reached at [smedinghoff@wildman.com](mailto:smedinghoff@wildman.com) and [hamady@wildman.com](mailto:hamady@wildman.com).*

<sup>1</sup> 201 CMR 17.00 *et. seq.*  
<sup>2</sup> Mass. Gen. Laws. Ch. 93H, § 2(a)  
<sup>3</sup> 201 CMR 17.01(b).

land, Oregon, Texas, and Utah—the Massachusetts Regulations are intended to protect the “security and confidentiality” of personal information about residents. But unlike those other state laws, which merely obligate companies to provide “reasonable security” to achieve that goal, these Regulations require companies to:

- Implement a risk-based, process-oriented, “**comprehensive, written information security program**” in accordance with a detailed list of requirements; and
- **Encrypt** all personal information stored on laptops or other portable devices, all records and files transmitted over public networks “to the extent technically feasible,” and all data transmitted wirelessly.

### A. Duty to Implement Comprehensive Written Information Security Program

The heart of the Regulations is the requirement that businesses “develop, implement, maintain and monitor a *comprehensive, written information security program*” designed to ensure the security and confidentiality of any records containing personal information. Such comprehensive information security program must be reasonably consistent with industry standards, and must include appropriate administrative, technical, and physical safeguards for such records.

While new at the state level, the basic requirements for a comprehensive security program set out in the Regulations are largely a restatement of the legal definition of “reasonable security” that has evolved over the past several years. Similar requirements are embodied in a series of existing federal financial and health care industry regulations and FTC enforcement actions. Massachusetts has now extended that approach to all businesses that maintain personal information of Massachusetts residents.

As such, the Regulations are the next logical step in a trend that began in 2004 when states began enacting legislation imposing a general obligation on all companies to “implement and maintain reasonable security procedures and practices” to protect personal information about residents from unauthorized access, destruction, use, modification, or disclosure. By adopting the Regulations, Massachusetts has, in effect, become the first state to formalize the definition of “reasonable security” under those laws.

#### 1. History

The obligation to develop and implement a comprehensive written information security program first appeared several years ago in sector-specific legislation and regulations at the federal level. It is required by the Gramm-Leach-Bliley Act financial industry security regulations titled *Guidelines Establishing Standards for Safeguarding Consumer Information* issued by the Federal Reserve, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, and the Office of Thrift Supervision, Feb. 1, 2001,<sup>4</sup> and later adopted by the FTC in its *Safeguards Rule* May 23,

<sup>4</sup> 66 Fed. Reg. 8616, Feb. 1, 2001; 12 C.F.R. Part 30, Appendix B, § II.A (OCC), 12 C.F.R. Part 208, Appendix D-2, § II.A (Federal Reserve System), 12 C.F.R. Part 364, Appendix B, Section II.A (FDIC), 12 C.F.R. Part 570, § II.A (Office of Thrift Supervision).

2002.<sup>5</sup> It is also required by the Federal Information Security Management Act of 2002 (“FISMA”), which applies to government agencies,<sup>6</sup> and somewhat indirectly by the Health Insurance Portability and Accountability Act (“HIPAA”) *Security Standards* issued by the Department of Health and Human Services Feb. 20, 2003,<sup>7</sup> which apply in the healthcare sector.

Before the ink was dry on this slate of federal regulations, however, we began to see a shift from a sector-specific approach to a more general one. The requirement for a comprehensive information security program was quickly adopted by the Federal Trade Commission as “best practices” that could be applied to all businesses and all industries in an enforcement context.<sup>8</sup> Thus, beginning in 2002, when the FTC began pursuing companies in a variety of non-regulated industries based on an alleged failure to provide adequate security for their data, all of the settlements and consent decrees in these cases required the defendants to develop and implement a comprehensive information security program.

Starting in 2004, several states also began passing laws imposing a general obligation on all companies to implement information security. The first was California, which enacted legislation requiring all businesses to “implement and maintain *reasonable security* procedures and practices” to protect personal information about California residents from unauthorized access, destruction, use, modification, or disclosure.<sup>9</sup> Thereafter, several states<sup>10</sup> enacted similar statutes. Most of these laws, however, did not define what constituted “reasonable security.”

That began to change in 2007 when Oregon enacted its security legislation. The Oregon statute expressly stated that its requirement for “reasonable safeguards” could be satisfied by compliance with the GLB Security Regulations, the HIPAA Security Regulations, or implementation of an information security program specified in the statute.<sup>11</sup> However, the foregoing were set forth only as a safe harbor for compliance, and the statute appears to leave open the possibility that there might be other approaches to “reasonable security.”

With its 2008 Regulations, Massachusetts became the first state to formally require a comprehensive written information security program and to define the mandatory requirements for such a program. Yet its requirements are similar to the approach in Oregon, and taken together, they represent the first state law definitions of

<sup>5</sup> 67 Fed. Reg. 36484, May 23, 2002; 16 C.F.R. Part 314.

<sup>6</sup> 44 U.S.C. § 3544(b).

<sup>7</sup> 45 C.F.R. Part 164.

<sup>8</sup> In March 2005 testimony before Congress, the Chairman of the Federal Trade Commission, Deborah Platt Majoras, provided further support for this view by suggesting that the extensive scope of the security obligations imposed on the banking industry should be expanded to cover all industries. “Senate Banking Committee Members Grill ChoicePoint Executive on Breaches,” BNA’s *Privacy & Security Law Report*, March 21, 2005 at p. 351 (4 PVL 351, 3/21/05).

<sup>9</sup> Cal. Civil Code § 1798.81.5(b) (emphasis added).

<sup>10</sup> See, e.g., Ark. Code Ann. § 4-110-104(b); Conn. Public Act No. 08-167; Md. Commercial Law Code Ann. § 14-3503; Mass. Gen. Laws. Ch. 93H, § 2(a); Nev. Rev. Stat. 603A.210; R.I. Stat. 11-49.2-2(2) and (3); Oregon Rev. Stat. § 646A.622; Tex. Bus. & Com. Code Ann. § 48.102(a); and Utah Code Ann. § 13-44-20.

<sup>11</sup> Or. Rev. Stat. § 646A.622.

“reasonable security” generally applicable to all businesses. But what is most noteworthy is the fact that the requirements in both states essentially mirror those imposed by the federal regulations and the FTC consent decrees.

## 2. Overview of the Obligation

The requirement for a comprehensive written information security program in all of the foregoing laws (including the new Massachusetts Regulations) is based on the view that data security is a relative concept, and thus, that providing “reasonable security” requires a fact-specific, risk-based, process that reflects the company’s current business realities, and is designed to respond to technological, regulatory and business-related changes. With some notable exceptions discussed below, the law generally rejects a one-size-fits-all approach to the specifics of a security program making it impossible to comply with these laws merely by implementing technologically sophisticated security “solutions.”<sup>12</sup>

These laws and regulations typically mandate a comprehensive security program that is, at its heart, an ongoing and repetitive process of assessment and verification; this legal requirement can be summarized by the phrase “*process plus categories*”—i.e., to satisfy its legal obligations to implement “reasonable security” a company must engage in a defined risk-based “*process*” to identify and implement appropriate security controls, which must include consideration of requirements in selected “*categories*” of security controls.

## 3. The Process

Like existing federal regulations and FTC policy, the Massachusetts Regulations and Oregon statute require each covered company to implement the following process as part of the mandated comprehensive security program:

- **Assign Responsibility:** Designate one or more employees to maintain the security program;
- **Identify Information Assets:** Identify the corporate information assets that need to be protected, including records containing personal information and computing systems and storage media (such as laptops and portable devices) used to store such personal information;
- **Conduct Risk Assessment:** Conduct a risk assessment to identify and assess internal and external risks to the security, confidentiality, and/or integrity of its information assets, and evaluate the effectiveness of the current safeguards for minimizing such risks;
- **Implement Security Controls:** Select and implement appropriate physical, administrative, and technical security controls to minimize the risks identified in its risk assessment, including security controls within certain identified “categories”;
- **Monitor Effectiveness:** Regularly monitor and test the security controls it has implemented to ensure that the security program is operating in a manner reasonably calculated to protect the personal infor-

mation; and upgrade the security controls as necessary to limit risks;

- **Regularly Review Program:** Review and adjust the security program at least annually, including: (i) whenever there is a material change in business practices that could affect personal information, and (ii) following any incident involving a breach of security; and
- **Address Third Party Issues:** Carefully select, retain and supervise contractors and third party service providers that have access to the company’s personal information by (i) taking reasonable steps to verify that they are capable of maintaining safeguards for the personal information; (ii) contractually requiring them to maintain such safeguards and to provide appropriate assurances, and (iii) monitoring their compliance with those commitments.

Where the Massachusetts Regulations differ somewhat from federal law is in how they address the required categories of security controls.

## 3. The Categories

The Massachusetts Regulations, like other laws requiring a comprehensive security program, specify certain *categories* of physical, administrative, and technical security controls that a covered company must address as part of the process to implement its security program. However, they also include specific requirements for encryption. They may be summarized as follows:

- The **Physical Security Controls** must include:
  - ✓ reasonable restrictions on physical access to records; and
  - ✓ storage of such records and data in locked facilities, storage areas or containers.
- The **Administrative Security Controls** must include:
  - ✓ Limits on the amount of personal information collected, the time such information is retained, and the persons who are allowed to access it;
  - ✓ Policies regarding employee access and transport of records outside of business premises;
  - ✓ Disciplinary measures for violations of the security program;
  - ✓ Procedures to prevent terminated employees from accessing records; and
  - ✓ Security education and training for employees.
- The **Technical Security Controls** must include the following elements:
  - ✓ Secure user authentication protocols;
  - ✓ Secure access control measures that restrict access to those who need such information to perform their job duties and assign unique identifications plus passwords to each person with computer access;
  - ✓ Encryption of all records containing personal information that travel across the Internet, are transmitted wirelessly, or are stored on laptops or other portable devices;
  - ✓ Monitoring of systems for unauthorized use of or access to personal information; and
  - ✓ Up-to-date firewall protection, operating system security patches for systems connected to the Internet, and up-to-date software providing malware and virus protection.

For the most part, the foregoing list specifies categories of required security controls, but generally leaves it

<sup>12</sup> For a more detailed examination of the legal requirements for “reasonable security” see Smedinghoff, “The State of Information Security Law: A Focus on the Key Legal Trends,” available at <http://ssrn.com/abstract=1114246>.

up to the company to determine how such categories will be addressed, consistent with its risk assessment. For example, the business is free to determine how it will satisfy requirements for security education and training, disciplinary measures for violations of the security program, and secure authentication protocols. However, the exacting nature of the Regulation's security categories raises at least two issues.

First, some have argued that the Massachusetts Regulations include categories of controls not found in federal regulations, thus complicating the compliance process. For example, the requirement that companies implement procedures to prevent terminated employees from accessing records is not expressly found in other laws, such as the GLB regulations. In many cases, however, such requirements are likely implied in other laws by the general process requirement to select and implement appropriate physical, administrative, and technical security controls to minimize the risks identified in the risk assessment. Only if there was no risk of unauthorized access by terminated employees would there be no need for such procedures in the comprehensive security program.

Second, and most significantly, however, is the Massachusetts requirement for encryption in certain cases.

## B. Duty to Encrypt Data

In a departure from reliance solely on a risk-based approach, the Massachusetts Regulations as well as some other newer state laws are beginning to impose obligations to use encryption in certain situations regardless of the presence or absence of otherwise reasonable security.

The trend began with laws regulating the transmission of social security numbers. Laws enacted in Arizona, California, and Connecticut, for example, mandated encryption of Social Security numbers in the limited situation where a company required an individual to transmit his or her Social Security number over the Internet.<sup>13</sup> Maryland later expanded the scope of this provision to also prohibit companies from initiating their own transmission of an individual's Social Security number over the Internet unless it was "encrypted or the connection was secure."<sup>14</sup>

Then, Oct. 1, 2008, a Nevada law took effect which prohibited the electronic transmission of any personal information<sup>15</sup> to a person outside of the secure system of the business (other than a facsimile) unless the information is encrypted.

The Massachusetts Regulations take the encryption requirement significantly farther, however. They require any entity that **stores or transmits** electronic records containing personal information to encrypt that information in specific situations.<sup>16</sup> Specifically:

- **Stored** personal information must be encrypted if it is stored on "laptops or other portable devices." While "portable device" is not defined, it is presumably includes portable communication devices such as Blackberries and cell phones, as well as portable storage devices such as iPods and USB flash drives.
- Personal information being **transmitted** must also be encrypted, "to the extent technically feasible" if it "will travel across public networks," or if it will "be transmitted wirelessly." Public networks clearly include the Internet and wireless transmission presumably includes communication even within a corporate network.

Such an absolute requirement for encryption of stored personal data, particularly on laptops and portable devices, represents a departure from existing law.<sup>17</sup> Legislative history of the Massachusetts Regulations at least, suggest that lawmakers are focused on these devices as a primary source of data breaches and are intent on providing regulatory incentives to prevent them in the future. However, whether mandating encryption or other technologically and procedurally specific requirements becomes a trend remains to be seen.

The definition of encryption, however, presents a unique challenge with all of these statutes. In many cases, issues such as what qualifies as encryption, and how strong it must be, are left unclear.

The Massachusetts regulations define "encryption" generally as "the transformation of data through the use of an algorithmic process, or an alternative method at least as secure, into a form in which meaning cannot be assigned without the use of a confidential process or key." By providing "an alternate method" to the standard algorithm approach to encryption, the regulations seem to provide for some flexibility in approach so long as the alternative method is "at least as secure" and the data is transformed "into a form in which meaning cannot be assigned without the use of a confidential process or key." However, what qualifies as an alternate method is unclear. The "at least as secure" requirement, for example, seems confusing and inconsistent, especially given the fact that Massachusetts specifies 128 bit encryption in its breach law and that the strength of differing encryption methods varies widely.

The definitions of encryption in other statutes are similarly ambiguous. The Nevada statute, for example, defines encryption as "the use of any protective or disruptive measure, including, without limitation, cryptography, enciphering, and coding or computer contaminant, to: (1) prevent, impede, delay or disrupt access to any data, information, image, program, signal or sound; (2) cause or make any data, information, image, program, signal or sound unintelligible or unusable; or (3) prevent, impede, delay or disrupt the normal operation or use of any component, device, equipment, system, or network." Because of the broad nature of this definition, and the fact that it does not absolutely require an algorithmic approach to encryption as found in cryptography, some have argued that other less-secure schemes to deter readability of data, such as file passwords, might also qualify. Whether such non-cryptographic approaches will qualify as encryption is one of the many enforcement quandaries that Nevada

<sup>13</sup> Ariz. Rev. Stat. § 44-1373, Cal. Civ. Code § 1798.85 and Conn. Gen. Stat. § 42-470.

<sup>14</sup> Md. Commercial Law Code Ann. § 14-3402(4).

<sup>15</sup> Personal information was defined as: "a natural person's first name or first initial and last name in combination with any one or more of the following data elements, when the name and data elements are not encrypted: (a) social security number; (b) driver's license number or identification card number; and (c) account number, credit card number or debit card number, in combination with any required security code, access code or password that would permit access to the person's financial account."

<sup>16</sup> 201 CMR 17.04(3) and (5).

<sup>17</sup> See, e.g., *Guin v. Brazos Higher Educ. Serv.*, 2006 U.S. Dist. Lexis 4846 (D. Minn. Feb. 7, 2006) (5 PVL 233, 2/20/06),

---

faces in policing technology and other issues that are not clearly defined under its law.

### **Conclusion**

Overall, the legal trend is clearly to expand corporate obligations to secure sensitive consumer data. As with the security breach notification laws that began in California, the nationwide scope of many businesses, and the borderless nature of modern electronic commerce may well make the Massachusetts Regulations *de facto* law of the land for many companies. If a company is not currently subject to a legal obligation to develop and implement a comprehensive written information security program, it likely will be soon.

For some companies, the internal changes required by the Regulations may be expensive and require significant organization resources. For example, complying with aspects of the employee training and monitoring aspects of the law could impose new burdens on the HR employee training function and internal audit, compliance and regulatory teams. As such, any initial compliance assessment should be operated with buy-in and support from top management to ensure that adequate human and capital resources will be available to adequately assess existing practices and respond to any deficiencies in light of the new Regulations.