



Washington Legal Foundation  
**Advocate for freedom and justice®**  
2009 Massachusetts Avenue, NW  
Washington, DC 20036  
202.588.0302

**THE BAY STATE RAISES THE BAR ON  
PERSONAL DATA SECURITY:  
ARE YOU IN COMPLIANCE?**

by  
Jeffrey D. Neuburger and Natalie Newman  
*Proskauer Rose LLP*



**Washington Legal Foundation**  
CONTEMPORARY LEGAL NOTE Series

Number 66  
June 2010

**THE BAY STATE RAISES THE BAR  
ON PERSONAL DATA SECURITY:  
ARE YOU IN COMPLIANCE?**

by  
Jeffrey D. Neuburger and Natalie Newman  
*Proskauer Rose LLP*

Washington Legal Foundation  
CONTEMPORARY LEGAL NOTE Series  
Number 66  
June 2010

Visit us on the Web at  
[www.wlf.org](http://www.wlf.org)

## TABLE OF CONTENTS

I. MASSACHUSETTS RAISES THE BAR.....	2
II. THE MAIN REQUIREMENTS OF THE REGULATIONS .....	4
III. THE WRITTEN INFORMATION SECURITY PROGRAM .....	5
IV. THIRD-PARTY PROVIDERS AND VENDORS .....	7
V. ENCRYPTION AND OTHER COMPUTER SECURITY REQUIREMENTS.....	8
VI. ENFORCEMENT.....	10
VII. WILL OTHER STATES OR THE FEDERAL GOVERNMENT FOLLOW SUIT? .....	12
VIII. WHAT YOU SHOULD DO NOW — SOME PRACTICAL ADVICE.....	13

## **ABOUT WLF'S LEGAL STUDIES DIVISION**

The Washington Legal Foundation (WLF) established its Legal Studies Division to address cutting-edge legal issues by producing and distributing substantive, credible publications targeted at educating policy makers, the media, and other key legal policy outlets.

Washington is full of policy centers of one stripe or another. But WLF's Legal Studies Division has deliberately adopted a unique approach that sets it apart from other organizations.

First, the Division deals almost exclusively with legal policy questions as they relate to the principles of free enterprise, legal and judicial restraint, and America's economic and national security.

Second, its publications focus on a highly select legal policy-making audience. Legal Studies aggressively markets its publications to federal and state judges and their clerks; members of the United States Congress and their legal staffs; government attorneys; business leaders and corporate general counsel; law school professors and students; influential legal journalists; and major print and media commentators.

Third, Legal Studies possesses the flexibility and credibility to involve talented individuals from all walks of life - from law students and professors to sitting federal judges and senior partners in established law firms.

The key to WLF's Legal Studies publications is the timely production of a variety of intelligible but challenging commentaries with a distinctly common-sense viewpoint rarely reflected in academic law reviews or specialized legal trade journals. The publication formats include the provocative COUNSEL'S ADVISORY, topical LEGAL OPINION LETTERS, concise LEGAL BACKGROUNDERS on emerging issues, in-depth WORKING PAPERS, useful and practical CONTEMPORARY LEGAL NOTES, interactive CONVERSATIONS WITH, law review-length MONOGRAPHS, and occasional books.

WLF's LEGAL OPINION LETTERS and LEGAL BACKGROUNDERS appear on the LEXIS/NEXIS® online information service under the filename "WLF" or by visiting the Washington Legal Foundation's website at [www.wlf.org](http://www.wlf.org). All WLF publications are also available to Members of Congress and their staffs through the Library of Congress' SCORPIO system.

To receive information about previous WLF publications, contact Glenn Lammi, Chief Counsel, Legal Studies Division, Washington Legal Foundation, 2009 Massachusetts Avenue, NW, Washington, D.C. 20036, (202) 588-0302. Material concerning WLF's other legal activities may be obtained by contacting Daniel J. Popeo, Chairman.

# **THE BAY STATE RAISES THE BAR ON PERSONAL DATA SECURITY: ARE YOU IN COMPLIANCE?**

by  
Jeffrey D. Neuburger and Natalie Newman<sup>1</sup>  
*Proskauer Rose LLP*

Newly effective regulations promulgated under Massachusetts' recent data security law, Mass. Gen. Law ch. 93H, have raised the bar for data security compliance.<sup>2</sup> Even companies that were compliant with applicable law prior to the enactment of the Regulations are obligated to review where they stand in light of these new requirements. Furthermore, companies outside of Massachusetts cannot ignore the Regulations – their effect is national and international in scope, as they apply to all companies – wherever located – using personal data of Massachusetts residents.

Despite the fact that the deadline for compliance with the Regulations – March 1, 2010 – has come and gone, many companies – both within Massachusetts, but particularly outside of Massachusetts – are not yet, in fact, compliant. These companies are finding themselves in a position of playing “compliance catch-up.” The concern over non-compliance is not limited to

---

<sup>1</sup>Jeffrey D. Neuburger is a Partner in New York office of Proskauer Rose LLP, is co-head of the law firm's Technology, Media and Communications group and a member of the firm's Privacy and Data Security group. Natalie Newman is an Associate in the New York office of Proskauer Rose, and is a member of both the Technology, Media and Communications group and the Privacy and Data Security group at the firm.

<sup>2</sup>201 Mass. Reg. Code tit. 201, § 1700 (the “Regulations”). The Regulations are explained by the Massachusetts Office of Consumer Affairs and Business Regulation (“OCABR”) in “Frequently Asked Question Regarding 201 CMR 17.00,” (hereafter “OCABR FAQ”) available at <http://www.mass.gov/Eoca/docs/idtheft/201CMR17faqs.pdf>.

Massachusetts regulatory enforcement. Companies are also concerned that private plaintiffs in data security breach-related litigation will allege that the Regulations establish a “standard of care” for the purpose of asserting a negligence claim.

Many people are now wondering what could be coming next from other well-intentioned state legislatures seeking to address the cracks in commercial information security practices. Will other states ratchet up the level of data security compliance even higher?

This CONTEMPORARY LEGAL NOTE discusses the Regulations and their implications, and provides a series of practical recommendations that entities can follow to comply with, and stay in compliance with, the Regulations.

## **I. MASSACHUSETTS RAISES THE BAR**

The Massachusetts Regulations include certain requirements which, in the aggregate, reach further in scope and effect than any other existing federal or state law.<sup>3</sup>

- They apply to all persons and businesses that “own, license, store or maintain personal information about a resident of the Commonwealth of Massachusetts.” Thus, the Regulations apply regardless of the state in which an entity maintains a place of business or where such entity is incorporated.<sup>4</sup>

---

<sup>3</sup>The regulation applies to those who collect and retain personal information in connection with the provision of goods and services or for the purposes of employment. The regulation does not apply, however, to natural persons who are not in commerce.” OCABR FAQ, *see* n. 2.

<sup>4</sup>The regulation applies to those who collect and retain personal information in connection with the provision of goods and services or for the purposes of employment. The

- The Regulations impose more detailed technical requirements that were not included as requirements in any previous information security regulatory law. In particular, in recognition of the increasingly prevalent role of portable devices in business, the Regulations impose data security requirements with respect to portable devices in a way that arguably goes beyond the current state of the law. Because of this breadth, the technical requirements may be the most significant aspect of the Regulations.
- The Regulations are broad in the scope of information they address. For example, they are not limited to information from or about consumers – they apply to all “personal information” of any Massachusetts resident, whether employees of, customers of, or investors in, a company. This is in contrast, for example, with the federal Gramm Leach Bliley Act privacy provisions<sup>5</sup> (the “GLB” Act), which apply only to “consumer” and “customer” non-public personal information, and with the federal Health Insurance Portability and Accountability Act<sup>6</sup> (“HIPAA”) and related laws, which apply only to certain health and health-related information.
- The Regulations apply to both paper and electronic records – an extension from the requirements of many other data security laws that apply only to electronic records.
- Entities already regulated by other regulations are not exempt from compliance with the Massachusetts Regulations. Thus, all companies that have information security programs – even companies already subject to other data security regulation – have to consider the effect of the Regulations. For example, a financial institution subject to and compliant with the federal GLB Act or an entity subject to the requirements of HIPAA must reevaluate and possibly modify its data protection programs and procedures in order to comply with the Massachusetts requirements.

---

regulation does not apply, however, to natural persons who are not in commerce.” OCABR FAQ, *see n. 2*.

<sup>5</sup>Gramm-Leach-Bliley Act, also known as the Financial Services Modernization Act of 1999, Pub.L. 106-102, 113 Stat. 1338. The privacy provisions are codified at 15 U.S.C. § 6801-6809.

<sup>6</sup>Health Insurance Portability and Accountability Act (HIPAA) (Pub. L. 104-191). *See also* HITECH Act, 111th Cong., 1st Sess. Feb. 17, 2009.

## **II. THE MAIN REQUIREMENTS OF THE REGULATIONS**

The Regulations concern “personal information” of Massachusetts residents. “Personal information” is defined as a Massachusetts resident’s name (first name and last name, or first initial and last name), in combination with his or her Social Security number, driver’s license or state-issued identification card number, or financial account or credit/debit card number, with or without any required security or access code, that would permit access to the resident’s financial account. The Regulations apply to both paper and electronic records, but they do not apply to information obtained from publicly available sources.

The Regulations were intended to accomplish three main objectives: (1) to ensure the security and confidentiality of personal information in a manner consistent with industry standards; (2) to protect against anticipated threats or hazards to the security or integrity of such information; and (3) to protect against unauthorized access to or use of such information that may result in substantial harm or inconvenience to any consumer.

To accomplish these objectives, the Regulations contain two primary requirements – the maintenance of a comprehensive written security program and the implementation of specific computer security requirements.

### III. THE WRITTEN INFORMATION SECURITY PROGRAM

Every entity subject to the Regulations must develop, implement, and maintain a comprehensive written information security program (a “WISP”). WISPs must include administrative, technical, and physical safeguards that are designed to meet the objectives of the Regulations. The program must reflect a “risk-based” approach in that it is appropriate to the size, scope, and type of business handling the information; the amount of resources available to the business; the amount of stored data; and the need for security and confidentiality of both consumer and employee information.

The Massachusetts Office of Consumer Affairs and Business Regulation (“OCABR”), in its “Frequently Asked Question Regarding 201 CMR 17.00,” (“FAQ”)<sup>7</sup> describes the “risk-based” approach as “one that directs a business to establish a written security program that takes into account the particular business’ size, scope of business, amount of resources, nature and quantity of data collected or stored, and the need for security.”<sup>8</sup> This, OCABR says, “differs from an approach that mandates every component of a program and requires its adoption regardless of size and the nature of the business and the amount of information that requires security.”<sup>9</sup> OCABR has also expressed that the “risk-

---

<sup>7</sup>*Supra* note 2.

<sup>8</sup>OCABR FAQ, “What are the differences between this version of 201 CMR 17.00 and the version issued in February of 2009?” *Supra* note 2.

<sup>9</sup>*Id.*

based” approach is primarily intended to ease the burden of the Regulations on small businesses that may not handle a significant amount of personal information or may not have the resources to develop a sophisticated security program.

Among other things, a WISP must designate one or more employees to maintain the program; identify and assess reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of the personal information covered by the program; and evaluate and improve, where necessary, the effectiveness of the current safeguards in order to minimize any of the risks identified through the risk assessment process. The WISP also must develop policies for employees relating to the storage, access, and transportation of records outside of business premises; impose disciplinary measures for violations of such rules; and implement measures to prevent terminated employees from accessing the business’ records.

A business’ ongoing compliance with its WISP must be regularly monitored, and the scope of security measures included therein must be reviewed at least annually or in connection with a material change to the company’s business practices that may implicate the security or integrity of records containing personal information. If the business experiences a data breach affecting personal information, it must document any remedial or responsive actions it takes in connection with any such incident. The WISP must also include a mandatory procedure for post-incident review of events

and actions taken, if any, to make the necessary changes in business practices.

#### **IV. THIRD-PARTY PROVIDERS AND VENDORS**

A covered entity's WISP also must include a requirement and procedure for overseeing all service providers and vendors that will receive, store, maintain, process, or otherwise be permitted access to the entity's personal information through their provision of services to that entity. Specifically, the Regulations mandate companies to conduct due diligence and take other "reasonable steps" to select and retain third party service providers who are capable of compliance with the Regulations. It is important to adequately perform and document such diligence. Companies are also required to contractually obligate all third-party service providers to implement and maintain appropriate security measures for personal information.

The Regulations extend a two-year grace period for contracts with third-party providers that were already in place as of the effective date of the Regulations, March 1, 2010. Essentially, all contracts with third-party providers where the handling of personal information is involved, must comply with the Regulations by March 1, 2012. However, all contracts entered into after March 1, 2010 must ensure that the third-party service provider is also protecting personal information in compliance with the Regulations.

## **V. ENCRYPTION AND OTHER COMPUTER SECURITY REQUIREMENTS**

The second of the Regulations' two major requirements is that all covered entities establish and maintain various computer security measures applicable to both the storage and the transmittal of personal information.

Among other things, "to the extent technically feasible," such computer security measures shall include: the use of secure user authentication protocols (including, for example, control over user IDs and "reasonably secure" methods for assigning, selecting, and controlling passwords); various secure access control measures; "reasonably up-to-date" firewall protection, operating system security patches, malware protection, and anti-virus software; and employee education and training programs for the proper use of the computer security system.

In addition, the Regulations require the encryption of all records containing personal information, whether such information is being stored electronically (on portable devices such as laptops or hand-held devices), electronically transmitted over a public network (such as the Internet), or transmitted wirelessly.

This means that, as of March 1, 2010, no company subject to the Regulations should be electronically transmitting, via e-mail or FTP over the Internet, by wire or wirelessly, any documents or materials containing qualifying personal information of Massachusetts residents, regardless of the

intended recipient of such communications, unless the transmitted data has been encrypted in compliance with the Regulations.

It is important to remember, however, that the security requirements of the Regulations are qualified by a standard of “technical feasibility.” Thus, encryption of personal information, for example, is only required to the extent “technically feasible.” Although “technically feasible” is not defined in the Regulations themselves, a definition and further explanation is provided in the OCABR FAQ that accompanies the Regulations.<sup>10</sup>

The OCABR FAQ defines “technically feasible” to mean “that if there is a reasonable means through technology to accomplish a required result, then that reasonable means must be used.” With respect to portable devices, the FAQ explains that “the ‘technical feasibility’ language of the regulation is intended to recognize that at this period in the development of encryption technology, there is little, if any, generally accepted encryption technology for most portable devices, such as cell phones, blackberries, net books, iphones and similar devices. While it may not be possible to encrypt such portable devices, personal information should not be placed at risk in the use of such devices. There is, however, technology available to encrypt laptops.”<sup>11</sup>

In addition, the Regulations are technology-neutral; in particular, “encryption” now includes any transformation of data into a form in which

---

<sup>10</sup>See, e.g., “What about the computer security requirements of 201 CMR 17.00?” OCABR FAQ, *supra* note 2.

<sup>11</sup>“Do all portable devices have to be encrypted?,” OCABR FAQ, *supra* note 2.

meaning cannot be assigned “without the use of a confidential process or key.” (Some will surely argue that this new definition of “encryption” does not necessarily require encryption at all; however, the OCABR’s statements made through the FAQ posted on its website suggests that the removal of references to specific technology from the definition was intended to allow for future encryption technologies, not necessarily earlier or less secure technologies.)

## **VI. ENFORCEMENT**

The law delegates enforcement of the Regulations to the Massachusetts State Attorney General’s Office.<sup>12</sup> To date, however, the Regulations remain unenforced (at least officially or publicly), and the level and extent to which the Regulations will be enforced in the future is unclear. The OCABR has, however, stated that a company’s compliance with the Regulations will be “judged on a case by case basis,” and, like the statute and the Regulations, will take into account “the size and scope of [the] business, the resources that [the business] has available to [it], the amount of data that [the business] store[s], and the need for confidentiality.”<sup>13</sup>

Although only the Massachusetts State Attorney General’s office can enforce the Regulations, they will certainly add fuel to private data security litigation. In cases where private plaintiffs bring suit against companies for

---

<sup>12</sup>Massachusetts consumer protection law, Mass. Gen. Laws ch. 93A.

<sup>13</sup>“What are the differences between this version of 201 CMR 17.00 and the version issued in February of 2009?” *supra* note 2.

inadequate data security practices, plaintiffs will point to a company's failure to meet these standards as a failure to satisfy a duty, thereby establishing one of the elements of a negligence claim.

The adequacy of due diligence on third-party vendors may be subject to litigation. The Regulations' risk-based approach could also make useful litigation fodder, as they leave open a level of discretion with respect to compliance. Similarly, the standard of "technically feasible" leaves open areas of challenge. While the Regulations are new, and we therefore cannot comment on how successful civil plaintiffs will be in this effort, we have seen plaintiffs argue in other circumstances, with mixed success, that the GLB Safeguard Rule<sup>14</sup> should operate as a standard for purposes of proving negligence.

## **VII. WILL OTHER STATES OR THE FEDERAL GOVERNMENT FOLLOW SUIT?**

Even though some companies are scrambling to conform their policies and practices to the Massachusetts requirements, a general fear persists in the business community that other states are soon to follow the Bay State's lead, especially with respect to requiring encryption and other specific security measures.

Thieves of personal information will continue to adapt their techniques

---

<sup>14</sup>See, e.g., *Guin v. Brazos Higher Education Service Corporation, Inc.*, 2006 WL 288483 (D. Minn. 2006),

and exploit technical vulnerabilities that others have previously discovered. As the law is a consistent laggard to technological malevolence, even those in full compliance with the Massachusetts regulations are still vulnerable to criminal activity.

While 46 states<sup>15</sup> now have data breach notification laws, and a large number of states also have laws requiring the protection of their residents' personal information, no state or federal law has proscribed data security requirements as specific and comprehensive as Massachusetts. In fact, only one other state as of the date of this LEGAL NOTE compares to Massachusetts in that respect. On January 1, 2010, Nevada's new identity theft law, S.B. 227<sup>16</sup> went into effect. Among other things (such as mandating compliance with the PCI Security Standards Council Data Security Standard<sup>17</sup> for all credit card information), S.B. 227 specifically requires the "encryption" of all personal information leaving the "logical or physical controls of the data collector," including electronic data on a "data storage device."<sup>18</sup> The Nevada law applies to entities "doing business in" the state (a phrase not defined in the law, but

---

<sup>15</sup>See Andrew Hoffman, *It's Not Too Late to Come to the Party: Mississippi Joins 45 Other States by Enacting a Security Breach Notification Law* (Apr. 13, 2010), available on the Proskauer Privacy Law Blog at <http://privacylaw.proskauer.com/2010/04/articles/data-breaches/its-not-too-late-to-come-to-the-party-mississippi-joins-45-other-states-by-enacting-a-security-breach-notification-law/>.

<sup>16</sup>S.B. 227, 75<sup>th</sup> Reg. Sess., ch. 355 (Nev. 2010), amending Chapter 603A of the Nev. Rev. Stat.

<sup>17</sup>S.B. 227 §1, 75<sup>th</sup> Reg. Sess., ch. 355 (Nev. 2010), amending Chapter 603A of the Nev. Rev. Stat.

<sup>18</sup>*Id.*

which predictably will be interpreted as narrowly as possible, at least until any enforcement actions are brought or other legislative clarifications or guidance are released).<sup>19</sup>

Does that mean that state privacy regulators are not done? Will newly recognized vulnerabilities be met by more stringent data security standards? Will companies that expend the resources to comply with the Regulations be asked again to comply with yet another set of data security requirements? Or, will the current national standards of technical security remain the de facto operating standard for the foreseeable future?

## **VIII. WHAT SHOULD YOU DO NOW – SOME PRACTICAL ADVICE**

All companies subject to the Regulations are expected to be in compliance with the requirements as of March 1, 2010. While many companies scrambled to bring their programs and procedures into compliance, others – especially those outside of Massachusetts – are just now learning of these requirements and their application.

If you have not evaluated the Regulations to determine whether they apply to you, and to determine whether you need to modify your policies and procedures, you should determine as a threshold matter, whether your

---

<sup>19</sup>For more information on Nevada S.B. 227 see Brendon Tavelli, *What Happens in Vegas Really Does Stay in Vegas (Unless It Is Encrypted)*, available on the Proskauer Privacy Law Blog at <http://privacylaw.proskauer.com/2009/06/articles/data-privacy-laws/what-happens-in-vegas-really-does-stay-in-vegas-unless-it-is-encrypted/>.

organization owns, licenses, or maintains any personal information of any Massachusetts residents. If the answer is “yes,” you need to quickly evaluate the Regulations to ensure compliance.

- If you already have a security policy in place, you need to evaluate if your policy fails to satisfy the requirements of the Regulations. To the extent you determine that a “risk-based” analysis suggests less than the most stringent level of requirements, you should consider engaging a consultant to document the grounds for such a determination, based on industry-standard benchmarks established across varying levels of risk. This is important not only with respect to being ready to respond in the event of a regulatory investigation, but also to defend against civil suits which allege that the “risk-based” analysis was improperly performed and resulted in a lower than appropriate standard of security.
- You should evaluate the technical requirements the Regulations impose to determine, what if any aspects of those requirements are not already in place as part of your operational procedures (including with respect to all portable devices). Any determination that something is not “technically feasible” should be well documented, supported by clear and consistent information, and consistent with legislative intent.
- To the extent you identify deficiencies, consult your information technology providers to ensure that you have compliant and up-to-date firewall and other network protections, as well as data encryption capabilities.
- You should ensure that you perform adequate due diligence on any third parties that you entrust with personal information. That diligence should be documented and retained. You should evaluate what information is provided to third parties (such as any service providers) to determine which of the Regulation’s requirements are relevant. You should create standard clauses to include in relevant agreements, and to the extent your current agreements are not compliant with the Regulations, you should set into place a plan for amending such agreements to achieve compliance by March 1, 2012.
- You should continue to monitor developments in Massachusetts to understand how the regulators will interpret the “risk-based” analysis and other aspects of the Regulations.

The Regulations represent an incremental rise in the level of technical compliance needed in the interest of data security. If they apply to you, you should evaluate them immediately. The only thing that can make a major security breach even worse is a regulatory investigation or civil action alleging that you failed to meet your obligations under applicable law, and that such a failure resulted in the breach.