

## EDITORS:

### Alysa Zeltzer Hutnik

ahutnik@kelleydrye.com

### Mary Ellen Callahan

mecallahan@hhlaw.com

### Kasey A. Chappelle

kasey@ebay.com

### Benita A. Kahn

bakahn@vorys.com

### Deborah Marrone

dmarrone@ftc.gov

### Kristen J. Mathews

kmathews@proskauer.com

The Secure Times is published by the American Bar Association Section of Antitrust Law's Privacy and Information Security Committee. The views expressed in The Secure Times are the authors' only and not necessarily those of the American Bar Association, the Section of Antitrust Law or the Privacy and Information Security Committee.

If you wish to comment on the contents of The Secure Times, please write to the American Bar Association, Section of Antitrust Law, 321 North Clark St., Chicago, IL 60610

©Copyright 2009 American Bar Association



## IN THIS ISSUE

### New Data Security Regulations Create Compliance Challenges for Businesses

By Thomas J. Smedinghoff and Laura E. Hamady..... 2

### Developing An ID Theft Protection Program: Compliance with the FTC's Red Flags Rule

By Betsy Broder..... 9

### No Harm, No Foul: Precedent-Setting Ruling Limits Potential Liability Stemming from Allegations of Improper Disposal of Documents

By Donna L. Wilson and Andrew S. Wein..... 13

### Recent Privacy and Data Security Developments

By The Privacy and Information Security Committee ..... 15

## A Word From the Chair:

We are pleased to present this latest edition of The Secure Times. While we strive to provide a healthy balance of both privacy and data security content, given the heightened activity in the last six months in the area of data security, this volume focuses primarily on these key developments. Included in this edition are an in-depth analysis of the new Massachusetts data security regulations and the evolving legal requirement that businesses have a comprehensive information security program; a thorough discussion by an Assistant Director in the FTC's Division of Privacy and Identity Protection on how to develop a compliant Red Flags program; insights from a recent Louisiana court decision in a data breach case alleging improper disposal; and a round-up of the last quarter's privacy and data security case filings, decisions, settlements, and other developments.

We also would be remiss if we didn't mention two significant consumer protection events. Next month, the Section will release its latest treatise, Consumer Protection Law Developments. The treatise, edited by August Horvath and John Villafranco, was the product of four years of work and included contributions by

more than 100 consumer protection lawyers. A preview of the treatise revealed comprehensive summaries of the law on deception and unfairness, privacy and data security, new technologies, private remedies, promotions marketing, state consumer protection law, and international consumer protection. The CPLD editors established a goal of creating a worthy companion to the Section's treatise on Antitrust Law Developments, which has been widely regarded as the most comprehensive and accurate treatment of United States antitrust laws and has been frequently cited by courts and in the legal and economic literature. This inaugural edition of CPLD continues and extends this distinguished tradition.

In addition, on June 18 and 19, the Section will present the 2009 Consumer Protection Conference in Washington, D.C. This conference will bring together leading government enforcers, public interest lawyers, academics, and private practitioners to discuss pressing issues related to consumer protection law. Speakers include Commissioner Pamela Jones Harbour and former Chairmen Robert Pitofsky and Timothy Muris, every Director of the FTC's Bureau of Consumer Protection since the mid-1980s, Assistant Attorneys General from Texas and Florida, among many other experts. Topics that will be addressed include protecting privacy and securing information, managing risks in new technologies, consumer research in policy-making, the use of extrinsic evidence in cases of deception and unfairness, green marketing, consumer protection in financial transactions and the need for a Financial Products Safety Commission, and many others. Stay tuned for more information.

Finally, if you would like to become more involved in our Committee – whether as a speaker, article or Secure Times blog contributor, or in a behind-the-scenes role – please

let us know. With our ambitious agenda for improving the resources available to privacy and data security practitioners, we need your participation more than ever.

*Alysa Z. Hutnik*

## **New Data Security Regulations Create Compliance Challenges for Businesses**

**By Thomas J. Smedinghoff and Laura E. Hamady**

On September 22, 2008, the Massachusetts Office of Consumer Affairs and Business Regulation (“OCABR”) released its “Standards for Protection of Personal Information of Residents of the Commonwealth”<sup>1</sup> (“Massachusetts Regulations”), as required by the 2007 Massachusetts security breach and data destruction law.<sup>2</sup> Those Regulations create the most comprehensive set of general data security obligations yet to be imposed on businesses by a state. Moreover, in the absence of comprehensive federal data security legislation,<sup>3</sup> the Massachusetts Regulations, like the first state breach notification law enacted by California in 2003,<sup>4</sup> will likely have a nationwide impact, both in terms of applicability and in encouraging other states to adopt similar rules. And in fact, on December 15, 2008, New Jersey released its “Pre-Proposal” for similar regulations.<sup>5</sup>

The Massachusetts Regulations apply to all businesses “that own, license, store or maintain personal information about a resident,”<sup>6</sup> regardless of where the business is located, its size or its industry sector. They define personal information as first name (or initial) and last name of a Massachusetts resident, in combination with at least one of the following data elements: (a) Social Security num-

ber; (b) driver's license number or state-ID number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, PIN or password.

The deadline for compliance with the Massachusetts Regulations, originally January 1, 2009, has been extended until January 1, 2010.<sup>7</sup> Regardless of the size or sophistication of the company, complying with the Regulations by their effective date will be daunting and likely to consume tremendous internal resources and in many cases, entail significant expense.

Like the law in at least nine other states, 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, the Massachusetts Regulations specifically 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 that is: (1) stored on laptops or other portable devices, (2) contained in records and files transmitted over public networks "to the extent technically feasible," and (3) transmitted wirelessly.

Although the way in which each business complies with the Massachusetts Regulations will necessarily be based on its unique circumstances, the OCABR has released compliance guidelines and other informational resources ("Guidance") that provide additional information to assist covered entities in complying with these requirements.<sup>8</sup> The

"Small Business Guide for Formulating a Comprehensive Written Information Security Program" (the "Guide") provides a template for a comprehensive written information security program.<sup>9</sup> A "Compliance Checklist" highlights individual features of the Regulations "that [require] attention in order for a [company's comprehensive information security program] to be compliant;" and a list of "Frequently Asked Questions" ("FAQ") highlights certain of the Regulations' provisions and emphasizes that compliance must be appropriate to a company's size, scope and type, its resources, the type and extent of personal data handled and the security needed for the covered data.

### Duty to Implement Comprehensive Written Information Security Program

At the heart of the Massachusetts Regulations is its requirement to "develop, implement, maintain and monitor a comprehensive, written information security program" designed to ensure the security and confidentiality of any records containing personal information. The Regulations specify that an entity's 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 embodied in the Massachusetts Regulations are largely a restatement of the legal definition of "reasonable security" that has evolved over the past several years at the federal level. Similar requirements are embodied in a series of existing federal financial and health care industry regulations and in numerous consent decrees entered in FTC enforcement actions. As such, the duty to implement a comprehensive written information security program should not be viewed as an anomaly,

but rather as part of an evolving trend that began in certain regulated industries at the federal level and is now being extended to all businesses at the state level.

### How Did We Get Here?

The obligation to develop and implement a comprehensive written information security program first appeared several years ago at the federal level in sector-specific legislation and regulations. The Gramm-Leach-Bliley Act financial industry security regulations titled *Guidelines Establishing Standards for Safeguarding Consumer Information* issued by the Federal Reserve, the OCC, FDIC, and the Office of Thrift Supervision, on February 1, 2001,<sup>10</sup> and later adopted by the FTC in its *Safeguards Rule* on May 23, 2002,<sup>11</sup> require such a security program. The Federal Information Security Management Act of 2002 (“FISMA”), which applies to government agencies,<sup>12</sup> and the HIPAA *Security Standards* issued by the Department of Health and Human Services on February 20, 2003,<sup>13</sup> which apply in the health-care sector, both also require comprehensive written information security plans.

Shortly after the first of these sector-specific Federal regulations were issued, the FTC began adopting the view that a comprehensive information security program is a “best practice” applicable to all businesses and all industries.<sup>14</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 required the defendants to develop and implement a comprehensive written information security program.

In 2004, several states started enacting 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>15</sup> Thereafter, several states<sup>16</sup> enacted similar statutes. These laws did not, however, define “reasonable security.”

In 2007, Oregon enacted security legislation that expressly stated that its requirement for “reasonable safeguards” could be satisfied by complying with the GLB Security Regulations, the HIPAA Security Regulations, or implementation of an information security program specified in the statute.<sup>17</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.”

In contrast, the Massachusetts Regulations represent the first time a state has required a formal comprehensive written information security plan using essentially the same requirements imposed by Federal regulations and FTC consent decrees. And if New Jersey adopts its proposed regulations, it will impose a similar obligation.

### Overview of the Comprehensive Security Program

The requirement for a comprehensive written information security program in all of the foregoing laws (including the Massachusetts Regulations) is based on the view that data security is a relative concept, and thus, that providing “reasonable security” requires implementing a fact-specific, risk-based *process* that addresses the company’s current business realities and adapts to future changes. With some notable exceptions in the Massachusetts Regulations discussed below, these laws generally reject 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>18</sup>

Instead, the legal requirement can be summarized by the phrase “*process plus categories*.” That is, to satisfy its legal obligations to implement “reasonable security” a company must: (i) engage in a defined and repetitive risk-based “*process*,” and (ii) apply that process to all areas of its risk, including to selected “*categories*” of security controls specified in the applicable regulations.

### **The Process**

Like existing federal regulations and FTC policy, the Massachusetts Regulations 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 safeguards currently in place for minimizing such risks;

**Select and 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” (discussed below);

**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 information; and upgrade the security controls as necessary to limit risks;

**Regularly Review Program:** Review and adjust the information 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:** Take all reasonable steps to verify that each third-party service provider that has access to personal information has the capacity to protect such information in the manner provided for in the Massachusetts Regulations; and take all reasonable steps to ensure that each third party service provider is applying to such personal information protective security measures at least as stringent as those required to be applied under the Massachusetts Regulations (discussed below).<sup>19</sup>

### **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 in assessing its particular risks and business model as part of the process of implementing a compliant security program. Without specifying which specific security controls must be put in place, the Massachusetts Regulations require that:

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:

- 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.

While the Massachusetts Regulations identify these *categories* of required security controls, like federal law, they leave it up to the company to determine how such categories will be addressed. The Regulations require only that the controls implemented in each category be responsive to its risk assessment. Thus, the Guidance stresses that compliance (and, conversely enforcement) will be based on how rigorously and appropriately a business has analyzed and documented risk, and whether it has implemented security controls in each such category consistent with its risk assessment. However, the Regulation's security categories also contain some exacting criteria which raise at least two issues.

First, some have argued that the Massachusetts Regulations include categories of controls not found in federal regulations, complicating the compliance process for entities already regulated by these statutes and introducing the possibility that a small state business could be more rigorously regulated than say, an international bank. 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. On the other hand, certain specified standards 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, although the OCABR stresses the fact that the Massachusetts Regula-

tions are technology neutral, they do include requirements for encryption in certain cases.

### 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>20</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>21</sup>

Then, on October 1, 2008, a Nevada law took effect which prohibited the *electronic transmission* of any personal information<sup>22</sup> to a person outside of the secure system of the business (other than a facsimile) unless the information is encrypted.<sup>23</sup>

The Massachusetts Regulations take the encryption requirement significantly farther. They require any entity that **stores or transmits** electronic records containing personal information to encrypt that information in specific situations.<sup>24</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 presumably includes

portable communication devices such as BlackBerrys and cell phones, as well as portable storage devices such as iPods and USB flash drives, and may include portable media such as DVDs.<sup>25</sup>

- 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>26</sup> Legislative history of the Massachusetts Regulations suggests that lawmakers were focused on these devices as a primary source of data breaches and sought to provide regulatory incentives to prevent such breaches in the future. However, whether mandating encryption or other technologically and procedurally-specific requirements becomes a trend remains to be seen.<sup>27</sup> Regardless, the definition of encryption presents a unique challenge with all of these statutes, as technical issues such as what qualifies as encryption, and how strong it must be, are left unclear and muddy both compliance and enforcement efforts.

### Responsibility for Employees and Third Parties

Although the Massachusetts Regulations allow a covered entity to determine how it will satisfy the various requirements of the legislation, the Guide suggests that the OCA-BR places particular importance on how a covered entity addresses its administrative obligations relative to its em-

employees and third party contractors and service providers who handle personal information.

For example, the Guide's model information security program contains a provision that requires companies to re-train all personnel after adoption of the program and to amend all employee contracts to require compliance with the program. It also includes a provision that requires companies to evaluate the ability of service providers to comply with the requirements of the Massachusetts Regulations and to contractually require that such service providers be in compliance with the Regulations.<sup>28</sup>

This concept – that a covered entity is ultimately responsible for the actions of its third parties service providers – is consistent with existing Federal data security law and is reinforced by a recent FTC enforcement action involving mortgage lender Premier Capital Lending, Inc. In that case, the FTC brought an action for, among other things, violating the Safeguards Rule by allowing a business partner that did not employ “reasonable and appropriate” security to safeguard sensitive data, to access consumer credit reports through Premier's system.<sup>29</sup>

## Penalties

Although compliance with the Massachusetts Regulations will be a fact-specific exercise, and for many companies, complicated by joint and overlapping obligations to comply with other privacy and security laws, the potential costs of not complying with the Regulations could be significant. The Massachusetts attorney general may seek a temporary restraining order or a preliminary or permanent injunction under the Massachusetts Unfair Competition Statute (“Chapter 93A”)<sup>30</sup> against any entity suspected of being in violation of the Regulations. If a court finds that the Regu-

lations were violated, it may impose civil penalties of up to \$5,000 per violation, as well as court costs and attorneys' fees. The damage to a company's goodwill and reputation that may likely accompany an enforcement action could also impose significant cost on a business.

The risk of class action litigation may also be a major concern for companies that fail to comply with the Regulations. Massachusetts residents may bring a claim for unfair or deceptive practices under Chapter 93A, or a negligence claim by using the Regulations and Chapter 93A to establish the company breached a specific duty to safeguard his or her personal information. Under Massachusetts law, a violation of the statute could constitute per se negligence and potentially expose defendant companies to claims in the amount of a plaintiff's actual damages, or \$25.00, whichever is greater. If damages are calculated on a per individual record basis, as is the case in CAN-SPAM litigation, they could be significant. Treble damages are available for willful or knowing violations.

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 the *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.

*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).

## Developing An ID Theft Protection Program: Compliance with the FTC's Red Flags Rule

By Betsy Broder

News stories continue to astonish and disturb us with reports of how identity theft has devastated consumers' lives. The time to marvel at the ingenuity of the crooks has passed, and the time to develop meaningful Programs to prevent identity theft has arrived. So what happens when a business sees signs of identity theft? Do employees know how to respond when they receive a credit application that has been ripped up, taped together and then submitted with a new address? Are there procedures in place for when you spot purchasing patterns that deviate from that customer's routine pattern? These types of patterns often signal identity theft. Having a written Program to identify, detect, and respond to these warning signs is not just good business; it's now the law.

To comply with the new Red Flags Rule – enforced by the FTC, the federal bank regulatory agencies, and the National Credit Union Administration (“NCUA”) – creditors and financial institutions may need to develop a written “Red Flags” Program to prevent identity theft, detect it, and help minimize the damage that identity thieves can do to consumers and businesses.<sup>1</sup> The Red Flags Rule was promulgated by these agencies pursuant to the 2003 Fair and Accurate Credit Transactions Act (“FACT Act”) amendments to the Fair Credit Reporting Act.<sup>2</sup>

**NOTE:** The FTC has announced that it will delay enforcement of the Rule as to those entities under its jurisdiction for six months, until May 1, 2009. The FTC's decision does not affect the enforcement against banks, federally chartered credit unions, savings and loans, and other entities that are regulated by the other Red Flag agencies. It does not affect enforcement of the Address Discrepancy Rule and Credit Card Issuer Rules, both of which were released concurrently with the Red Flags Rule. See the FTC's Policy Enforcement Statement [here](#).

Do you have clients that are covered by the Red Flags Rule? If so, have they put the Red Flags procedures into place?

### Who Must Comply

Although every business that has an ongoing relationship with consumers should keep an eye out for the possibility of identity theft, the Red Flags Rule applies only to “**financial institutions**” and “**creditors.**” To determine if a business or organization is covered by the Rule and needs to implement a written ID Theft Program, you will need to answer two questions:

- 1) Is the business a “**financial institution**” or “**creditor,**” as those terms are statutorily defined?
- 2) If so, does it have “**covered accounts**”?

The FACT Act imported the definition of “**financial institution**” from Section 19(b) of the Federal Reserve Act.<sup>3</sup> This definition covers banks, savings and loans, credit unions, or any other entity that directly or indirectly holds a “transaction account” belonging to a consumer. A