BNA, INC.

PRIVACY & SECURITY LAW

BNA Employee-Owned Since 1947

REPORT

Reproduced with permission from Privacy & Security Law Report, 10 PVLR 64, 01/10/2011. Copyright © 2011 by The Bureau of National Affairs, Inc. (800-372-1033) http://www.bna.com

Practical Implications of Massachusetts' New Comprehensive Data Security Regulations

BY BETH I.Z. BOLAND, KRISTEN E. FERRIS, AND SCOTT C. KLEEKAMP

Overview—The Massachusetts Regulations May Affect *Your* Business

In response to the growing number of data and identity theft incidents involving residents of the Commonwealth in recent years, Massachusetts regulators took significant steps toward increasing regulatory control over data security. Effective March 1, 2010, the Massachusetts Office of Consumer Affairs and Business Regulation (OCABR) adopted 201 CMR 17.00 *et seq.* (the "Regulation"), which is intended to establish the "minimum standards to be met in connection with the safeguarding of personal information" with the objective of ensuring the "security and confidentiality of customer information in a manner fully consistent with industry practice."[1]

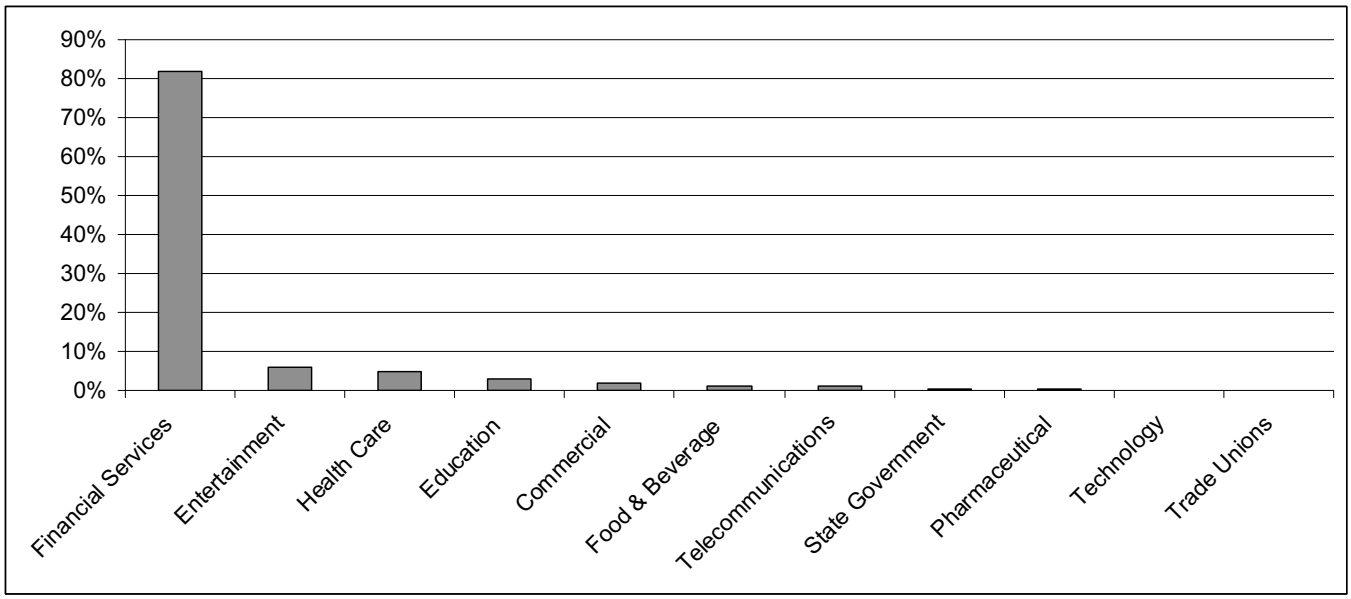
The Regulation is comprehensive in substantive scope and in geographic reach, and applies to *any* entity—*no matter where located*—that "owns or licenses"[2] any "personal information"[3] about a resident

Beth I.Z. Boland is a partner in the Privacy and Security Practice Group at Bingham McCutchen, LLP. Kristen E. Ferris and Scott C. Kleekamp are associates in the Corporate and Financial Services areas, respectively, at the firm.

[1] 201 CMR 17.01(1) (emphasis added).

[2] The Regulation defines "owns or licenses" to include any entity that "receives, stores, maintains, processes, or otherwise has access to" personal information "in connection with the provision of goods or services or in connection with employ-

COPYRIGHT © 2011 BY THE BUREAU OF NATIONAL AFFAIRS, INC. ISSN 1538-3423



of the Commonwealth. The Regulation implements a risk-based approach to information security instead of a one-size-fits-all approach to complying with every component of the Regulation. According to the OCABR, an organization should take into account its size, scope and type of business, the amount of resources available to the organization, the amount and type of data collected or stored, and the need for security and confidentiality of employee and/or consumer information.[4] How, exactly, this ''risk-based'' approach will be enforced remains an open question: while many aspects of the Regulation are seemingly straight-forward, compliance with the Regulation raises practical and legal questions for many companies.

Background

Some clues may lie in the history behind the adoption of the Regulation. In 2007, the Massachusetts legislature enacted Mass. Gen. Laws ch. 93H: Security Breaches, which, among other things, mandates the reporting of data breaches involving personal information and the disposal of personal information.[5] The law also directed OCABR to adopt regulations ''designed to safeguard the personal information of residents of the commonwealth and shall be consistent with the safeguards for protection of personal information set forth in the federal regulations by which the person is regulated.''[6]

OCABR analyzed the breach notifications it received under the new law, and released two reports, on Feb. 2, 2009 and Nov. 4, 2009 (the ''OCABR Reports''). The OCABR Reports indicated that over 800 breach notifications were filed with the OCABR between October 2007 and November 2009; we understand that the frequency of breaches has increased since then. Of those notifications, approximately 750 were reported by businesses, approximately 40 were reported by educational institutions and 45 were reported by state government.[7] Moreover, almost 500 cases ''were the result of criminal or otherwise unauthorized acts, including the theft of laptops, outside intrusion into databases that may not have been protected by encryption, or the intentional accessing of information by unapproved individuals.''[8] The reports also showed that the industry most affected by reported breaches was the financial services sector,

---

ment.'' 201 CMR 17.01(1). *See also* Commonwealth of Mass. Office of Consumer Aff. and Bus. Reg., Frequently Asked Questions Regarding 201 CMR 17.00 (Nov. 3, 2009) (''Frequently Asked Questions''). The use of credit card swiping technology, which batches out such data in accordance with the Payment Card Industry (PCI) standards and does not otherwise have actual custody or control over the personal information, is not considered sufficient to ''own or license'' personal information with respect to that data. *Id.*

[3] ''Personal information'' is defined as a Massachusetts resident's first name (or initial) and last name in combination with any one of the following: (1) Social Security number, (2) driver's license number or state-issued identification card number, or (3) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account. 201 CMR 17.02. The term ''financial account'' includes checking accounts, savings accounts, mutual fund accounts, activity accounts, any kind of investment accounts, and credit or debit accounts, as well as other accounts, such as insurance policy numbers if it ''grants access to a person's finances, or results in an increase of financial burden, or a misappropriation of monies, credit or other assets.'' *See Frequently Asked Questions,* at 3, 4.

[4] *Id*. Notably, OCABR published a guide to assist small businesses including self-employed persons, in developing a WISP. *See* Commonwealth of Mass. Office of Consumer Aff. and Bus. Reg., A Small Business Guide: Formulating A Comprehensive Written Information Security Program, *available at:* http://www.mass.gov/Eoca/docs/idtheft/sec_plan_smallbiz_guide.pdf

[5] Mass. Gen. Laws ch. 93H (2007).

[6] Mass. Gen. Laws ch. 93H § 2(a).

[7] *See* Commonwealth of Mass. Office of Consumer Aff. and Bus. Reg., 2009 Report on Data Breach Notifications (Nov. 4, 2009), *available at* http://www.mass.gov/Eoca/docs/idtheft/breachreport20091104.pdf.

[8] *Id.*

 COPYRIGHT © 2011 BY THE BUREAU OF NATIONAL AFFAIRS, INC. PVLR ISSN 1538-3423

which alone accounted for over 80 percent of the breaches reported.[9]

OCABR also issued its first iteration of the Regulation on November 14, 2008, which was promulgated as an ''emergency regulation'' and originally scheduled to be effective January 1, 2009.[10] OCABR proposed amending the Regulation to, among other things, extend the deadline for compliance from January 1, 2009 generally to May 1, 2009, in order to give businesses the opportunity to undertake compliance, and held a public hearing on January 16, 2009 to provide parties an opportunity to comment on the Regulation and to provide written comments thereto.[11] OCABR filed revisions to the Regulation on Feb. 12, 2009 and Aug. 17, 2009, and, after a final notice and comment period, filed its final amended version of the Regulation in October 2009 with an effective date of March 1, 2010.[12]

Not surprisingly, the Regulation focuses in large part on the sources of data breaches identified in the OCABR Reports. More to the point, those industries which have experienced large numbers of breaches—*e.g.*, the financial services industry and retail industries—may be particularly prone to heightened regulatory and enforcement scrutiny.

Written Information Security Program

Under the Regulation, all persons who own or license personal information about a Massachusetts resident must develop, implement, and maintain a comprehensive written information security program (WISP). The requirements may have different meanings and effects on different organizations given the risk-based approach, thus each requirement should be tailored to your organization's needs.

A look at some of the requirements and a practical analysis for each:

- **Designate one or more employees to maintain the WISP.** Determine who in your organization should be the point person to lead and coordinate your compliance efforts. A larger organization may wish to designate a team to be responsible for ongoing compliance, which can and should include representatives from various departments, including information technology, human resources, legal, corporate communications, audit and key business divisions. A smaller organization, or even sole practitioner, can probably manage with a single point person coordinating the various aspects of such departments as applicable. It is important to keep in mind the goal of a unified WISP that is appropriate for your organization given the type of industry, the amount of data collected, stored and transmitted.
- **Identify and assess reasonably foreseeable internal and external risks: data mapping.** Knowing how much personal information is owned and stored, as well as where it is maintained and how it is transmitted, will impact the extent of procedures your organization must follow. Although the Regulation does not require an organization to create a written inventory of its paper or electronic records or to post its WISP publicly, your organization should perform an internal risk assessment and analysis of the personal information it owns, stores, maintains and transmits in order to properly handle and protect that personal information in accordance with the Regulation.[13] For instance, a smaller organization that has limited employees and does not store any personal information besides employee data can perform an analysis of where the information resides and how it is used with relative ease. The larger the organization, however, the more involved a risk assessment and data inventory process will be. Again, a team comprised of representatives from various departments would serve useful, and we recommend that larger organizations consider utilizing data mapping as a tool to track hard copy and electronically-stored personal information.[14] Once your organization understands what, where and why personal information is owned, stored, maintained or transmitted, you can assess what type of security measures are needed to protect such personal information.
- **Develop security policies and training for employees.** Each organization should have policies in place relating to the storage, access and transportation of records containing personal information both inside and outside of business premises. A policy for a smaller organization that does not store any personal information besides employee data can be as simple as locking all files in storage cabinets, locking the storage room and permitting access only to those who require it for official duties.[15] As a rule, employees should not have access to records that contain personal information if such access is not required to do an employee's job. A more robust policy may be required, however, if your organization's employees travel frequently outside of the business premises and travel with company-owned equipment that contains personal information, such as laptops, blackberries or even hard-copies of files.

  Each organization should develop a process that prevents terminated employees from accessing records containing personal information, such as disabling access cards, usernames and passwords, and requiring the return of all company-owned equipment. Any process must be coordinated with your organization's information technology department (if applicable) and operations and/or security departments. We recommend incorporating this process and return of equipment as part of an

[9] *Id.; see also* Commonwealth of Mass. Office of Consumer Aff. and Bus. Reg., Report on the M.G.L. Chapter 93H Notifications (Sept. 18, 2009), *available at* http://www.mass.gov/Eoca/docs/idtheft/notificationsrpt20080918.pdf.

[10] Commonwealth of Mass. Office of Consumer Aff. and Bus. Reg., Notice of Public Hearing (Dec. 1, 2008), *available at http://www.mass.gov/Eoca/docs/idtheft/publichearing_201cmr17amend.PDF*.

[11] *Id.*

[12] 201 CMR 17.00 *et seq.* (2009).

[13] *See* Frequently Asked Questions, at 4.

[14] *See e.g.* Mary Beth Hamilton, *Defining Data Mapping and Data Loss Prevention Technology for Financial Firms*, Hedge IT Blog, May 6, 2010, http://www.eci.com/blog/13-defining-data-mapping-and-data-loss-prevention; David Wetmore and Scott Clary, *To Map or Not to Map: Strategies for Classifying Sources of ESI*, Information Management, September/October 2009, at 33.

[15] *See* Frequently Asked Questions, at 4.

exit interview process.

What is most important for all organizations, is the education and training of its employees. There is no ''bright line'' rule as to the amount of employee training required under the Regulation—OCABR merely suggests that an organization conduct ''enough training to ensure that the employees who will have access to personal information know what their obligations are regarding the protection of that information.''[16] We recommend providing a copy of your WISP to each of your employees and requiring them to sign a compliance and/or acknowledgement certificate. In addition, businesses should host mandatory training sessions at least annually for employees that address your organization's security practices and procedures, reporting procedures and any updates to your organizations WISP.

- **Oversee third-party service providers.** Organizations are required to (1) take ''reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect such personal information consistent with these regulations and any applicable federal regulations,'' and (2) require third-party service providers by contract to ''implement and maintain such appropriate security measures for personal information.''[17] Although the Regulation does not elaborate on the ''reasonable steps'' required in selecting a third-party service provider, organizations should be diligent in selecting third-party service providers. Each industry may differ slightly, but third-party service providers should be asked whether they have had any incidents of data breaches and the courses of action taken. Businesses should also request a copy of the service provider's WISP and any other policies and procedures it maintains with respect to data security. To assist your organization in requiring your third-party service providers to maintain the appropriate security measures, the Regulation also requires that third-party providers to contractually agree to implement and maintain appropriate security measures. Although there is no specific contractual language required, businesses should consider adding specific provisions in contracts, such as:

  1. Remedies provisions in the event the third-party provider breaches its security obligations (*i.e.*, liquidated damages and indemnification obligations, including attorney's fees and any costs associated with any loss of personal information by the third-party provider);
  2. Adequate level of insurance provisions; and
  3. Notice provisions that requires the third-party provider to notify you in the event of a suspected or known security breach, whether or not directly involving your organization.

  These contractual provisions may help ensure that the third-party service provider is aware of and agreeing to its obligations under the Regulation. Such provisions can also provide your organization with some comfort that while you cannot constantly monitor the service provider's activities to ensure compliance, the service provider is contractually obligated to comply with the Regulation.
- **Regular monitoring.** The Regulation requires ''[r]egular monitoring to ensure that the comprehensive security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information,'' and ''ongoing employee (including temporary contract employee) training.''[18] Although the Regulation requires, at minimum, an annual review of the scope of an organization's security measures, the frequency of such monitoring again depends on a risk-based approach, which in turn depends largely on the nature of the organization's business, the amount of personal information owned or licensed by the organization and whether the personal information is maintained in paper records or electronically-stored records.[19] While each organization must determine what is necessary, required and appropriate for compliance with the Regulation, to the extent data security maintenance within the organization is subject to changing industry standards, the need for more frequent monitoring of the sufficiency of the WISP may increase as well.
- **Establish and maintain up-to-date computer security systems.** To the extent personal information is electronically-stored or transmitted by your organization, the WISP must also include the establishment and maintenance of security system covering your computers, including any wireless system and encryption methods.[20] The Regulation outlines certain ''minimum'' security requirements that an organization must adopt so long as they are ''technically feasible'':

  1. ''Reasonably up-to-date'' firewall protection and operating system security patches for files containing personal information on a system that is connected to the Internet and versions of system security agent software, which must include malware protection and ''reasonably up-to-date'' patches and virus definitions;
  2. Secure user authentication protocols including (i) control of user IDs, (ii) ''reasonably secure'' methods of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices, (iii) control of data security passwords, (iv) restricting access to active user and user accounts, and (v) blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system; and

[16] *Id.*

[17] 201 CMR 17.03(f). We note that there is a carve-out for contracts entered into prior to March 1, 2010, which will be deemed to satisfy the Regulation's provisions regarding third-party service providers until March 1, 2012. This exception applies even if the contract does not include any provisions requiring the third-party service provider to maintain appropriate security measures. New service provider contracts, as well as any grandfathered contracts that extend past March 1, 2012, however, must require by contract that the third-party provider will implement and maintain such appropriate security measures for personal information.

[18] 201 CMR 17.03.

[19] *See* Frequently Asked Questions, at 1, 3.

[20] 201 CMR 17.04.

 COPYRIGHT © 2011 BY THE BUREAU OF NATIONAL AFFAIRS, INC. PVLR ISSN 1538-3423

3. Encryption of all transmitted records and files containing personal information that will travel across public networks and encryption of all data containing personal information to be transmitted wirelessly.[21]

According to the OCABR, a security requirement is considered ''technically feasible'' ''if there is a reasonable means through technology for an organization to accomplish a required result.''[22] Unfortunately, there is little guidance as to what this phrase means in practice. For example, the OCABR in November 2009 suggested that ''there is little, if any, generally accepted encryption technology for most portable devices, such as a cell phones, blackberries, net books, iphones and similar devices,''[23] but since that time those technologies have progressed significantly. We do know that the Regulation takes into account industry standards in determining what is ''reasonable'' and ''technically feasible''; as data security technology becomes more accessible, advanced, or well-adopted, the standards for what is considered ''reasonable'' or ''reasonably up-to-date'' will inevitably evolve as well. As a result, organizations should be aware that a technology platform that makes them Regulation-compliant today may not be compliant tomorrow, and should monitor their systems and make upgrades when appropriate.

- **Encryption decrypted.** One of the requirements that has raised many practical questions with organizations is the duty to encrypt certain types of data transmissions and storage devices. The Regulation requires an organization to encrypt personal information (1) traveling across ''public networks'' or ''transmitted wirelessly,'' or (2) stored on ''laptops and other portable devices.''[24] The requirements are fairly straight-forward if the personal information is stored on laptops or other portable devices and backup tapes, but the Regulation contains no definition or other guidance as to what constitutes a ''public network'' or ''wireless transmission.'' And because data encryption requires the ''transformation of data into a form in which meaning cannot be assigned without the use of a confidential process or key,'' the data must be altered into an unreadable form: password protection alone does *not* satisfy the regulatory requirements.[25]

  To the extent that encryption is not ''technically feasible,'' your organization must take alternative and appropriate steps to secure and protect the personal information.[26] Alternative means may include the following:

  1. Uploading the data to a secure website or datasite that requires the recipient to log in with a username and password to access the data;
  2. Employing a mandatory transport layer security (TLS) link, which provides security for e-mail communication; or
  3. Utilizing a virtual private network (VPN) link, which can be used to encrypt all types of Internet communication between organizations. We recommend working with your information technology department (if your organization has one) to understand what encryption technology is available to your organization and any alternative means available, to the extent encryption is not ''technically feasible.''

  If your organization needs to send data that contains personal information to another organization that cannot receive encrypted data, such as certain governmental agencies, you should contact the recipient to set up an alternative means of transmission. And, for certain regulated entities such as broker-dealers that are required to review and monitor employee e-mails in accordance with industry-specific regulations, if mass encryption interferes with that obligation, that entity should discuss with their information technology group an alternative means by which the requisite sampling of e-mails can be reviewed.

  It is important to educate all members of your organization, which can and should be done in conjunction with your employee training, regarding the encryption requirement so that each employee understands that e-mails should *not* be sent outside of your organization that contain personal information without being encrypted. If an e-mail cannot be encrypted, one of the alternative methods (or other similar methods that your organization may utilize) should be utilized.
- **Backup Tapes.** If your organization maintains backup tapes, tapes created after March 1, 2010 must be encrypted as they are being created, but tapes created prior to March 1, 2010 need not be encrypted unless they will be transported from current storage elsewhere.[27] In such case, the tapes must be encrypted prior to transfer if the tape allows it and if not, OCABR suggests taking additional steps to safeguard the tapes, such as using secured transport.[28] We recommend taking the same care and steps that your organization takes with respect to transporting other hard copies of documents that contain personal information, which may include a third party information management service to transport your tapes. In addition, unencrypted backup tapes, like other media containing personal information, should be stored using reasonable precautions to ensure their security.

Pay Attention to Industry Standards and Other Data Security Regimes

The Regulation specifically states that its objectives are to ensure the security and confidentiality of customer information in a manner ''fully consistent with industry standards,'' and that the safeguards contained

[21] 201 CMR 17.04; *See also* Frequently Asked Questions, at 2.

[22] 201 CMR 17.04; *See also* Frequently Asked Questions, at 2.

[23] *See* Frequently Asked Questions, at 2.

[24] 201 CMR 17.04.*; See also* Frequently Asked Questions, at 2.

[25] 201 CMR 17.02; *See also* Frequently Asked Questions, at 3.

[26] 201 CMR 17.04; *See also* Frequently Asked Questions, at 2.

[27] *Id.*

[28] *Id.* While OCABR suggests utilizing secure transport such as armored vehicles and guards, Frequently Asked Questions, at 2, OCABR staff has informally noted that other reasonable means of curing transport may also suffice.

in a WISP ''must be consistent with the safeguards for protection of personal information and information of a similar character set forth in any state or federal regulations.''[29] There is no interpretation in the Regulation nor from OCABR that explains what level of ''consistency'' is required under this language. Similarly, the Regulation requires compliance with its provisions even if an organization is compliant with another security regime, such as HIPAA.[30] As such, any organization that is subject to the requirements of the Regulation must not only be mindful of other state and federal laws or regulations, but also relevant industry standards.[31] Until additional guidance is provided by OCABR or via enforcement actions, organizations should aim to implement ''best practices'' to the extent necessary and appropriate, from each of the regimes to which it is subject.

* * *

The Regulation requires companies to take a variety of measures to protect and safeguard personal information of Massachusetts residents. Given the nuances of the Regulation, to the extent your organization still has questions as to the practical implications of the Regulation, you should contact your attorney or a member of Bingham's Privacy and Security Group to ensure your organization is fully compliant.

---

[29] 201 CMR 17.03(1).

[30] *See* Frequently Asked Questions, at 3.

[31] Note, in particular, that recent litigation involving theft of credit card numbers from retailers have cited the retailers' noncompliance with Payment Card Industry standards as a factor in support of the statutory violations alleged. *See e.g.*, *In Re TJX Companies Retail Security Breach Litigation*, No. 07-10162 (D. Mass.) (docket # 203, Plaintiff's Memorandum In Support Of Motion For Leave To Amend); Jaikumar Vijayan, *TJX Violated Nine of 12 PCI Controls At Time Of Breach, Court Filings Say*, Computerworld, October 26, 2007, *http://www.computerworld.com/s/article/9044321/TJX_violated_nine_of_12_PCI_controls_at_time_of_breach_court_filings_say*.

 COPYRIGHT © 2011 BY THE BUREAU OF NATIONAL AFFAIRS, INC. PVLR ISSN 1538-3423