EDWARDS ANGELL PALMER & DODGE

eapdlaw.com

Client Advisory | *November 2008*

New Massachusetts Guidelines for Mandatory Computer Security Policies

Massachusetts already has one of the most aggressive data security regulations in the country, and robust new guidelines were just issued to implement this regulation, effective January 1, 2009.

Mark E. Schreiber, Partner
Chair, Privacy Group

Theodore P. Augustinos, Partner

Socheth Sor, Associate

The Massachusetts Office of Consumer Affairs and Business Regulations (OCABR) recently released and posted on its website three new documents designed to assist companies in complying with heightened standards for the protection of personal information and to reduce the risk of data breaches. Any business, regardless of where they are located, that owns, licenses, stores or maintains defined personal information of Massachusetts residents, including employees, must develop or revise its existing security policies to satisfy the new Massachusetts rules.

This will be a challenging task even for sophisticated corporations, much less small businesses, to have in place by January 1, 2009, and will necessitate the collaboration of various company personnel in their compliance, IT and human resources departments.

While the enforcement date of the new Federal Red Flag rules for financial institutions and creditors has been extended by the FTC to May 1, 2009, companies with Massachusetts personal data will have enhanced security compliance obligations much sooner. How large corporations will begin to fold or integrate these new Massachusetts policies into their existing security, incident response and data breach procedures remains to be seen. The effects of and penalties for non-compliance, especially in the event of later data breach cases, lie in uncharted territory.

The scope and depth of these guidelines will require significant time and effort for companies owning or storing personal data of Massachusetts residents. There is no "de-minimus" standard, small companies are not exempt, and no particular industry segments are excluded. Companies that operate outside of Massachusetts are covered with respect to personal data of Massachusetts residents, including employees, that the entity maintains. Personal information is defined as first and last name (or initial) with any one or more of: Social Security number, driver's license number, state I.D. card number, financial account number, or credit or debit card number, with or without security code, access code, passwords or PIN.

While many companies already have dedicated security and incident response policies in place, the Massachusetts requirements go further in critical respects. These new requirements mandate data encryption covering laptops and wireless devices, training and monitoring of employees who use such systems, and pass-through obligations to third-party vendors. A comprehensive, written information security program ("WISP") applicable to any records containing such personal information is now required.

The new OCABR documents clarify 201 CMR 17.00, Standards for the Protection of Personal Information of Residents of the Commonwealth (the "Regulation"), which was finalized and issued in recent months. As reported in our previous Advisory, the Regulation, effective January 1, 2009, establishes minimum standards for safeguarding personal information contained in both paper and electronic records. Under the Regulation, every person (defined to include business entities) that owns, licenses, stores or maintains personal information about Massachusetts residents is required to develop, implement, maintain and monitor a WISP. A WISP must address

the establishment and maintenance of a detailed computer security system with respect to personal information.

New FAQs, Guide and Checklist

The three new OCABR documents are a set of frequently asked questions (FAQs), guidelines intended to assist with the development of the required WISP, and a checklist to assist in compliance with the Regulation.

The FAQs address certain obligations and computer system requirements under the Regulation. The "Small Business Guide for Formulating a Comprehensive Written Information Security Program" (the "Guide") contains a model WISP to aid individuals and small businesses in their development of a compliant WISP. The checklist contains questions with respect to how a company safeguards personal information and the efforts a company has to take to ensure an effective security policy. All of the documents are available on the OCABR's website, links for which are noted at the end of this Client Advisory.

Note that the term "small business" is not defined under the Regulation, and it is unclear what constitutes a small business as the term is used in the Guide and checklist. (The OCABR Small Business Impact Statement uses a figure of 10 employees and estimates a $3,000 upfront compliance cost with no more than $500/month maintenance.) However given the comprehensive detail of the Guide and checklist, even large companies may want to review them in tailoring their policies and practices.

Under the Regulation, compliance will be evaluated by taking into account (1) the size, scope and type of business; (2) the amount of resources available to such person; (3) the amount of data stored; and (4) the need for security and confidentiality of both consumer and employee information. The OCABR stresses in the FAQs, Guide and checklist that compliance under the Regulation is determined on a case-by-case basis, and as such, a WISP must be customized for each business.

The Massachusetts Attorney General's office is responsible for enforcement, not the OCABR.

Technical Compliance

The Regulation, FAQs, Guide and checklist make clear that computer systems must be updated to provide the level of security required under the Regulation. For example, a computer security program must have the following with respect to protection of "personal data:"

- Encryption of all transmitted records and files containing personal information that will travel across public networks and wirelessly;
- Secure user authentication protocols and access control measures, including control over user identifiers, passwords and access;
- A system for monitoring unauthorized use;
- Updated firewall and operating system security patches; and
- Post-incident review of security breaches and remedial action.

A company must evaluate its computer systems to determine what must be done to bring the company into compliance with these requirements. Whether these requirements or "selective protection" can be limited, as a practical matter, to systems that contain Massachusetts personal information, remains to be seen. The technical requirements listed above, particularly encryption of laptops and pda's, and others may be difficult to achieve, even if a company has an adequate IT staff to evaluate or resources to implement a compliant computer security system. The OCABR suggests in the FAQs that a company hire outside technical consultants if it does not have its own IT staff.

Training and Monitoring of Employees, and Post-Termination Limitations

Training and monitoring of employees with access to personal data are important requirements under the Regulation. The WISP must provide for ongoing employee training and procedures for monitoring employee compliance. One or more employees must be designated to maintain the WISP. When an employee is terminated, the WISP must provide a policy for blocking the terminated employee's physical and electronic access to records containing personal information.

In addition, the Guide provides a model provision which states that employment contracts must be amended to require all employees comply with the provisions of the WISP and prohibit any non-conforming use of personal information during or after

The model WISP also requires the retraining of employees immediately after the adoption of a WISP. Thus, human resource departments will need to be drawn into the WISP implementation process and new variations on acceptable use, e-mail, mail, and post-termination and related policies will need to be crafted.

employment. The model WISP also requires the retraining of employees immediately after the adoption of a WISP. Thus, human resource departments will need to be drawn into the WISP implementation process and new variations on acceptable use, e-mail, mail, and post-termination and related policies will need to be crafted.

Third-Party Vendors

The Regulation requires that companies select and oversee third-party service providers that are capable of maintaining safeguards for personal information and contractually require that third-party service providers adhere to such safeguards. In addition, the Regulation and Guide make clear that a company has a duty to ensure that independent contractors and third-party service providers who are hired to store or maintain, or who have access to, personal information provide written certification of their compliance with the Regulation.

In some instances this will require new provisions in independent contractor and service and vendor agreements, including possibly detailed security schedules. Whether existing pass-through security obligations and conditions in such agreements are sufficient will require a case-by-case review, and doubtlessly new versions, compliant with the Regulation, will start to emerge.

Amount of Personal Information Collected

Under the Regulation, a company must limit the amount of personal information collected to that reasonably necessary to accomplish the legitimate purpose for which it is collected. The period during which personal information is stored and/or available to be accessed must also be limited.

A company must evaluate its own specific needs to determine how to limit the amount of personal information collected and time and access to personal information. The determination should be based on the company's needs to perform the tasks required to satisfy its particular business needs. These stipulations are far easier said than done, as data storage and deletion procedures, particularly e-retention policies, have long been problematic in execution.

Source Information

Click below to view the new guidelines regarding the mandatory written security program.

- Frequently Asked Questions Regarding 201 CMR 17.00
- 201 CMR 17.00 Compliance Checklist
- Small Business Guide for Formulating a Comprehensive Written Information Security Program

The Regulation requires that companies select and oversee third-party service providers that are capable of maintaining safeguards for personal information and contractually require that third-party service providers adhere to such safeguards.

This advisory is for guidance only and is not intended to be a substitute for specific legal advice. If you would like any further information please contact:

Mark E. Schreiber, Partner and Chair, Privacy Group	617.239.0585	mschreiber@eapdlaw.com
Theodore P. Augustinos, Partner	860.541.7710	taugustinos@eapdlaw.com
Socheth Sor, Associate	860.541.7773	ssor@eapdlaw.com

EDWARDS ANGELL PALMER & DODGE

111 Huntington Avenue
Boston, MA 02199
Tel 617.239.0100
Fax 617.227.4420
eapdlaw.com