



Compliance Deadlines Extended But Comprehensive Data Security Regulations Still Looming in Massachusetts

*Do you have Massachusetts customers? Massachusetts employees? Do you maintain information about Massachusetts residents for any other reason?
Read on!*

Following on the heels of major data security breaches at TJ Maxx and other companies, the Massachusetts Legislature enacted a data security law intended to protect consumers' personal information. On September 19, 2008, the Massachusetts Office of Consumer Affairs and Business Regulation (OCABR) issued regulations prescribing specific policies and practices that must be adopted to comply with the law. OCABR's regulations establish requirements that far exceed data security provisions under federal law or the law of other states. Therefore, even businesses that have adopted security "best practices" or who – like banks and other financial service providers – have been subject to federal privacy and security laws for many years, will need to implement new security procedures to comply with the Massachusetts law.

Originally, the effective date for compliance with OCABR's regulations was January 1, 2009. However, as the complexity and extent of the regulations became evident, trade groups and others contacted OCABR and Governor Patrick requesting an extension. On November 14, 2008, OCABR announced a postponement. New compliance dates are as follows:

- General compliance, May 1, 2009
- Encryption of laptops, May 1, 2009
- Vetting of third party service providers, May 1, 2009
- Certifications by third party service providers, January 1, 2010
- Encryptions of PDAs and other portables, January 1, 2010

OCABR's decision to extend the effective dates reflects the difficulty of complying with the regulations. Implementing a comprehensive written information security program requires the involvement of human resources, technology, record retention, and administrative personnel. Postponement of the effective date should be viewed as breathing room, not break time. Efforts to implement a plan should continue as quickly as possible. Anyone who has not yet begun the process should do so immediately.



ALERT

The regulations are summarized below. Please pay particular attention to the provisions regarding encryption, identification of records containing personal information, and third party providers, which are likely to present the most challenging compliance issues.

If you have questions about the regulations or need help with implementation, please contact your Brown Rudnick attorney or one of the attorneys listed at the end of this Client Alert.

Who is subject to the law and regulations?

The law applies to any “legal entity,” including an individual or any form of business enterprise, that owns, licenses, stores, or maintains personal information about a resident of the Commonwealth of Massachusetts. This includes businesses that employ Massachusetts workers, providers of goods and services that have Massachusetts customers, third party service providers who receive information about Massachusetts residents under outsourcing contracts, and virtually anyone else who owns, licenses, stores, or maintains personal information about Massachusetts residents.

On their face, the regulations are not limited to persons doing business in Massachusetts or holding information in Massachusetts. Thus, any business that holds personal information about Massachusetts residents – even businesses located outside of Massachusetts – must be concerned. While it is possible that a person – or group of persons – with no direct contacts to Massachusetts may challenge the state’s authority to regulate businesses over which the state otherwise has no jurisdiction, the law, as it stands today, applies very broadly.

What is “personal information”?

“Personal information” is defined as a Massachusetts resident’s first name (or initial) and last name, in combination

with at least one of the following pieces of information;

(a) Social Security number, (b) driver's license or state issued identification number, or (c) financial account number, including but not limited to credit or debit card number.

Personal information does not include lawfully obtained public information or information from government records lawfully made available to the public.

The regulations apply to all personal information, whether contained in paper or electronic records.

What you need to know about the regulations

The regulations have three goals:

- Ensure the security and confidentiality of personal information,
- Protect against anticipated threats or hazards to security or integrity of personal information,
- Protect against unauthorized access to or use of such information in manner that creates a risk of theft or fraud.

Compliance with Massachusetts regulations may not satisfy the requirements of personal information laws of other states, and compliance with federal law or the laws of other states may not satisfy the Massachusetts requirements. If you or your business operates or has clients in more than one state, you must review the personal information laws of such states to ensure compliance with all relevant law. Compliance with these regulations is in addition to compliance with other federally mandated privacy or data security laws.

Standards for Protecting Personal Information

All persons subject to the regulations must implement, maintain and monitor a written information security program (sometimes referred to as a “WISP”). While the regulations itemize minimum requirements for a security program,

OCABR will take into account the size, type, and scope of business of the person, the person's available resources, and the amount and sensitivity of the data in determining whether the security program is sufficient.

The minimum requirements for an information security program are:

- *Employee Designee*
One or more employees must be designated to maintain the security program.
- *Identification of Internal and External Risks*
Risks to the security, confidentiality or integrity of personal information must be identified and assessed.
- *Evaluation and Improvement of Effectiveness of Current Safeguards*
Where necessary, the effectiveness of the safeguards limiting reasonably foreseeable risks must be evaluated and improved.
- *Employee Access*
Specific security program policies must be developed for employees, including whether and how employees will be permitted to handle records outside of the office.
- *Disciplinary Measures*
Internal disciplinary measures must be imposed for violations of the security program.
- *Terminated Employees*
An employee's physical and electronic access to personal information must expire immediately upon termination.
- *Third Party Providers*
Procedures must be put in place to verify that third party service providers (vendors) have the capacity to protect personal information. Before being given access to personal information, vendors must (a) enter into contractual commitments that they will maintain safeguards for personal information and (b) provide written certification that they have adopted a written information security program that complies with the Massachusetts regulations.
- *Limitation on Amount of Personal Information Collected*
Personal information may only be collected to the extent "reasonably necessary to accomplish a legitimate purpose" and may be held only for the time required to accomplish that purpose.
- *Identification of Storage of Personal Information*
Unless all records are secured as if they contain personal information, records containing personal information must be identified.
- *Physical Access to Personal Information*
Physical access to records containing personal information must be reasonably restricted in accordance with a written procedure.
- *Monitoring of the Security Program*
The security program must be monitored and upgraded as necessary to ensure it is operated in a manner that limits risks to the system.
- *Review of the Scope of the Regulations*
The security program must be reviewed and updated at least annually, and whenever there is a material change in business practice that the security of personal information.
- *Document Responsive Action*
Actions taken in response to a breach of security must be documented.

ALERT

Computer System Requirements

Persons who store or transmit personal information electronically must include computer system requirements in their security program. The requirements must apply to all systems, including wired and wireless systems, desktop and laptop computers, and PDAs.

■ *User Authentication Protocols*

The security program must include the following secure user authentication protocols:

- control of user IDs and other identifiers;
- a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;
- control of data security passwords;
- restricting access to active user accounts only; and
- blocking access to user identification after multiple unsuccessful attempts to gain access to the system.

■ *Secure Access Control Measures*

Access to records or files containing personal information must be limited to those who need such information to perform their job duties.

■ *Encryption of Transmitted Records and Files Containing Personal Information*

To the extent technically feasible, all transmitted records and files containing personal information that will travel across public networks must be encrypted, and all data to be transmitted wirelessly must be encrypted.

■ *Monitoring of Systems for Unauthorized Access*

Computer systems must be monitored for unauthorized use or access.

■ *Encryption of Stored Personal Information*

All personal information stored on laptops or other portable devices must be encrypted.

■ *Firewall Protection and Operating System Security Patches*

Reasonably up-to-date fire-wall protections and operating system security patches must be maintained to protect personal information on a computer system that is connected to the internet.

■ *Security System Agent Software*

Computer systems connected to the internet must include reasonably up-to-date versions of system security software that includes spy-ware, anti-virus and malware protection and must be set up to receive the most current security updates regularly.

■ *Education and Training*

Employees must be educated and trained in regard to the proper use of the computer security system and the importance of personal information security.

To view the full content of the regulations, please visit:

http://www.mass.gov/?pageID=ocamodulechunk&L=1&L0=Home&sid=Eoca&b=terminalcontent&f=idtheft_201cmr17&csid=Eoca

Notification Requirements

In addition to directing OCABR to adopt regulations on information security programs, the Massachusetts data security law mandates that persons who own, license, maintain, or store personal information comply with certain notification obligations in the event of a breach of security or unauthorized access or use. In essence, a person who maintains or stores personal information that is owned by another is obligated to notify the owner of the breach and cooperate with the owner by providing needed information. The owner of the information must notify the person whose information was affected, the state Attorney General, OCABR, and any consumer reporting agency or state agency OCABR instructs the owner to notify. All required notifications of breaches must be made as promptly as practicable, but a law enforcement agency can require that

Boston

One Financial Center
Boston, MA 02111
+1.617.856.8200
+1.617.856.8201 [fax]

New York

Seven Times Square
New York, NY 10036
+1.212.209.4800
+1.212.209.4801 [fax]

Hartford

City Place I
185 Asylum Street
Hartford, CT 06103
+1.860.509.6500
+1.860.509.6501 [fax]

Providence

121 South Main Street
Providence, RI 02903
+1.401.276.2600
+1.401.276.2601 [fax]

London

8 Clifford Street
London, W1S 2LQ
United Kingdom
+44.20.7851.6000
+44.20.7851.6100 [fax]

Washington, D.C.

601 Thirteenth Street NW
Suite 600
Washington, DC 20005
+1.202.536.1700
+1.202.347.4242 [fax]

Dublin

Alexandra House
The Sweepstakes
Ballsbridge, Dublin 4
Ireland
+353.1.664.1738
+353.1.664.1838 [fax]

www.brownrudnick.com

notice be delayed if notice could impede a criminal investigation. The statute specifies the information required to be provided in the notice.

Brown Rudnick Can Help

Although you now have a bit more breathing room, security programs that comply with the Massachusetts regulations must still be implemented very soon.

If you have any questions or need assistance with the implementation of the Massachusetts regulations or the requirements of other states, please contact your Brown Rudnick attorney or one of the following attorneys:

Cheryl B. Pinarchick

(617) 856-8266

cpinarchick@BrownRudnick.com

Elizabeth A. Ritvo

(617) 856-8249

eritvo@BrownRudnick.com

Nancy R. Wilsker

(617) 856-8343

nwilsker@BrownRudnick.com

Jennifer Herz contributed to this alert

Brown Rudnick is an international law firm with offices in the United States and Europe. Our 220 attorneys provide assistance across key areas of the law, including complex litigation and arbitration, government law and strategies, climate and energy, corporate and securities, finance, bankruptcy and restructuring, health law, intellectual property, and real estate.

Information contained in this Alert is not intended to constitute legal advice by the author or the attorneys at Brown Rudnick LLP, and they expressly disclaim any such interpretation by any party. Specific legal advice depends on the facts of each situation and may vary from situation to situation.

Distribution of this Alert to interested parties does not establish an attorney-client relationship. The views expressed herein are solely the views of the authors and do not represent the views of Brown Rudnick LLP, those parties represented by the authors, or those parties represented by Brown Rudnick LLP.

