

## News from our Privacy Group

# Massachusetts Significantly Revises Information Security Regulations and Extends Compliance Deadline Again

The Massachusetts information security regulations that propose new standards for how personal information of Massachusetts residents must be protected—201 CMR 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth—have been amended yet again and the deadline by which companies must be in compliance with the regulations has also been extended until March 1, 2010. For the second time now, the Massachusetts Office of Consumer Affairs and Business Regulation (OCABR) has taken a red pen to the regulations [[www.mass.gov/Eoca/docs/idtheft/201CMR1700reg.pdf](http://www.mass.gov/Eoca/docs/idtheft/201CMR1700reg.pdf)] and what was originally intended to be sweeping changes to how businesses must deal with and protect personal information of Massachusetts residents has been substantially softened. Additionally, the OCABR has issued a list of Frequently Asked Questions (“FAQ”) [[www.mass.gov/Eoca/docs/idtheft/201CMR17faqs.pdf](http://www.mass.gov/Eoca/docs/idtheft/201CMR17faqs.pdf)], that provides some detail into the changes and interpretation of certain language in the regulations.

According to the FAQ, these most recent changes are aimed at bringing the requirements of the regulations more in line with a “risk-based approach.” As revised, the regulations now direct a business to adopt a written security program that takes into account (1) that business’s size and scope, (2) its resources, (3) the nature and quantity of the data collected or stored and (4) the need for security. The revised regulations make this intent clear by including this language with what is required of the

written security policy, replacing the previous language that required such policy to be “reasonably consistent with industry standards.” Among the other changes to the regulations are:

- ▶ Whereas the original regulations required the encryption of personal information and defined encryption to involve “the use of an algorithmic process, or alternative method at least as secure,” the revised regulations remove this language from the definition of encryption in an attempt to make this technology neutral where encryption is required in the regulations.
- ▶ The revised regulations remove several specific provisions that were listed as requirements of any written security policy under the original regulations. Since the original list was not intended to be exhaustive, it is possible that these provisions may still be appropriate when applying the risk-based approach; however, they are no longer absolutely required in order to comply with the regulations. The provisions removed from the requirements of a security policy are: (1) taking into account whether and how employees should keep, access and transport records when developing the policy for employees, (2) immediately terminating physical and electronic access to records by terminated employees, (3) limiting the amount of personal information collected and the amount of time records are retained, (4) identifying where personal information is used

and stored and (5) requiring a written procedure for how access to records is restricted.

- ▶ For businesses using third party service providers given access to personal information, the revised regulations soften the oversight requirements on businesses so as to be more consistent with federal law. Businesses must still take reasonable steps to retain service providers capable of protecting personal information and contractually require that such provider implement and maintain appropriate security measures, but the revised regulations now

## KEY ATTORNEY CONTACTS

Alfred Browne	617/937-2310 abrowne@cooley.com
Robin Lee	650/849-7013 rjlee@cooley.com
Mike Rhodes	858/550-6017 rhodesmg@cooley.com
Adam Ruttenberg	703/456-8065 aruttenberg@cooley.com
Charles Schwab	720/566-4064 schwabca@cooley.com
Miguel Vega	617/937-2319 mvega@cooley.com

This information is a general description of the law; it is not intended to provide specific legal advice nor is it intended to create an attorney-client relationship with Cooley Godward Kronish LLP. Before taking any action on this information you should seek professional counsel.

Copyright © 2009 Cooley Godward Kronish LLP, 3000 El Camino Real, Palo Alto, CA 94306. Permission is granted to make and redistribute, without charge, copies of this entire document provided that such copies are complete and unaltered and identify Cooley Godward Kronish LLP as the author. All other rights reserved.

include a grandfather clause regarding the contractual requirement. Any contract with a third party service provider entered into before March 1, 2010 will be deemed to meet the contractual requirements of the regulations.

- ▶ Where personal information is electronically stored or transmitted, the regulations require additional provisions to be included in the written security policy to cover a business's computers and portable devices, such as authentication protocols, access controls and encryption. The revised regulations now only require all of these additional provisions to be included to the extent "technically feasible." Although not defined in the regulations, the FAQ defines "technically feasible" to mean that "there is reasonable means through technology to accomplish a required result."

If you receive, maintain, process, or otherwise have access to personal information of Massachusetts residents, you must comply with these revised regulations by the new deadline of March 1, 2010. If you have any questions regarding this update or how the regulations discussed herein could affect your company, please contact one of the attorneys listed above. ■