

## News from our Privacy Group

# Effective January 1, 2009, Massachusetts Regulations to Mandate Standards for Data Protection of Personal Information

Massachusetts has issued sweeping regulations requiring companies to incorporate features into their security policies in an effort to combat identity theft. With the advent of the Digital Age and the near ubiquitous use of computers and the Internet in the U.S., a growing number of individuals regularly provide companies with their personal data—information that identifies a person such as a name, social security number, driver's license or financial account information. As the sharing of personal data has become somewhat commonplace for consumers and businesses, this information has also become the growing target of identity thieves, as evidenced by the occurrence of several large data breaches in recent years.

Most companies already take some precautions to protect and secure the personal data that they use and maintain. Recognizing the importance of this issue, almost all of the states, starting with California, have enacted some form of data breach notification law that require businesses to notify individuals if a breach of stored personal data occurs. These laws protect individuals by allowing them to take measures to limit the damages from a breach as well as reduce the risk of identity theft by encouraging companies to bolster their security policies since notifications can be both costly and damaging to a company's reputation.

More recently, there has been a focus at both the state and federal level to enact legislation that goes beyond mere notification

of data breaches. Some states, most recently Nevada, have enacted regulations or laws that mandate specific security requirements and impose legal liability on companies storing personal data who do not provide adequate security for the personal data they store.<sup>1</sup> However, most states that have passed or that are considering such laws often only require a reasonable level of security rather than a comprehensive set of security requirements for a company to comply with.

Starting in January 2009, however, companies dealing with Massachusetts' residents will now have a very specific set of security standards to guide and regulate their implementation of a data protection policy—*201 CMR 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth*.<sup>2</sup> Recently released by the Massachusetts' Office of Consumer Affairs and Business Regulations, these regulations specify the types of personal data protected, what uses of this data by companies are covered by the regulations, and a set of standards and security requirements for companies to implement.

### Scope of the regulations

To fall under these regulations, personal information must take on a very specific form. The information must be non-public data that contains a Massachusetts resident's first and last name or first initial with last name, in combination with any of the following:

- (1) Social Security number; or

- (2) driver's license number or state-issued identification card number; or
- (3) financial account number or credit card or debit card number (with or without any security code, access code or password).

The regulations apply in every circumstance irrespective of how a company obtains the information. They apply to companies that host consumer data of the types described above, but also to any company that employs a Massachusetts resident, because employee records will always contain data that is personal information. If you are a company that owns, licenses, stores or maintains this type of data either electronically or on paper, then

### KEY ATTORNEY CONTACTS

Alfred Browne	617/937-2310 abrowne@cooley.com
Jim Donato	415/693-2047 jdonato@cooley.com
Charles Schwab	720/566-4064 schwabca@cooley.com
Paul Schwartz	720/566-4082 schwartzph@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 © 2008 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.

you must meet the minimum standards of protection set forth in these regulations.

### What is required to comply?

Where a company is using personal information within the regulation's scope, that company must develop, implement, monitor *and* maintain a comprehensive, written information security program. This program must be reasonably consistent with industry standards and contain some administrative, technical, and physical safeguards. Although there is no bright line as to whether a company's security program will comply, since this depends on the nature of the business and the amount of personal information processed, the regulations do provide a list of features that every written information security program must contain. These features are as follows:

- (1) Designate at least one employee to maintain the program
- (2) Regularly assess risks to the security of stored personal information and mitigate any risks by improving the safeguards
- (3) Develop security policies for employees that access and transport personal data records and prevent terminated employees from access these records
- (4) Impose disciplinary measures for violations of a company's security program
- (5) If using third-party service providers, take reasonable steps—including obtaining written certification—to verify that they have an information security program that complies with these regulations
- (6) Limit the amount, time retention, and access of personal information to that reasonably necessary to accomplish the company's legitimate purpose
- (7) Regularly identify which records and storage media (including laptops) contain personal information
- (8) Adequately store and restrict physical access to personal information
- (9) Regularly monitor the effectiveness of the security program and review the scope of the security program at least annually
- (10) Document actions taken in response to security breaches

Where a company using personal information within the regulation's scope also electronically stores *or* transmits that information, that company must also establish and maintain a security system covering its computers and must educate its employees on the proper use of such system. Features that the security system must contain are:

- (1) Secure user authentication protocols, such as control of user IDs and passwords
- (2) Secure access control measures to properly restrict access
- (3) Encryption of data that is sent over public networks, transmitted wirelessly, or stored on laptops or other portable devices
- (4) System monitoring for unauthorized use, firewall protection for Internet connections and use of up-to-date versions of software in the security systems.

### What should you do?

Evaluate your existing IT security policies now. These regulations impose a level of protection of personal data never before seen in the U.S., but are frequently covered by existing IT security policies. Begin working with your outside counsel to determine the extent these new regulations will affect you and identify what steps you need to take to become in compliance when the regulations go into effect on January 1. Depending on what safeguards your company already has in place, extensive modifications and documentation may be necessary.

If you have any questions regarding this update or how the regulations discussed herein would affect your company, please contact one of the attorneys listed above. ■

### Notes

1 See Nev. Rev. Stat. § 597.970 (2007) (*effective* Oct. 1, 2008).

2 Authorized under Mass. Gen. L. ch. 93H.