KIRKLAND ALERT
October 2008

New Laws Significantly Regulate Business Practices Relating to Personal Information

Executive Summary

Massachusetts and Nevada have recently enacted groundbreaking laws governing businesses that own, license, or possess certain personal information about individuals. These laws significantly expand a continuing legal trend of increasing regulation of — and potential liability relating to — the business use of individuals' personal information.

The new Massachusetts regulation is more sweeping than the Nevada law. The Massachusetts regulation governs any business that owns, licenses, or possesses "personal information" about Massachusetts residents. "Personal information" (which can be employee or customer information) is defined as a person's name in combination with a Social Security number, driver's license number, state ID number, or financial account, credit card, or debit card number. Note that the law is not limited to businesses with a physical presence in Massachusetts.

If a business is subject to the Massachusetts regulation, then effective January 1, 2009, the business must meet multiple detailed requirements, including: (i) adopting a written information security program that meets approximately fourteen enumerated standards and specific requirements; and (ii) implementing a computer security program that meets at least eight enumerated requirements. These requirements are summarized in more detail below, but noteworthy examples include the encryption of all personal information stored on company laptops or other portable devices, and compliance with the "need-to-collect" and "need-to-retain" limitations (*i.e.*, collecting and retaining personal information only if "reasonably necessary to accomplish legitimate purposes"). Notably, the requirements also apply to any third-party service providers that have access to the personal information.

In a similar but narrower enactment, a Nevada law (originally passed in 2005 but effective October 1, 2008) requires businesses in Nevada to use encryption to protect electronic transmissions (but not faxes) of customer personal information. The Nevada definition of "personal information" is slightly narrower than the Massachusetts definition, and the Nevada law applies only to "customers." However, the application of the Nevada law — particularly the meaning of "a business in" Nevada and the definition of "encryption" — may create compliance uncertainty.

Broader Aspects of Massachusetts Regulation

The Massachusetts regulation is significant for three additional reasons.

First, the Massachusetts regulation represents the most far-reaching and technically-detailed data security law in the United States. Although several of the Massachusetts requirements have been argued to be "best practices"

for data security, the requirements now have the force of law (to the extent a business is governed by the Massachusetts regulation).

Second, despite its specificity, the regulation also contains broad and general requirements that the legally-required information security program be "reasonably consistent with industry standards" and consistent with any other data security laws that may regulate the business. This generality may create compliance uncertainty.

Finally, the Massachusetts regulation may ultimately become a *de facto* nationwide legal standard. This is because several other states are currently evaluating similar legislation, and also because many companies possess information about Massachusetts residents. As an increasing number of companies comply with the regulation, parties seeking to impose liability for data security incidents will argue that the business practices prompted by the Massachusetts law should constitute the reasonable standard of care. In this regard, even companies not directly subject to the Massachusetts regulation may want evaluate the law and consider potential pro-active steps.

Additional Background Regarding the Massachusetts Regulation

The following is a general overview of certain requirements imposed by the Massachusetts regulation. This overview is not a comprehensive list of the requirements.

I. Written Information Security Program

With respect to written information security programs, a business must at least undertake the following:

- develop, implement, maintain and monitor a program that protects any record — written or electronic — that contains personal information;
- create a program reasonably consistent with industry standards;
- identify and assess reasonably foreseeable internal and external risks;
- develop policies for the possession of personal information by employees outside of business premises;
- contractually require, and take steps to verify, compliance by third-party service providers, including obtaining a written compliance certification;
- limit the amount of personal information collected, and the duration for which it is retained, to that reasonably necessary to accomplish legitimate purposes;
- document responsive actions relating to any breach of security, and conduct post-incident review; and
- impose disciplinary measures for violations of the program.

II. Computer System Security Requirements

With respect to the computer system security requirements, a business must at least:

- implement five different user authentication protocols, and access control measures meeting two standards;
- to the extent technically feasible, encrypt all files (containing personal information) that will travel across public networks;
- encrypt all personal information stored on laptops or other portable devices; and
- use "reasonably up-to-date" firewalls, operating system patches, malware protection, and other security software.

Conclusion and Recommendations

We recommend that companies evaluate whether these new laws apply to company operations and, if so, update relevant policies, procedures, and technologies. If the laws do not technically apply, we generally recommend being aware of these laws and their requirements for purposes of staying current on potential industry standards and/or best practices.

Members of the Kirkland & Ellis Data Security and Privacy practice routinely counsel clients on matters relating to the security of sensitive corporate and personal information. Seth Traxler, together with litigator Tom Clare, also assist clients facing regulatory, litigation, and media challenges arising from data security breaches. Should you have any questions about the matters addressed in this Alert, please contact the following Kirkland & Ellis authors or the Kirkland & Ellis attorney you normally contact:

Seth Traxler
Kirkland & Ellis LLP
200 E. Randolph Dr.
Chicago, IL 60601
straxler@kirkland.com
+1 (312) 861-2241

Thomas A. Clare
Kirkland & Ellis LLP
655 Fifteenth Street, N.W.
Washington, D.C. 20005
tclare@kirkland.com
+1 (202) 879-5993