

February 2009

## New Data Encryption Laws and Regulations Require Compliance

In recent years data security and privacy have become increasingly important to businesses large and small. Along with increased threats to the security of personal information have come calls by lawyers for companies to implement effective data security policies. These admonitions do not merely constitute good practice, as the implementation of data security practices and data security policies is now required in an increasing number of states.

New laws, rules and regulations intended to increase the security of personal information have now been enacted in two states. In late 2008, two states (Massachusetts and Nevada) passed or promulgated sweeping new legal requirements in this area pertaining to the encryption of personal information. Other states and the federal government are expected also to legislate or regulate in this area. As a result, all businesses should understand fully the importance of these new legal requirements and take steps to comply with them either because the new laws or regulations apply directly, or because the concepts contained in these new laws or regulations will likely become applicable in one form or another.

Some of these new requirements are technical, requiring businesses to implement technological measures to protect personal information stored or transmitted by them. Others are legal requirements requiring businesses to prepare and implement new types of data security and privacy policies. Whether your business operates in, or has customers or employees in, Massachusetts or Nevada, the new laws and regulations may apply. Similar laws in other states are soon to follow. As a result, staying ahead of the curve in this area is vitally important to any business.

In this *Client Alert* we summarize the new laws and regulations passed or promulgated in Massachusetts and Nevada. While an exhaustive recitation of the regulations would be outside the scope of this *Alert*, we hope that this provides a useful overview.

### CONTACT INFO:

#### Cleveland Office

Michael D. Stovsky  
Chair, Intellectual  
Property &  
Technology Group  
216.583.7136  
mstovsky@ulmer.com

1660 West 2nd St.  
Suite 1100  
Cleveland, Ohio  
44113-1448  
firm 216.583.7000  
fax 216.583.7001

[www.ulmer.com](http://www.ulmer.com)

## MASSACHUSETTS

### Introduction

In September 2008, Massachusetts promulgated new regulations which require companies that store or transmit personal information about Massachusetts residents to encrypt the information while stored and while transmitted. These regulations were released by the Massachusetts Office of Consumer Affairs and Business Regulation and were intended to take effect on January 1, 2009. This date has since been extended to May 1, 2009. These regulations essentially require businesses to encrypt all personal information that is stored on portable devices. The regulations apply to all businesses that possess personal information about a Massachusetts resident even if the business is not located in Massachusetts.

**Personal Information**

What is defined as "personal information"? Essentially, personal information includes a combination of a person's name and one or more of the following: social security number, driver's license number, credit or debit card account number or other financial account number. Personal information does not include that which is lawfully obtained from publicly available data or from federal, state or local government records lawfully made available to the public.

Under the regulations, a business that stores or transmits electronic records (e.g., email) containing personal information must encrypt the personal information in several circumstances. First, personal information that is stored by the business must be encrypted if it is stored on a portable device such as a laptop computer. Most of the commentary that we have reviewed assumes that "portable device" includes PDAs and Blackberries, cell phones, iPods, MP3 players, portable hard drives, memory cards and others.

Second, a business that transmits personal information must encrypt the information transmitted if it will be sent wirelessly (e.g., Wi-Fi, Wi-Max, cellular or other similar networks) or via public networks (e.g., the Internet). Again, most of the commentary that we have reviewed assumes that wireless transmission includes transmission within an intranet or other corporate computer or telecommunications network.

**Encryption**

Under the regulations, the term "encryption" is defined generally without reference to a particular technology or strength. The definition does, however, state that the data must be transformed using an encryption algorithm or some other equally secure method so that the meaning of the information cannot be assigned without using a confidential process or encryption key. The regulations do not mandate that a particular process be used, only that the data be transformed and its meaning not be assignable except as mentioned above.

Under the regulations, businesses that possess personal information about Massachusetts residents must ensure that third parties that have access to the personal information also encrypt it. The regulations also require that businesses that possess personal information take reasonable steps to control access to the personal information by end-users, and protect any authentication information that could be used to gain access to the personal information.

**Other Requirements**

The regulations include a comprehensive set of criteria pursuant to which the written information security programs will be judged, and include a comprehensive list of



elements which must be included in written information security programs. A full recitation of these requirements is outside of the scope of this *Alert*, but can be provided upon request and should be reviewed in detail in connection with the preparation and implementation of the mandatory information security program.

### **Potential Penalties**

Penalties for failure to comply with the regulations could include enforcement actions by the Attorney General of Massachusetts. There is also a substantial risk that failure to comply would give rise to private actions for damages and equitable relief under other legal theories as applicable.

## **NEVADA**

### **Introduction**

As of October 1, 2008, the State of Nevada enacted legislation which requires that a business in the State of Nevada shall not transfer any personal information of a customer through an electronic transmission other than a fax to a person outside of the secure system of the business unless the business uses encryption to ensure the security of the electronic transmission.

### **Personal Information**

Nevada defines "personal information" as a person's name together with a social security number, a driver's license number, or a financial account number plus a PIN or other code to gain access to the account. Significantly, the encryption of personal information is not limited to personal information about Nevada residents. The law requires that all businesses operating in Nevada encrypt all personal information about their customers when they send it electronically, other than by fax.

### **Encryption**

Nevada defines encryption broadly to mean "any protective or disruptive measure, including, without limitation, cryptography, enciphering, encoding or a computer contaminant, to prevent access, make the information unusable or disrupt the use of the network.

All businesses that operate in Nevada must encrypt all customers' personal information when they send it electronically, other than by fax. Unfortunately, the law does not define what it means to "do business in Nevada." However, case law on this point suggests that a determination of whether a business is doing business in Nevada includes an analysis of the nature of the company's business in Nevada and the quantity of business conducted in Nevada. Inquiries of Nevada authorities yielded no



determination or guidance as to whether being incorporated in Nevada constitutes doing business in Nevada for purposes of this law.

### **Other Requirements**

The encryption regulations do not require additional written plans or measures; however, other laws such as Nevada's data breach law may apply if personal data of any Nevada citizens whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

### **Potential Penalties**

While specific penalties under the Nevada data encryption law are unclear at present, many commentators currently agree that if a business fails to comply and a customer's data is intercepted and misused, there is a substantial risk that the business may face consumer protection, or negligence and other tort claims.

