

Celebrating 25 years of dedicated service to clients in the communications industries.

To: All Clients

October 1, 2008

**EFFECTIVE OCTOBER 1, 2008, NEVADA STATE LAW REQUIRES
ENCRYPTION OF THE TRANSMISSION OF SENSITIVE DATA**

A Nevada state law goes into effect today requiring that businesses in the state that engage in the electronic transmission of certain “personal information” encrypt such transmissions to protect the security of such data.

The law does not identify whether these requirements apply only to those businesses headquartered in the state, or whether they also apply to non-Nevada businesses that communicate with residents within the state. Therefore, if you conduct any business—even on a limited basis—within the state of Nevada, we recommend that you comply with these statutory requirements.

The law protects a customer’s sensitive data and defines the term “personal information” as:

A natural person’s first name or first initial and last name in combination with such person’s: a) social security number; b) driver’s license number or identification number; or c) account number, credit card number or debit card number, in combination with any required security code, access code or password that would permit access to the person’s financial account.

The term does not include the last four digits of a social security number or publicly available personal information that is lawfully made available to the general public.

The law requires encryption standards that employ any protective or disruptive measure, including, without limitation, cryptography, enciphering, encoding or a computer contaminant that:

1. prevents, impedes, delays or disrupts access to any data, information, image, program, signal or sound;
2. causes or makes any data, information, image, program, signal or sound unintelligible or unusable; or
3. prevents, impedes, delays or disrupts the normal operation or use of any component, device, equipment, system or network.

If you operate in the State of Nevada and collect “personal information” from customers or send such information either through your website or via email, you should make sure to employ encryption software to protect the transmission of such information and to comply with the requirements listed

above. Many software companies offer such encryption programs.

The law excludes fax transmissions from these encryption requirements, but it is unclear how it would apply to electronic faxes transmitted via email. Therefore we recommend that such information be encrypted in the same manner as other digital transmissions of “personal information.”

The statute is silent with respect to the potential criminal or civil penalties that could be imposed for failure to comply. Therefore, courts may interpret the law broadly, with varying outcomes.

This new law accompanies Nevada’s security breach notification law, which became effective January 1, 2007. Nevada is one of forty-two states, plus the District of Columbia, that have enacted security breach notification laws.

Should you have any questions about the requirements of this law, please contact S. Jenell Trigg (strigg@lsl-law.com) or Katrina Gleber (kgleber@lsl-law.com) in our office.

Leventhal Senter & Lerman PLLC