Legal Updates & News

Bulletins

Nevada Law Mandates Encryption of Electronically-Transmitted Personal Information

October 2007
by Marian A. Waldmann

Privacy Bulletin, October 2, 2007

Even though a company has not experienced an unauthorized access or acquisition of its customer information (and thus has not been subject to Nevada's breach notification law), in 2008 merely transmitting customer information in an unencrypted format may violate a separate Nevada data security law.

Nevada has enacted a data security law that mandates encryption for the transmission of personal information (*see* Nev. Rev. Stat. § 597.970 (2005)). Specifically, the Nevada encryption statute generally prohibits a business in Nevada from transferring "any personal information of a customer through an electronic transmission," except via facsimile, "unless the business uses encryption to ensure the security of electronic transmission."[1] The Nevada encryption law goes into effect on **October 1, 2008**.

Summary of the Nevada Law

The "personal information" covered by the Nevada encryption law is the same information that is subject to that state's security breach notification law, namely: "a natural person's first name or first initial and last name in combination with any of the following: (a) social security number or employer identification number; (b) driver's license number or identification card 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 Nevada encryption law does not define a "customer." Because neither the "personal information" nor the "customer" covered by the Nevada encryption law is limited with respect to a Nevada resident, the law could be interpreted as applying to a covered entity's transmission of "any personal information of a customer," regardless of where the customer resides.

The Nevada encryption law does not define the scope of "[a] business in this state" that is subject to the law. However, in addressing whether a foreign corporation had satisfied qualification requirements under Nevada law, the Nevada Supreme Court interpreted "doing business" in Nevada by approvingly citing a two-pronged standard: (a) the nature of the company's business in the state; and (b) the quantity of business conducted by the company in the state. In that case, the Court noted that assessing whether a foreign company is "doing business" in the state is "often a laborious, fact-intensive inquiry resolved on a case-by-case basis."[2] Moreover, the prohibition under the Nevada law is limited to transmission of personal information "to a person outside of the secure system of the business."

The new law does not include any specific penalty provisions, making it unclear what types of sanctions may be imposed on companies for violations. While the section falls under the Miscellaneous Trade Regulations and Prohibited Acts Chapter, the chapter also does not carry any generally applicable penalty provisions.

The Nevada Encryption Law In Light of General Data Security Obligations

The Nevada encryption law is not alone in mandating data security measures for personal information and companies subject to the Nevada law should take steps to develop compliance procedures that are consistent with general data security obligations under other state laws. For example, the California Security Safeguard

Act[3] applies to a company that owns or licenses unencrypted "personal information" about California residents and, in general, requires the company to implement and maintain "reasonable security procedures and practices" to protect such data. Texas and Rhode Island[4] have enacted similar laws requiring companies to adopt procedures relating to information security. In this context, the Nevada encryption law is unique in mandating the use of a particular security measure, rather than "reasonable" security procedure, but this may signal the beginning of a trend.

Companies that do business on a nationwide basis, which are already required to have an information security policy that complies with the laws of several states, should employ standards that do not leave them inadvertently out of compliance with this new Nevada law.

---

[1] Nev. Rev. Stat. § 597.970 (2005).

[2] Executive Mgmt. Ltd. v. Ticor Title Ins. Co., 38 P. 3d 872 (Nev. 2002).

[3] Cal. Civ. Code § 1798.81.5(b).

[4] R.I. Gen. Laws § 11-49.2-2(2) (2006); Tex. Bus. & Com. Code § 48.102(a) (2006).