MORRISON | FOERSTER

Legal Updates & News

Bulletins

Nevada Requires Encryption of Personal Information in Transit and in Storage on Portable Devices

June 2009
by Vanessa R. Waldref, Nathan D. Taylor, Charles H. Kennedy

Related Practices:

- Privacy and Data Security

Nevada Requires Encryption of Personal Information in Transit and in Storage on Portable Devices

In 2005, Nevada enacted a data security law that required businesses to encrypt customer personal information before electronically transmitting it outside of an internal secured network.[1]

Nevada recently amended this law to also cover personal information not related to customers, and to require data collectors that conduct business in the state to encrypt data storage devices containing personal information that they move outside the secured physical and logical boundaries of the entity.[2] Data storage devices include, among other things, computers, cellular phones, and thumb drives. The amended Nevada encryption law goes into effect **January 1, 2010**.

New Amendments Expand Encryption Requirements

Nevada's first encryption law was adopted at the same time as the state's data breach notification law, which requires businesses to alert Nevada residents to the unauthorized access or acquisition of their personal information.[3] The 2005 legislation required the encryption of all customer personal information transferred electronically outside of the secure system of a business, with the exception of fax transmissions.[4]

The new law expands the original encryption requirement to both customer and non-customer personal information, and also requires encryption of all personal information that is transferred "beyond the logical or physical controls" of a business or its data storage provider on any data storage device. The amended statute also extends encryption obligations to all "data collectors" doing business in the state, a category that includes governmental agencies, institutions of higher learning, corporations, financial institutions, retail operators, or "any other type of business entity or association" that deals with non-public personal information.

Additionally, these amendments include a technical standard for encryption that was absent in the original statute, and requires businesses that accept credit or debit cards to meet the Payment Card Industry Data Security Standard.

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

The new law defines a "data storage device" as "any device that stores information or data from any electronic or optical medium, including, but not limited to, computers, cellular telephones, magnetic tape, electronic computer drives and optical computer drives, and the medium itself." Data collectors in Nevada should note that the definition of data storage device is expansive, and is not limited to portable devices, such as laptops and blackberries. The encryption requirements also apply to CDs, DVDs, desktop computers, and servers that contain personal information that are, for example, moved to another office location.

Putting these provisions together, data collectors that do business in Nevada must use encryption for: (1) all electronic transmissions of personal information, except faxes, outside the secure system of the data collector; and (2) any movement of a data storage device containing personal information outside the confines of the workplace of the data collector or its data storage contractor.

Nothing in the Nevada statute limits its application to personal information of Nevada residents that is transmitted or stored by a data collector. Accordingly, the Nevada encryption law could be interpreted as applying to a covered entity's transmission or storage on a portable device of any personal information, regardless of where the subject of that information resides.

Also, the Nevada encryption law does not define the scope of a "data collector doing business in this State." However, in addressing whether a foreign corporation had satisfied qualification requirements under Nevada law, the Nevada Supreme Court interpreted "doing business" in Nevada by adopting 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."[5]

Encryption Standard

Under the new law, data collectors seeking to comply with the encryption requirement for either electronically transmitted personal information or information transferred on a storage device must use encryption that meets a certain standard. Specifically, data collectors must use an encryption technology "that has been adopted by an established standards setting body, including, but not limited to, the Federal Information Processing Standards issued by the National Institute of Standards and Technology, which renders such data indecipherable in the absence of associated cryptographic keys necessary to enable decryption of such data." Data collectors must also use established standards to ensure "appropriate management and safeguards of cryptographic keys to protect the integrity of the encryption."

The amended law will provide a damages liability safe harbor for covered entities that meet the data encryption requirements for the electronic or data storage device transfer of personal information. This safe harbor, however, will not apply for businesses that face a data breach resulting from gross negligence or intentional misconduct.

Businesses That Accept Credit Cards Must Comply with Industry Standards

The new law requires that data collectors doing business in Nevada that accept credit or debit card payments for goods or services must comply with the Payment Card Industry Data Security Standard. This Standard is a set of industry self-regulatory data security standards for merchants and other businesses that accept credit card and debit cards as payment, and merchant banks and other financial services businesses that process payment card transactions.

Unless a business engages in gross negligence or intentional misconduct, the new law will provide a safe harbor

from damages liability for security breaches if a covered business complies with the Payment Card Industry Data Security Standard.

On its face, the new law appears to provide that data collectors that accept credit cards or debit cards as payment are only required to comply with the Payment Card Industry Data Security Standard and not the Nevada encryption requirements. Specifically, the statute provides that the encryption requirements only apply to data collectors to whom the Payment Card Industry Data Security Standard do not apply. It is not clear whether the Nevada legislature intended such a result. The more likely intent may have been that data collectors that accept credit or debit card payments must comply with the encryption standards with respect to personal information to which the Payment Card Industry Data Security Standard would not otherwise apply, including, for example, employee personal information and non-payment card financial information.

New Trends in Data Security Measures

Many state laws, like a number of federal statutes and regulations, mandate that businesses take reasonable data security measures to safeguard personal information. For example, the California Security Safeguard Act[6] 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[7] have enacted similar laws requiring companies to adopt procedures relating to information security. Only Nevada and Massachusetts specifically mandate the use of encryption to protect personal information.

As states respond to an increasing public concern about the safety of personal information and the threat of identity theft, Nevada's encryption requirements may signal a new trend. Companies subject to the Nevada law should take steps to develop compliance procedures that meet the new encryption requirements and that are also consistent with general data security obligations mandated under federal law and the laws of other states.

---

[1] Nev. Rev. Stat. § 597.970 (2005).

[2]Nevada Senate Bill 227, which is available here.

[3] Nev. Rev. Stat. § 603A et seq.

[4] The new law maintains this "fax" exception and defines "facsimile" as "an electronic transmission between two dedicated fax machines using Group 3 or Group 4 digital formats that conform to the International Telecommunications Union T.4 or T.38 standards or computer modems that conform to the International Telecommunications Union T.31 or T.32 standards."

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

[6] Cal. Civ. Code § 1789.81.5(b).

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