

Revised Nevada Privacy Law Furthers Encryption and Payment Card Law Trends

Melissa J. Krasnow, Dorsey & Whitney LLP

Nevada was the first state to enact a law requiring a company that transfers customer personal information outside of its secure system through an electronic transmission (other than a facsimile) to use encryption.¹ This law continues in effect until January 1, 2010. This law was amended and the effective date for the amended law is January 1, 2010.² Interestingly, other privacy laws (examples include the Massachusetts written information security program law and the Federal Trade Commission's Red Flags Rule) also were amended during the past year.³ The amended Nevada law is notable for many reasons. The amended law continues the trend of two newer types of state privacy laws – encryption laws and payment card laws. Massachusetts has a written information security program law that mandates the use of encryption.⁴ Minnesota was the first state to enact a payment card law.⁵ More specifically, the amended law expands coverage beyond customer personal information to all personal information. The amended law also requires compliance with the Payment Card Industry Data Security Standard.⁶ Finally, the amended law provides for relief from damages in the event of a data breach.

Application

The amended law applies to a company doing business in Nevada that deals with nonpublic personal information, except for telecommunication providers. The amended law covers a company outside of Nevada that does business in Nevada. Whether a company does business in Nevada depends on (i) the nature of the company's business in Nevada and (ii) the quantity of business conducted by the company in Nevada.⁷

The definition of “personal information” is from the Nevada data breach law and means an individual's first name or first initial and last name in combination with their (i) Social Security Number (excluding the last four digits), (ii) driver's license number or identification card number or (iii) account number, credit card number or debit card number, together with any required security code permitting access to their financial account, when both the name and the foregoing data element are not encrypted.⁸

Encryption Requirements

There are two encryption requirements under the amended law. A company that does not accept a payment card (a credit card, charge card, debit card or similar card) in connection with a sale of goods or services must use encryption (i) to transfer any personal information through an electronic, nonvoice transmission (other than a facsimile) outside the company's secure system or (ii) when a data storage device (like a computer, cell phone, magnetic tape, electronic computer drive and optical computer drive) containing personal information is moved beyond the company's physical or logical controls. However, the amended law does not apply to data transmission over a secure, private communication channel for the (A) approval or processing of negotiable instruments, electronic fund transfers or similar payment methods or (B) issuance of reports regarding account closure due to fraud, substantial overdrafts, abuse of automatic teller machines or related information regarding a customer.

“Encryption” means the protection of data in electronic or optical form, in storage or in transit, using: (i) an encryption technology that has been adopted by an established standards setting body like the Federal Information Processing Standards issued by the National Institute of Standards and Technology (NIST), that renders the data indecipherable in the absence of associated cryptographic keys necessary to enable decryption and (ii) appropriate management and safeguards of cryptographic keys to protect the integrity of the encryption using the guidelines of an established standards setting body such as the NIST.

Payment Card Requirement

A company that accepts a payment card in connection with a sale of goods or services must comply with the current version of the Payment Card Industry Data Security Standard as adopted by the PCI Security Standards Council or its successor organization (PCI DSS), not later than the date for compliance in PCI DSS or by the PCI Security Standards Council or its successor organization. PCI DSS is an industry security standard developed by the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa, Inc., with requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. PCI DSS is intended to help organizations proactively protect customer account data.

Liability for Data Breach

A company that (i) complies with the amended law and (ii) suffers a data breach that is not caused by gross negligence or intentional misconduct by the data collector, its officers, employees or agents is not liable for damages.

Conclusion

A company that must comply with the Massachusetts law and the amended Nevada law must reconcile the encryption requirements under these laws. The amended Nevada law is effective January 1, 2010, and the Massachusetts law is effective March 1, 2010. The Massachusetts law requires a company to establish a comprehensive written information security program that contains the encryption requirements, so a company needs to revisit these requirements in light of the encryption requirements under the amended Nevada law. Further, a company that must comply with the Minnesota law and the amended Nevada law must address the payment card requirements of both laws. A company that is subject to the payment card requirement under the amended Nevada law needs to determine the requirements for compliance with PCI DSS.

Melissa J. Krasnow is a partner in the Corporate Group of Dorsey & Whitney LLP.

¹ NRS 597.970.

² Nev. S.B. No. 227.

³ 201 CMR 17.00 et seq. and 16 C.F.R. § 681.1.

⁴ 201 CMR 17.00 et seq.

⁵ Minn. Stat. § 325E.64.

⁶ PCI Security Standards Council, <http://www.pcisecuritystandards.org> (last visited Aug. 11, 2009).

⁷ *Executive Management, Ltd. v. Ticor Title Insurance Co.*, 38 P.3d 872 (Nev. 2002).

⁸ NRS 603A.040.