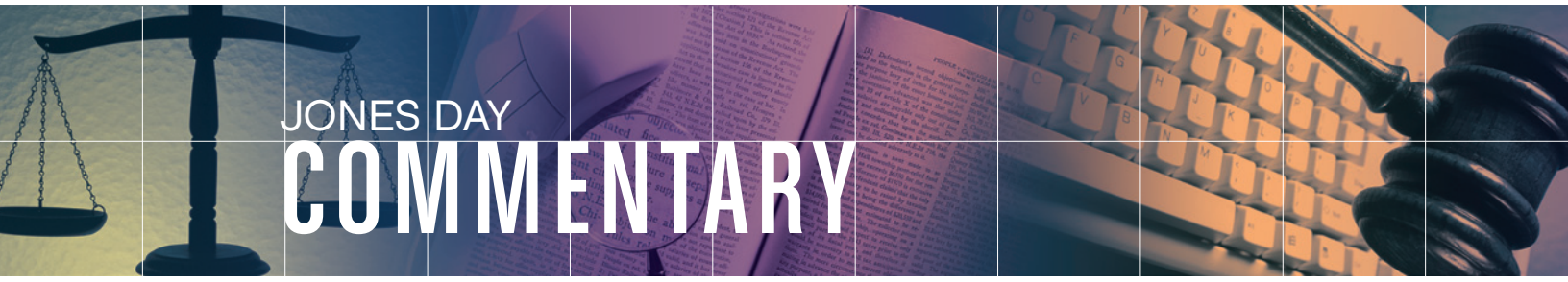
JULY 2009



NEVADA IMPOSES NEW REQUIREMENTS FOR CREDIT CARD TRANSACTIONS AND DATA TRANSFERS

Nevada recently amended its law on the Security of Personal Information[1] to require Nevada businesses to comply with the Payment Card Industry Data Security Standards ("PCI DSS") in any transaction where the business accepts a credit card (or other payment card) for the sale of goods or services, and to require Nevada businesses to encrypt any personal information the business transfers. Nevada's recent amendment, S.B. 227,[2] will take effect January 1, 2010, and will considerably broaden the information security obligations of companies "doing business" within the state's borders. Moreover, by incorporating and referencing various industry standards, the state's new law could be a precursor to similar state laws that may mandate higher standards for privacy and data security, much as California's data protection statute caused a wave of data breach notification laws throughout the country.

PCI DSS is a set of principles adopted by the PCI Security Standards Council, a consortium of major credit card companies, and organized around a group of six principles with 12 accompanying requirements.[3] Businesses accepting credit card payments are likely already bound by contract to comply with PCI DSS. Despite such existing contractual obligations (which often exist within a complex web of contractual relationships among the merchant or other business accepting credit card payment, the consumer, the issuing credit card company, the payment processor, and others), Nevada's S.B. 227 turns PCI DSS compliance into a mandatory statutory obligation with associated penalties for noncompliance beyond what may be imposed for breach of contract. Subsection 1 of S.B. 227 requires all companies doing business in Nevada that accept "a payment card in connection with a sale of goods or services" to comply with PCI DSS and associated deadlines "with respect to those transactions."

The amendment further requires companies doing business in Nevada to encrypt any personal information transferred electronically "outside of the [business's] secure system" or when a data storage device, such as a computer, cellular telephone, computer drive or tape, etc., containing personal information is

transferred beyond the business's "logical or physical controls." This provision extends beyond credit card transactions, as Nevada's Security of Personal Information law defines personal information to include a natural person's first name or first initial and last name with (1) Social Security number, (2) driver's license or identification card number, or (3) financial account number (with security code, access code, or password).[4] S.B. 227 defines "adequate means of encryption" to include encryption technology adopted by an established standards-setting body, such as the National Institute of Standards and Technology ("NIST").[5] In addition, adequate encryption requires "[a]ppropriate management and safeguards of cryptographic keys" promulgated by an established standard-setting body, such as NIST. Companies doing business in Nevada should review their compliance programs, privacy policies, and third-party contracts to determine whether modifications are necessary for compliance with these encryption requirements. Companies should pay particular attention to policies and practices governing mobile storage devices, including laptops and thumb drives, as data security practices on these mobile devices are often lax despite the increased risk for loss or theft posed by their small size and portable nature. Although encrypting data stored on laptops, thumb drives, and other mobile storage devices may be legally sufficient, a more prudent approach would be to limit the amount of personal information stored on such devices in the first instance.

Nevada's amendment contains certain exemptions; for example, it exempts from data breach liability all businesses that comply with its requirements and do not engage in "gross negligence" or "intentional misconduct" in handling personal data. While the exact scope of the amendment remains unclear, its language suggests that the amendment covers all companies (including their third-party agents) considered to be "doing business" in Nevada that collect, store, or transfer personal information.

Like Minnesota's 2007 Plastic Card Security Act,[6] which incorporated part of the PCI DSS requirements, Nevada's S.B. 227 may set a precedent for a new round of state data protection legislation that adopts industry standards, such as PCI DSS and NIST, to strengthen their data protection laws. Other states could pass broader and more comprehensive laws that affect companies outside their borders. For example, Massachusetts requires compliance with industry standards (without referencing specific industry or technical requirements) that will affect companies collecting data from Massachusetts residents, regardless of where the company is located.[7]

Nevada's S.B. 227 and similar legislation will encourage businesses to stay current with technology and best practices as industry standards are constantly evolving. The PCI Security Standards Council has already planned a revision of PCI DSS and will accept comments from July 1 to November 1, 2009, for a new version of PCI DSS that may be released in fall 2010.[8] To comply with current and forthcoming industry standards—and state laws mandating compliance with same—companies will need to evaluate regularly their information security regimes and implement necessary updates to meet appropriate state and industry requirements.

LAWYER CONTACTS

For further information, please contact your principal Firm representative or one of the lawyers listed below. General email messages may be sent using our "Contact Us" form, which can be found at www.jonesday.com.

Kevin D. Lyles
1.614.281.3821
kdlyles@jonesday.com

Steven C. Bennett
1.212.326.3795
scbennett@jonesday.com

Mauricio F. Paez
1.212.326.7889
mfpaez@jonesday.com

Joseph J. Bernasky
1.212.326.3799
jjbernasky@jonesday.com

ENDNOTES

1. Nev. Rev. Stat. § 603A (2009).

2. S. B. 227, 2009 Leg., 75th Sess. (Nev. 2009).

3. PCI DSS's six principles and 12 accompanying requirements are:

   Build and Maintain a Secure Network

   Requirement 1: Install and maintain a firewall configuration to protect cardholder data

   Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

   Protect Cardholder Data

   Requirement 3: Protect stored cardholder data

   Requirement 4: Encrypt transmission of cardholder data across open, public networks

   Maintain a Vulnerability Management Program

   Requirement 5: Use and regularly update antivirus software

   Requirement 6: Develop and maintain secure systems and applications

   Implement Strong Access Control Measures

   Requirement 7: Restrict access to cardholder data by business need-to-know

   Requirement 8: Assign a unique ID to each person with computer access

   Requirement 9: Restrict physical access to cardholder data

   Regularly Monitor and Test Networks

   Requirement 10: Track and monitor all access to network resources and cardholder data

   Requirement 11: Regularly test security systems and processes

   Maintain an Information Security Policy

   Requirement 12: Maintain a policy that addresses information security

   See PCI Security Standards Council, *About the PCI Data Security Standard (PCI DSS)*, at https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml.

4. Nev. Rev. Stat. § 603A.040 (2009).

5. The Department of Health and Human Services has referenced NIST's encryption technology in guidelines concerning the protection of computerized health information under the Health Information Technology for Economic and Clinical Health Act.

6. H.F. 1758, 2007-2008 Leg., 85th Sess. (Minn. 2007).

7. *See* 201 Mass. Code Regs. 17 (2009), applying Mass. Gen. Laws Ann. ch. 93H (2009). The regulation's effective date has been extended to January 1, 2010, from the original date of January 1, 2009, due to concerns regarding the law's regulatory burden on businesses. Proposed S.B. 173, 2009 Leg., 186th Sess. (Mass. 2009) includes further revisions.

8. More information is available at https://www.pcisecuritystandards.org/.