HUNTON& WILLIAMS

CLIENT ALERT

June 2009

Contacts

Lisa J. Sotto
200 Park Avenue
New York, NY 10166
(212) 309-1223
lsotto@hunton.com

Elizabeth H. Johnson
One Bank of America Plaza
Suite 1400
421 Fayetteville Street
Raleigh, NC 27601
(919) 899-3073
ehjohnson@hunton.com

Rachel M. St. John
200 Park Avenue
New York, NY 10166
(212) 309-1361
rst.john@hunton.com

Additional Lawyers
Cédric Burton
Purdey Castle
Jörg Hladjk
Natalie Hunt
Christopher Kuner
Ryan P. Logan
Manuel E. Maisog
Melinda L. McLellan
Olivier Proust
Boris Segalis
Aaron P. Simpson
Bridget C. Treacy
Mason A. Weisz
John W. Woods, Jr.

Centre for Information Policy Leadership
Martin E. Abrams*
Paula J. Bruening
Fred H. Cate
Orson Swindle*

*Not a lawyer

Nevada Updates Encryption Law and Mandates PCI DSS Compliance

As of January 1, 2010, Nevada law will require businesses to use encryption when data storage devices that contain personal information are moved beyond the physical or logical controls of the business, in addition to continuing to require that personal information be encrypted if it is transferred outside the secure system of the business. The new law repeals the existing Nevada encryption law, which will remain in effect until January 1, 2010. (For more information on the existing Nevada encryption law, please see our previous Client Alert.) The new law also mandates compliance with the Payment Card Industry Data Security Standard ("PCI DSS") for businesses that accept payment cards. The law applies to organizations doing business in Nevada and provides that compliance will shield such businesses from liability for damages from a security breach.

PCI DSS Compliance

The new law codifies industry standard practice for businesses that accept payment cards. Once the law takes effect, businesses that accept payment cards in connection with a sale of goods or services will be required to comply with PCI DSS. Minnesota law currently codifies certain select PCI DSS requirements. The new Nevada law is significantly more comprehensive, however, since it adopts the PCI DSS in its entirety by reference.

Mandatory Encryption

Under the new encryption law, businesses must encrypt any personal information transferred by electronic transmission, other than a facsimile, outside the secure system of the business. Businesses are also prohibited from moving any data storage device containing personal information beyond the "logical or physical controls" of the business, or those of storage contractors, unless encrypted. A "data storage device" is 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. These requirements will not apply to businesses that accept payment cards in connection with a sale of goods or services, which are instead required by the law to comply with PCI DSS.

Required Encryption Technology

The existing Nevada encryption law provides a vague definition of "encryption" that does not delineate an established standard for encryption technology. The new law provides a more comprehensive definition that references technological industry standards. Specifically, "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, including, but not limited to, the National Institute of Standards and Technology ("NIST") that issues the Federal Information Processing Standards, which technology must render data indecipherable in the absence of associated cryptographic keys necessary to enable decryption, and (ii) appropriate management and safeguarding of cryptographic keys to protect the integrity of encryption using guidelines promulgated by an established standards-setting body including, but not limited to, the NIST. NIST encryption standards are also referenced by the Department of Health and Human Services ("HHS") in its information security guidance on methodologies that render protected health information unusable, unreadable or indecipherable to unauthorized individuals for purposes of breach notification under the Health Information Technology for Economic and Clinical Health (HITECH) Act. Our analysis of the HHS guidance is available here. The adoption of the HHS guidance, closely followed by enactment of this Nevada law, marks a trend toward established standards for encryption technology.

Interestingly, Nevada's new definition of encryption applies only to the specific provisions described above. This limited application creates a dichotomy (perhaps unintended) between the new provisions and Nevada's definition of "personal information," which applies to both the new provisions and existing provisions, such as Nevada's breach notification requirements. That definition provides that personal information means "a natural person's first name or first initial and last name in combination with specified data elements, when the name and data elements *are not encrypted*" (emphasis added). For purposes of this provision, Nevada does not require that encryption meet standards specified by an established standards-setting body. This outcome seems to indicate that data, such as a name plus a Social Security number, if encrypted to any standard, would not constitute personal information and, therefore, would not be subject to the more stringent encryption requirements specified by the new Nevada law. In short, the new, stricter standards would appear to be rendered inapplicable if data that would otherwise constitute personal information were encrypted to some lower standard.

Liability for Security Breach Damages

A business that complies with the new Nevada law is not liable for damages resulting from a security breach, provided that the security breach is not caused by the gross negligence or intentional misconduct of the business, its officers, employees or agents. The effect of the law is to create a potential safe harbor against liability for damages resulting from a security breach.

We Can Help

A number of states require business to implement information security measures, although Nevada is the first to require full PCI DSS compliance. Hunton & Williams' Privacy and Information Management practice assists clients in developing, implementing and evaluating privacy and information security programs to comply with federal and state requirements. If you would like assistance reviewing your organization's privacy or data security practices, or developing new policies or training programs, please contact us.

Visit the Privacy and Information Security Law Blog at www.huntonprivacyblog.com for global privacy and information security law updates and analysis.