How New State Encryption Laws Will Affect Your Business

by David J. Leffler, Esq.

Nevada and Massachusetts have recently passed legislation mandating the encryption of personal information transmitted electronically. So far, Nevada and Massachusetts are the only two states to mandate particular security measures required to protect personal information, however, other states, such as Michigan and Washington, are also considering similar regulations. The Massachusetts law is not limited to activities within it borders, but instead applies to any party handling personal information of its residents.

Massachusetts

A newly enacted law in Massachusetts requires all companies that own, license, store or maintain personal information concerning any Massachusetts resident take comprehensive measures to protect that information contained in paper or electronic records held in its possession from unauthorized access, disclosure or misuse. See, 201 Mass. Code Regs. 17.01 - 17.04 (2008). The new regulation establishes the minimum standard for entities maintaining private information of Massachusetts residents and codifies many elements that are currently the best practice with respect to data security. The deadline for compliance with this law has been set in two stages. The compliance date for encryption of laptops and data sent over public networks and wireless systems has been set for May 1, 2009, whereas the compliance deadline for encrypting non-laptop portable devices, such as PDAs, memory sticks and DVDs, and obtaining compliance certifications from vendors that have access to personal information of Massachusetts residents is set for January 1, 2010.

The most pressing compliance issue is the obligation to encrypt all personal information of Massachusetts residents stored on a laptop, or other portable device, that is transmitted over public networks, like the Internet. Further, it should be noted that the law applies to all parties handling personal information of Massachusetts residents, and therefore, the new law will affect out of state businesses, as well as Massachusetts's domestic entities. Moreover, the regulation requires more than just the encryption of consumer's private information. There are significant requirements for risk assessment, maintaining security programs, training personnel and reviewing relationships with other service providers and vendors that have access to the personal information of Massachusetts residents.

The new Massachusetts law includes sanctions and penalties in the event of a violation. Though there is no private right of action, the Massachusetts Attorney General may bring an action against a person or entity and civil penalties, such as fines, costs and attorneys fees may be granted as relief.

Nevada

Effective October 1, 2008, a new data security law mandates encryption for the transmission of personal information. Specifically, the Nevada encryption statute generally prohibits a business in Nevada from transferring "any personal information of a customer through an electronic transmission, other than facsimile, to a person outside of the secure system of business unless the business uses encryption to ensure the security of electronic transmission." See, Nev. Rev. Stat. § 597.970 (2005). Mandatory encryption is required regardless of whether

or not the business has experienced a breach of security, and it is unclear what penalties or sanctions may apply in the event of a violation.

Personal information under the law is defined as "a 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." NRS, § 603A.040. Personal information does not include the last four digits of a social security number or any information that is lawfully made available to the general public. Id.

The Nevada law, however, does not define "customer," so it is unknown whether the encryption requirement applies only to Nevada residents or to all customers regardless of residence. Further, since the law also neglects to define "[a] business within this state," it is unknown whether the encryption regulation is only required of domestic entities or also of foreign entities doing business in Nevada. A Nevada Supreme Court case suggests that this will be determined on a case-by-case basis and may incorporate foreign businesses depending on the nature and quantity of the business within the state.

Conclusion

The evolution of data security laws, and specifically the complexity of the Massachusetts regulation, requires businesses to review their current data security procedures and possibly update their information protection policies.

David J. Leffler can be reached at dleffler@lmmlawfirm.com