Proskauer

A Moment of Privacy

September 2008

Welcome to “A Moment of Privacy,” a newsletter brought to you by the Privacy and Data Security Practice Group at Proskauer Rose LLP.

“A Moment of Privacy” addresses one legal development each month in the area of privacy and data security law. We answer the questions our clients are asking, in a way that we hope gives practical information to our readers. If you send us your question, you may find your answer in an upcoming newsletter.

And now for this month’s question:

Q: I understand that Massachusetts’ new information security rule reaches beyond what other states require. What do these new rules mean for my company?

A: If your company “owns, licenses, stores or maintains” personal information about Massachusetts residents, then MA’s new rules impose specific information security requirements onto your company that may require it to increase its standard of care.

Massachusetts’ new rule covers “personal information” of both consumers and employees, defined as a Massachusetts resident’s name in combination with his or her Social Security number, driver’s license or state ID card number, or financial account or credit or debit card number that would permit access to the resident’s financial account. The rule applies to both paper and electronic records, but does not apply to publicly available information.

Covered entities must develop, implement, maintain, and monitor a comprehensive written information security program that is reasonably consistent with industry standards and that contains administrative, technical and physical safeguards to ensure the security and confidentiality of records that contain personal information. The safeguards must be consistent with any safeguards required by other federal and state regulations to which the entity is subject. Programs must include:

- Designation of employee(s) responsible for program

- Identifying and assessing risks; evaluating and improving current safeguards; training; employee compliance; and detection of failures
- Policies for whether and how employees can keep, access, and transport personal information off premises
- Disciplinary measures for employee violations
- Discontinuing access by terminated employees
- Management of service providers
- Limiting collection and retention of personal information to that which is necessary for a legitimate purpose; “need-to-know” access to personal information
- Inventorying records that contain personal information
- Management of physical access to personal information
- Regular monitoring and upgrading of safeguards
- Review of program annually or whenever there is a relevant material change in business practices
- Documenting incident response; post incident review of program

Entities that electronically store or transmit personal information also must include in their program:

- Establishment and maintenance of a security system covering its computers and wireless systems, including secure user authentication protocols, secure access control measures, encryption (under certain circumstances), monitoring, firewalls, operating system patches, up-to-date security system software, and education and training

Whether an entity’s program is compliant will be evaluated based on the size, scope and type of business of the entity, how much resources the entity has, how much data it stores, and the need for security and confidentiality of the information.

Coincident with the promulgation of this rule, the Governor of Massachusetts also signed an executive order requiring Massachusetts state agencies to implement security measures consistent with the requirements imposed by the rules onto private companies.

Massachusetts’ new rule will become effective January 1, 2009.

For information about Nevada's similar law which will become effective onOctober 1, 2008, see Proskauer's Privacy Law Blog at http://privacylaw.proskauer.com/2008/09/articles/data-privacy-laws/leaving-las-vegas-if-encrypted/.

*201 CMR 17.00 “Standards for The Protection of Personal Information of Residents of the Commonwealth” [http://www.mass.gov/?pageID=ocaterminal&L=3&L0=Home&L1=Business&L2=Identity+

(Rule promulgated pursuant to M.G.L. c. 93H [http://www.mass.gov/legis/laws/seslaw07/sl070082.htm])

Have a question? E-mail Kristen J. Mathews at kmathews@proskauer.com.

Related Professionals

- **Jeffrey D. Neuburger**
  Partner
- **Anthony J. Oncidi**
  Partner