Hughes Hubbard & Reed

Yet Another Data Security Bill Introduced

Client Advisories

Hughes Hubbard & Reed LLP • A New York Limited Liability Partnership
One Battery Park Plaza • New York, New York 10004-1482 • +1 (212) 837-6000

The march towards the establishment of some sort of national standards on data security and breach notification continued last week with the introduction in the Senate of yet another piece of legislation. This one, descriptively titled the Data Security and Breach Notification Act of 2012, would not only set benchmarks for companies to comply with but would also expressly preempt any state law or regulation on data protection and security and notification to affected individuals in case of a breach, even if such state law provides greater protection to consumers. The newly-proposed bill, if enacted would require covered commercial entities–defined as any entity which "acquires, maintains or utilizes personal information"–to take "reasonable measures" to protect and secure the personal information that they hold. In the event of a security breach the covered entity "reasonably believes" has caused or will cause identity theft or other financial harm, affected consumers must be notified "as expeditiously as practicable and without reasonable delay". The bill also requires companies to notify the Secret Service of the FBI of the breach if it affects more than 10,000 individuals. All-in-all, these are fairly loose standards, providing businesses with a great deal of discretion in implementing security protocols and procedures and determining whether or not notification is necessary. In contrast, the Obama administration's proposal from last year required companies to notify affected consumers within 60 days of the discovery of the loss or theft of personally identifiable information, regardless of whether or not actual identity theft or financial harm was likely. The bill also would expressly prohibited a private cause of action for security breaches (a right that was included in a competing proposal made by Connecticut Senator Richard Blumenthal last year). A violation of the bill's provisions would be deemed an unfair or deceptive practice in violation of the Federal Trade Commission Act punishable by a civil penalty of up to $500,000 per incident. Currently 46 states have implemented data security and protection laws or regulations, in many cases establishing much more stringent standards than those contained in the bills proposed in the Senate. Proponents of a national standard have argued that businesses have a tremendous burden complying with this patchwork of rules and regulations. While privacy advocates would likely not argue with that premise, their concern is that any national standard should be mirrored on the most comprehensive and stringent state standard currently in place. This latest bill obviously reignites the discussion on data security standards, a discussion we've written about here, here and here. However, it is unlikely that the establishment of a national standard is around the corner, particularly in this election year. But even without a national standard, it is important for entities collecting and utilizing consumer data to be keenly

aware of the various state and local rules and regulations that are applicable to its operations, and to establish and maintain best practices in its collection, use and security initiatives.

Related Areas of Focus

Media, Technology & Commercial Transactions