Dickie McCamey
ATTORNEYS AT LAW

2/24/2017 | Articles

New York Rolls Out New Cybersecurity Requirements For Banks, Insurers

According to the New York Department of Financial Services ("DFS"), new cybersecurity rules aimed at safeguarding consumer data go into effect on March 1, 2017. The regulations will require banks, insurers, and money services to strengthen their cybersecurity protocols by, in part, putting data security programs in place and accepting greater responsibility for monitoring the vendors with whom they do business. The rules also require reporting breaches within 72 hours.

The new rules impose obligations which could create liability from regulatory actions or consumer litigation. According to attorneys quoted in a recent article appearing on *Law360.com,* the new guidelines will give enterprising plaintiffs' lawyers new claims against financial services firms, as well as firm directors and officers.

Under the new DFS scheme, company executives must certify compliance with the NY DFS regulations on an annual basis. Should those certifications prove incorrect, they could provide the basis for the DFS or consumers to make claims against banks, insurers, and other financial services firms for breach of such certification. Because of that, companies should devote considerable attention and resources to two areas: 1) implementation of cybersecurity programs and systems in compliance with DFS requirements; and 2) making sure company executives have liability insurance coverage for cyber-related missteps, including coverage for both regulatory and consumer claims.

With respect to adequately insuring cyber exposures, companies should undertake review of D&O policies to make sure any cyber-related liability is not excluded, and also that the insurance will cover the costs of defending against regulatory actions and any resulting penalties.

With respect to DFS requirements for the supervision of third-party vendors, the rules call for vendors to encrypt nonpublic information and to set up robust protection systems. Companies should require and review both vendor cybersecurity policies and related liability insurance products to make sure the vendors have technology errors and omissions coverage. Companies may wish to secure additional insured protection in such policies as well.

A copy of the regulations can be read by clicking here.

Charles E. Haddick, Jr.
717-731-4800
chaddick@dmclaw.com
@cjhinsurancelaw
blog: badfaithadvisor.com