Winget | Spadafora | Schwartzberg | LLP

NY | NJ | CT | FL | CA | TX | IL | CO

www.WSSLLP.com

Winget, Spadafora & Schwartzberg, LLP - Client Alert

www.WSSLLP.com

About Us

Offices

Practice Areas

News & Events

Cybersecurity Requirements – First New York, is Colorado Next?

April 17, 2017

Getting in Cyber Shape is taking off in the United States. New York's groundbreaking Cybersecurity Regulations are well underway with the first deadline to be satisfied by September 2017. New York State Department of Financial Services Superintendent Maria T. Vullo is actively encouraging states to adopt Regulations similar to New York's March 1, 2017 Cybersecurity Regulations. Colorado's Department of Regulatory Agencies, Division of Security recently published a notice about proposed guidance for Broker-Dealers and Investment Advisors. As stated in the Notice of Proposed Rulemaking "[t]he general purpose of adding Rule 51-4.8, Broker-Dealer Cybersecurity, and Rule 51-4.14(IA), Investment Adviser Cybersecurity, is to clarify what a broker-dealer and investment adviser must do in order to protect information stored electronically. The Rule provides guidance to broker-dealers and investment advisers on what factors the Division will consider when determining if the procedures by the firm are reasonably designed to ensure cybersecurity." The proposal states that "a broker-dealer must include cybersecurity as part of its risk assessment."

To the extent reasonably possible, the Colorado proposed cybersecurity procedures must provide for:

1. An annual cybersecurity risk assessment;
2. The use of secure email, including use of encryption and digital signatures;
3. Authentication practices for employee access to electronic communications, databases and media;
4. Procedures for authenticating client instructions receive via electronic communication and
5. Disclosure to client of the risks of using electronic communications.

The proposal goes on to describe what may be considered in evaluating reasonableness as follows:

1. The firm's size;
2. The firm's relationship with third parties;
3. The firm's policies, procedures, and training of employees with regard to cybersecurity practices;
4. Authentication practices;
5. The firm's use of electronic communications;
6. The automatic locking of devices uses to conduct the firm's electronic security; and
7. The firm's process for reporting of lost or stolen devices.

While Colorado's proposed additions to the Colorado Security Act are nowhere near as detailed or extensive as New York's Cybersecurity Regulation, they do demonstrate that states are actively encouraging and forcing companies conducting business within the state to get in Cyber Shape. We expect additional states to continue this trend.

Winget, Spadafora & Schwartzberg, LLP is closely monitoring these developments and assisting clients to get in Cyber Shape. If you would like to discuss the implications of the proposed requirements on your pre-breach preparations, policies, and procedures, please do not hesitate to contact Dianna McCarthy at (212) 221-6900 (mccarthy.d@wssllp.com) or Hillard Sterling at (312) 985-5600 (sterling.h@wssllp.com).
