Brian Hoffman

Partner
303.295.8043
Denver, Washington, D.C.
bnhoffman@hollandhart.com

Colorado Investment Advisers and Broker-Dealers May Soon Face New Cybersecurity Requirements

Publication — 4/13/2017

Recently proposed additions to the Colorado Securities Act would require Colorado investment advisers (IAs) and broker-dealers (BDs) to establish and maintain written procedures “reasonably designed to ensure cybersecurity” and to include cybersecurity as part of their risk assessments. Colorado's proposed additions are the latest in an ongoing trend of close regulatory scrutiny of cybersecurity matters.

Colorado's Proposed Additions

An accompanying rulemaking notice explained that Colorado's proposed additions are designed “to clarify what a broker-dealer and investment adviser must do in order to protect information stored electronically.” Specifically, the proposed additions would require firms' procedures to, the extent reasonably possible, provide for:

1. An annual cybersecurity risk assessments;
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 received via electronic communication; and
5. Disclosure to clients of the risks of using electronic communications.

Colorado does not appear to expect a “one-size-fits-all” solution among firms. Rather, the proposed additions enumerate a list of factors that the Commissioner may consider when determining whether a firm's procedures are reasonably designed:

1. The firm's size;
2. The firm's relationships 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 used to conduct the firm's

electronic security; and

7. The firm's process for reporting of lost or stolen devices;

A public hearing on these, and other, proposed changes to the Colorado Securities Act will be held on May 2, 2017.

Cybersecurity Regulatory Trends Continue

Colorado is not the first state to venture into the cybersecurity regulatory realm for securities and financial firms. The New York Department of Financial Services, for example, adopted even more far-reaching cybersecurity requirements for financial services companies. See our prior alert on the national reach of these regulations. And we may soon see other state financial and securities regulators follow suit by adopting their own cybersecurity regulations as well.

Additionally, the U.S. Securities and Exchange Commission (SEC) has long focused on cybersecurity procedures at investment advisers and broker-dealers. In April 2015, for example, the SEC encouraged firms to conduct periodic assessments of its information collection, potential threats and vulnerabilities, and security controls; develop strategies to respond to threats and incidents; and implement those strategies through written policies and procedures. Even now, cybersecurity remains one of the SEC's top examination priorities for 2017. And the SEC has multiple times taken enforcement action against firms for their alleged failures to adopt written policies and procedures reasonably designed to protect customer data, which later led to a compromise of the customer data.

Moreover, numerous other non-securities-specific federal and state agencies are likewise active in the cybersecurity regulatory realm.

Proactive Attention

As a result of this continued federal and state regulatory focus on cybersecurity issues, investment advisers and broker-dealers are well-advised to proactively review their existing policies and procedures, and assess potential improvements as appropriate.