CARLTON FIELDS

Colorado Set to Regulate Cybersecurity Practices of Broker-Dealers and Investment Advisers

June 23, 2017

On May 15, Colorado became the latest state to publish major regulations tackling cybersecurity in the financial services industry when the Colorado Division of Securities released amendments to existing division rules previously proposed in late March 2017. These new rules clarify what broker-dealers and state registered investment advisers must do to protect the security of "confidential personal information," defined as a first name or initial and a last name in combination with any one of a variety of data elements such as a Social Security number, driver's license or identification card number, or credit card number accompanied by a password or access code information. The rules detail the factors the Division will consider when assessing whether a firm's cybersecurity procedures are sufficient. Substantively the rules for broker-dealers (51-4.8) and investment advisers (51-4.14(IA)) contain identical language. They require broker-dealers and investment advisers to establish and maintain written procedures "reasonably designed" to ensure cybersecurity. When assessing whether the procedures are "reasonably designed," the Commissioner will consider:

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. the firm's authentication practices;
5. the firm's use of electronic communications;

6. the firm's use of automatically locking devices with access to confidential personal information; and,

7. the firm's process for reporting lost or stolen devices.

Firms also are required to include cybersecurity as part of their risk assessments. Furthermore, the regulations specify that the following procedures be included within the adopted written cybersecurity policies, to the extent "reasonably possible":

1. annual cybersecurity risk assessments;

2. use of secure email for emails containing confidential personal information;

3. authentication practices for access to electronic communications, databases, and media by employees;

4. authentication procedures for client instructions received electronically; and,

5. disclosures to clients regarding the risks of using electronic communications.

Colorado follows in the footsteps of New York and Vermont — both of which have adopted cybersecurity regulations — continuing a trend of increased proactivity by states in regulating cybersecurity absent uniform, binding federal legislation or regulations. New York's regulations are more comprehensive than Colorado's; however, they do not apply to investment advisers or broker-dealers because individuals not licensed or registered under New York banking, insurance, or financial regulations do not qualify as covered entities. Colorado's regulations were modeled after Vermont's, which apply to "securities professionals" including broker-dealers and investment advisers, but Colorado's rules stop short of Vermont's requirements that securities professionals maintain evidence of "adequate" cybersecurity insurance proportional to the firm's business and provide free restoration services to victims if a cybersecurity breach occurs. The Colorado regulations are the latest at the state level to impose mandatory cybersecurity procedures upon broker-dealers and investment advisers. The SEC and FINRA have acknowledged the importance of cybersecurity protections via their respective regulatory and examination priorities issued over the past three years, and FINRA issued an extensive report on cybersecurity practices in February 2015. However, SEC and FINRA involvement in cybersecurity has largely been in the form of general guidance. For instance, the SEC's Division of Investment Management issued cybersecurity guidelines in April 2015 for registered investment companies and registered investment advisers. The Colorado and Vermont regulations impose mandatory requirements on state registered investment advisers. And while both FINRA and the SEC require broker-dealers to adopt written data security policies and procedures, Colorado and Vermont's regulations go further by requiring broker-dealers to conduct annual cybersecurity risk assessments and articulating specific cybersecurity procedures to include in broker-dealers' written cybersecurity policies.

Related Practices

Cybersecurity and Privacy
Financial Services Regulatory
Technology
Intellectual Property

Related Industries

Life, Annuity, and Retirement Solutions
Technology