Code of Colorado Regulations – 3 CCR 704-1

Division of Securities

Rule 51-4.8 Broker-Dealer Cybersecurity

A. A broker-dealer must establish and maintain written procedures reasonably designed to ensure cybersecurity. In determining whether the cybersecurity procedures are reasonably designed, the commissioner may 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. Authentication practices;

5. The firm's use of electronic communications;

6. The automatic locking of devices that have access to Confidential Personal Information; and

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

B. A broker-dealer must include cybersecurity as part of its risk assessment.

C. To the extent reasonably possible, the cybersecurity procedures must provide for:

1. An annual assessment by the firm or an agent of the firm of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of Confidential Personal information;

2. The use of secure email for email containing Confidential Personal Information, 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.

Rule 51-4.14(IA) Investment Adviser Cybersecurity

A. An investment adviser must establish and maintain written procedures reasonably designed to ensure cybersecurity. In determining whether the cybersecurity procedures are reasonably designed, the commissioner may 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. Authentication practices;

5. The firm's use of electronic communications;

6. The automatic locking of devices that have access to Confidential Personal Information; and

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

B. An investment adviser must include cybersecurity as part of its risk assessment.

C. To the extent reasonably possible, the cybersecurity procedures must provide for:

1. An annual assessment by the firm or an agent of the firm of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of Confidential Personal Information;

2. The use of secure email containing Confidential Personal Information, 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