Published on *The National Law Review* https://natlawreview.com

New York And Colorado Propose “New” Cybersecurity Regulations for Broker-Dealers

Article By:

Robert V. Cornish Jr.

Richard L. Reiter

In the wake of the promulgation of new cybersecurity regulations by New York State’s Department of Financial Services, Colorado has proposed cybersecurity regulations for broker-dealers, investment advisers and other fund managers in the ever-changing privacy landscape. Financial services firms subject to the rule-making and regulatory authority of the Financial Industry Regulatory Authority (FINRA) and the United States Securities and Exchange Commission (SEC), however, will find that much of what states require is generally reflected in existing rules and the regulatory interpretations of them.

The SEC earlier this year specifically noted that cybersecurity would be one of its examination priorities of broker-dealers, funds and investment advisers. Further, the SEC recently issued an alert on the proliferation of ransomware and repeated the need for those subject to SEC oversight to have adequate cybersecurity procedures, tests and reviews in place. While the New York and Colorado regulations may appear to be new in substance, a significant portion of the issues these regulations address are discussed in detail by the SEC in prior guidance cited in its May 17, 2017, alert. Namely, the need for documented “audit trails” and the substance and nature of systems testing appear in other SEC alerts and in the New York and Colorado regulations. Certainly, attention should be paid to those distinctions to ensure compliance with independent state obligations.

FINRA considers cybersecurity procedures to be part of a registrant’s overall supervisory oversight systems. Strikingly similar to recent FINRA guidance are the provisions of the New York and Colorado regulations dealing with encryption. Also similar to FINRA’s guidance are efforts in the New York rules to offer reasonable regulatory relief to smaller business operations.

Taking things one step further, the National Futures Association (NFA) not only directs its members in the commodities and futures industry to devise and implement supervisory systems to address cybersecurity issues but also suggests in rule-interpretation guidance that members should consider adopting procedures recommended by the SANS Institute (officially, Escal Institute of Advanced Technologies), the Open Web Application Security Project (OWASP), ISACA's Control Objectives for Information and Related Technology (COBIT), and/or the National Institute of Standards and Technology (NIST). See NFA Interpretive Notice 9070 (August 20, 2015). A preponderance of the

rules promulgated by New York and Colorado borrow from these procedures.

While there are distinct differences regarding reporting obligations to notify state regulators of “breach events” and the like, the promulgation of the New York and Colorado cybersecurity regulations essentially codify what broker-dealers, investment advisers and fund managers are or should be doing as required by their respective regulatory or self-regulatory bodies. Nevertheless, compliance with the New York or Colorado regulations, to the extent applicable to a specific business, is essential for a business’s cybersecurity program. Guidance and directives from respective regulator(s) should then be reconciled accordingly in designing, modifying and implementing a cybersecurity compliance program.

National Law Review, Volume VII, Number 145