Client Alert

May 1, 2015

SEC Issues Cybersecurity Guidance for Registered Investment Advisers and Registered Funds

By Kelley Howes and Matthew Kutner

The SEC's Division of Investment Management issued guidance highlighting the importance of cybersecurity and discussing measures that registered investment companies ("funds") and registered investment advisers ("advisers") should consider when addressing cybersecurity risk. The latest guidance reflects the Staff's continuing focus on cybersecurity as a key compliance issue (see our related report on the SEC's cybersecurity sweep exam here).

Other regulators, including FINRA and certain state regulators, have also recently highlighted the importance of this issue for their members and registrants (see our related posts here and here).

As the Staff noted, the nature of cybersecurity threats is "rapidly changing." While that makes the implementation of effective compliance policies challenging, the SEC has made clear that it will continue to examine firms' cybersecurity policies and procedures and their ability to mitigate the impact of a cyber attack.

The guidance highlights a number of measures that funds and advisers may wish to consider when developing cybersecurity policies. The Staff stressed that its suggestions are not comprehensive and that registrants should consider the nature of their businesses and operations to ensure that policies adequately protect fund investors and advisory clients.

ASSESSMENTS

The Staff urged funds and advisers to implement a program to periodically assess:

- The nature, sensitivity, and location of information (collected, processed, and stored) and the technology systems utilized;
- Internal and external threats and vulnerabilities;
- Security controls and processes;
- The potential impact if systems are compromised; and
- The effectiveness of the firm's governance structure for managing cybersecurity risk.

STRATEGIES

The Staff encouraged funds and advisers to develop strategies to prevent, detect, and respond to cybersecurity threats. A list of such strategies might include:

- System access controls;
- Data encryption;
- Restrictions on the use of removable storage media and monitoring for deviations from such restrictions;
- Data backup and retrieval; and
- Developing an incident response plan.

The Staff said that such strategies should be implemented through written policies and procedures and related training for the officers and/or employees of funds and advisers. For example, the training should educate officers and/or employees regarding cybersecurity threats, preventive measures being taken by the entity, and compliance monitoring.

The Staff also suggested that firms consider educating investors and clients about how to reduce their exposure to cybersecurity threats that might affect their accounts.

INTEGRATION INTO COMPLIANCE PROGRAMS

The Staff clearly views cybersecurity policies as integral to a comprehensive compliance program "reasonably designed" to ensure compliance with the federal securities laws and recommends that cybersecurity should be integrated into existing policies rather than established only as a stand-alone program. Funds and advisers should therefore keep cybersecurity in mind when identifying their obligations under the federal securities laws for purposes of developing and implementing their compliance policies. Moreover, they should consider a firm's unique operations when assessing their ability to combat and prevent cybersecurity threats.

The Staff also joined other regulators in stating the importance of assessing the adequacy of cybersecurity protections at vendors and other service providers.

OUR TAKE

Cybersecurity is an area that can affect almost every facet of a firm's business and its relationship with its shareholders, clients, and service providers. As the Staff pointed out, cybersecurity touches not only on technology-related matters (e.g., data protection and identity theft) but also broader issues including business continuity plans and potential disruptions in shareholder services. In short, this is not only a "compliance" issue, it's a business issue.

The Staff recognizes that cybersecurity is an area that moves rapidly, and funds and advisers therefore cannot anticipate and prevent every cyber attack. Nevertheless, funds and investment advisers should consider comprehensively reviewing their cybersecurity policies and related compliance policies. Moreover, firms should consider implementing a crisis response program that would be utilized in the case of a cybersecurity breach.

Doing so now could not only result in a cleaner bill of health from the Staff in the case of an examination, but could very well help a firm maintain the trust and confidence of its shareholders and clients.

Contact:

Jay G. Baris
(212) 468-8053
jbaris@mofo.com

Daniel A. Nathan
(202) 887-1687
dnathan@mofo.com

Stephanie C. Thomas
(916) 325-1328
sthomas@mofo.com

Kelley A. Howes
(303) 592-2237
khowes@mofo.com

Matthew J. Kutner
(212) 336-4061
mkutner@mofo.com

About Morrison & Foerster:

We are Morrison & Foerster—a global firm of exceptional credentials. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We've been included on *The American Lawyer*'s A-List for 11 straight years, and *Fortune* named us one of the "100 Best Companies to Work For." Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations. Prior results do not guarantee a similar outcome.