The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

MEMO# 34030

February 11, 2022

SEC Proposes Amendments to Require Funds, Advisers, and Business Development Companies to Establish Cyber Risk Programs

[34030]

February 11, 2022

TO: Chief Information Security Officer Committee
Technology Committee RE: SEC Proposes Amendments to Require Funds, Advisers, and Business Development Companies to Establish Cyber Risk Programs

The U.S. Securities and Exchange Commission has published for comment proposed rules that will require registered investment companies, investment advisers, and business development companies to "adopt and implement written policies and procedures that are reasonably designed to address cybersecurity risks."[1] The Commission's proposal is briefly described below.

Comments on the proposal are due the later of April 11, 2022, or 30 days following the proposal's publication in the Federal Register. The Institute will be scheduling a call to get members' feedback on the proposal. Prior to that call, we encourage members to review the proposal so you will be prepared to share your comments and thoughts during the call.

I. Cyber Risk Programs of Registered Investment Companies: Rule 38a-2

The SEC proposes to adopt a new rule, Rule 38a-2 under the Investment Company Act of 1940 requiring registered investment companies to have cyber risk programs. The structure of the required program largely tracks those of the SEC's Mutual Fund Compliance Rule (Rule 38a-1)—i.e., they require written policies and procedures, board approval of such policies and procedures, and an annual written report containing certain information about the investment company's program. As noted below, they also, however, include required reporting to the SEC of any "significant fund cybersecurity incident" and disclosures to fund investors of such incidents.

A. Required Policies and Procedures

Proposed subsection (a) of Rule 38a-2 will require all funds to adopt and implement written

policies and procedures that are reasonably designed to address cybersecurity risks. These policies and procedures must include the following elements:

1. A Periodic Risk Assessment. This assessment, which must be in writing, shall include: (a) the categorization and prioritization of the fund's cybersecurity risks "based on an inventory of the components of the fund information systems and fund information residing therein and the potential effect of a cyber incident on the fund;" and (b) the identification of the fund's service providers that receive, maintain, process, or have access to fund information and an assessment of "the cybersecurity risks associated with the fund's use of these service providers."

2. User Security and Access. The rule will require controls designed to minimize user-related risks and prevent unauthorized access to fund information systems and the information in those systems. These controls must:

    a. Require standards of behavior for individuals authorized to access such systems and their information, "such as an acceptable use policy;"
    b. Identify and authenticate individual users, including authentication methods "that require users to present a combination of two or more credentials for access verification;"
    c. Establish procedures for the "timely distribution, replacement, and revocation of passwords or methods of authentication;"
    d. Restrict access to specific fund information systems or components on a needs-to-know basis; and
    e. Secure remote access technologies.

3. Information Protection. The fund's program must include "measures designed to monitor fund information systems and protect fund information from unauthorized access or use." Such measures must be based on a periodic assessment of the fund's information systems and take into account:

    a. The sensitivity level and importance of the information on the system to the fund's business operations;
    b. Whether any of the information is personal information;
    c. Where and how information is accessed, stored, and transmitted, including any monitoring of information in transmission;
    d. Access controls and malware protections; and
    e. The potential effect a cyber incident could have on the fund and its shareholders, "including the ability for the fund to continue to provide services."

As part of its Information Protection policies and procedures, the fund must, pursuant to a written contract between the fund and its service providers that receive, maintain, process, or have access to funds' information systems, require such service providers "to implement and maintain appropriate measures . . . designed to protect fund information and fund information systems." Such measures must include the practices outlined in the rule for funds (i.e., those described above in 1-3 and below in 4-5).

B. Cybersecurity Threat and Vulnerability Management

Under the rule, the fund's policies and procedures must include measures to "detect, mitigate, and remediate any cybersecurity threats and vulnerabilities" to the fund's information systems.

C. Cybersecurity Incident Response and Recovery

The final element required of the fund's policies and procedures (and its service providers') is a duty to have "measures to detect, respond to, and recover from a cybersecurity incident," including those reasonably designed to ensure: continue operation of the fund; the protection of the funds' systems and information; external and internal cybersecurity incident information sharing and communications; and reporting of a "significant fund cybersecurity incident by the fund's investment adviser" under proposed Rule 204-6 under the Investment Advisers Act.[2] The policies and procedures must additionally include written document "of any cybersecurity incident, including the fund's response to and recovery from such incident."

D. An Annual Review and Report

Proposed Rule 38-2(b) requires every fund to, at least annually, "review and assess the design and effectiveness of the cybersecurity policies and procedures" required by subsection (a) of the rule.

E. Board Oversight[3]

As with the Mutual Fund Compliance Program Rule, Rule 38a-2 will require funds to both: (a) obtain the board's approval of the new cybersecurity policies and procedures; and (b) review an annual report prepared on such policies and procedures. The annual report must, at a minimum, include a description of the review, the assessments, any control tests performed, and an explanation of the test results. It must also document any cybersecurity incidents that occurred since the date of the last report and discuss any material changes to the cybersecurity policies and procedures since the last report.

F. Recordkeeping

The rule imposes the following recordkeeping requirements:

1. Policies and procedures must be maintained in an easily accessible place for five years;
2. Copies of written reports provided to the board must be maintained for five years, the first two in an easily accessible place;
3. Records documenting the required annual review for at least five years, the first two in an easily accessible place;
4. Any reports provided to the Commission regarding an adviser's significant cybersecurity events for at least 5 years, the first two in an easily accessible place; and
5. Records documenting the occurrence of any cybersecurity incident, including records related to any response and recover from such incident, for at least five years after the date of the incident, the first two in an easily accessible place.

G. Definitions

Subsection (f) of the proposed rule includes definitions for the following terms:

- Cybersecurity incident[4]
- Cybersecurity risk
- Cybersecurity threat
- Cybersecurity vulnerability

- Fund
- Fund information
- Fund information systems
- Personal information[5] and
- Significant fund cybersecurity incident.[6]

II. Prospectus Disclosure

The Commission's proposal includes revisions to Item 10 of Form N-1A,[7] which governs disclosure relating to a fund's Management, Organization, and Capital Structure. Added to Item 10 is the following:

(4) *Significant Fund Cybersecurity Incident*. Provide a description of any significant fund cybersecurity incident as defined by rule 38a-2 . . . that has or is currently affecting the Fund or its service providers.

Such disclosure must include a description of all significant incidents that have occurred within the last 2 fiscal years as well as any that are currently ongoing. It must include each of the following "to the extent known:"

- The entity or entities affected;
- When the incident was discovered and whether it is ongoing;
- Whether any data was stolen, altered, or accessed or used for an unauthorized purpose;
- The effect of the incident on the Fund's operations; and
- Whether the Fund or a service provider has remediated or is currently remediating the incident.

According to the Release, the Commission is proposing to require all funds to tag information about their significant cybersecurity incidents in a structured, machine-readable data language - i.e., in Inline XBRL in accordance with Rule 405 of Regulation S-T and the EDGAR Filer Manual.

Aside from this required disclosure, the Release notes that:

" . . . a fund that has experienced a number of significant fund cybersecurity incidents in a short period of time may need to disclose heightened cybersecurity risk as a principal risk of investing in the fund." [8]

Also,

". . . funds should generally include in their annual reports to shareholders a discussion of cybersecurity risks and significant fund cybersecurity incidents, to the extent that these were factors materially affected performance of the fund over the past fiscal year." [9]

III. Cybersecurity Programs of Registered Investment Advisers

The Commission's proposal also includes revisions to rules under the Investment Advisers Act that will govern investment advisers' cyber hygiene. These are briefly described below.[10]

A. Rule 204-2, Books and Records

This rule would be revised to require advisers to maintain documents related to the adviser's cybersecurity policies and procedures, annual written report of its cybersecurity

policies and procedures, Form ADV-C, records of cybersecurity incidents, and records documenting any risk assessment. These records must be maintained for five years.

B. 204-3, the Brochure Rule

The Brochure Rule under the Advisers Act would be revised to require advisers' disclosure to include information regarding the adviser's cybersecurity risks and incidents as reported on Form ADV.

C. Rule 204-6, Cybersecurity Incident Reporting

This rule will require advisers to report to the Commission any significant adviser cybersecurity incident or significant fund cybersecurity incident "promptly, but in no even more than 48 hours, after having a reasonable basis to conclude that any such incident has occurred or is occurring." Such report must be made by filing Form ADV-C electronically with the IARD. All Forms ADV-C must be amended within 48 hours as necessary to ensure the information reported remains "materially accurate" or to report the incident has been resolved or an internal investigation relating to it has been closed.

D. Rule 206(4)-9, Advisers' Cybersecurity Policies and Procedures

This new rule imposes upon advisers a duty to have policies and procedures designed to address the adviser's cybersecurity risks. With the exception of the board approval process and board reporting, the requirements for the adviser's policies and procedures are substantially similar to those imposed on funds under Rule 38(a)-2.

IV. Form ADV Disclosure

A. Part 2, Item 20

A new Item 20 would be added to Part 2 of Form ADV to require disclosure of an adviser's cybersecurity risks and incidents. The cybersecurity risks that must be disclosed are those "that could materially affect the advisory services" the adviser offers and how the adviser assesses, prioritizes, and addresses cybersecurity risks created by the nature and scope of its business.

The incidents that must be disclosed are those that have occurred within the last 2 fiscal years that "significantly disrupted or degraded" the adviser's "ability to maintain crucial operations, or has led to the unauthorized access or use of adviser information, resulting in substantial harm" to the adviser or its clients. [Emphasis in rule.] The description of each incident must include, to the extent known: the entity or entities affected; when the incident was discovered and whether it is ongoing; whether any data was stolen, altered, accessed, or used for an unauthorized purposes the effect of the incident on the adviser's operations; and whether the incident has been remediated or is being remediated.

According to the proposal, advisers would be required to deliver interim brochure amendments to existing clients promptly if the adviser adds or materially revises information in the brochure about a cyber incident.

B. New Form ADV-C

The SEC's proposal includes a new Form ADV-C that advisers would use to report the cybersecurity incidents they are required to report pursuant to new Rule 206(4)-6 within 48

hours of an incident. If the incident impacts either private funds or funds of a registered investment company, the adviser would have to provide information on such funds. It also would require reporting of:

- The approximate date the significant cybersecurity incident occurred;
- The approximate date it was discovered;
- Whether it is ongoing and, if not, the approximate date it was resolved or an investigation of it was closed;
- Whether law enforcement or a government agency has been notified;
- The nature and scope of the incident, including impact on critical operations;
- Actions taken or planned in response to the incident;
- Whether data was stolen, altered, access, or used for an unauthorized purpose;
- Whether any personal information was lost, stolen, modified, deleted, destroyed, or accessed without authorization;
- Whether the event has been disclosed to the adviser's clients and/or to investors in a registered investment company and, if so, when the disclosure was made. If not, the adviser must explain why it was not disclosed; and
- Whether the event is covered by a cybersecurity policy and, if so, whether the insurance company has been notified.

According to the Release, the SEC's preliminary view is that the information provided on the form should be confidential and not available to the public.[11]

Tamara K. Salmon
Associate General Counsel

Peter G. Salmon
Senior Director, Technology & Cybersecurity

Endnotes

[1] See Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies, SEC Release No. 33-11028 (February 9, 2022)(the "Release"), which is available at: https://www.sec.gov/rules/proposed/2022/33-11028.pdf.

[2] This is discussed below under III.

[3] If the fund is a unit investment trust, the fund's principal underwriter or depositor must perform the required oversight.

[4] A "cybersecurity incident" is defined as "an unauthorized occurrence on or conducted through a fund's information systems that jeopardizes the confidentiality, integrity, or availability of a fund's information systems or any fund information residing therein."

[5] "Personal information" is defined as information that alone or in conjunction with other information can be used to identify an individual such as "name, date of birth, place of birth, telephone number, street address, mother's maiden name, SSN, driver's license number, electronic mail address, account number, account password, biometric records, or

other non-public personal information."

[6] A "significant fund cybersecurity incident" is defined as one "that significantly disrupts or degrades the fund's ability to maintain critical operations, or leads to the unauthorized access or use of fund information, where the unauthorized access or use of such information results in substantial hard to the fund or to an investor whose information was accessed."

[7] Similar changes were made to other registration statements under the Investment Company Act (i.e., Forms N-2, N-3, N-4, N-6, and N-8B2.

[8] Release at p. 66-67.

[9] Release at p. 67.

[10] As discussed above, proposed new Rule 38a-2, in part, requires a fund's policies and procedures related to cybersecurity incident response and recovery to ensure the "reporting of significant fund cybersecurity incidents by the fund's adviser under Rule 204-6."

[11] Release at p. 59.
