Schulte Roth&Zabel

# Alert

## SEC Proposes Cybersecurity Risk Management

February 10, 2022

On Feb. 9, 2022, the Securities and Exchange Commission ("SEC") proposed new cybersecurity risk management rules and amendments (the "Proposed Cyber Rules")[1] intended to enhance cybersecurity preparedness of registered investment advisers ("RIAs") and registered investment companies and business development companies (together, "Regulated Funds") and to require more disclosure regarding cyber risks and incidents.

Specifically, the Proposed Cyber Rules seek to: (1) require RIAs and Regulated Funds to adopt and implement written policies and procedures that are reasonably designed to address cybersecurity risks; (2) require advisers to report significant cybersecurity incidents to the SEC on proposed Form ADV-C; (3) enhance adviser and fund disclosures related to cybersecurity risks and incidents; and (4) require advisers and funds to maintain certain cybersecurity-related books and records.

### Cybersecurity Policies and Procedures

The proposed new risk management rules would require RIAs and Regulated Funds to adopt and implement cybersecurity policies and procedures, which can be tailored to the individual cybersecurity risks for the business but at a minimum must incorporate the following general elements:[2]

- Risk Assessment – periodic assessments (1) to identify "cybersecurity risks"[3] to "Information Systems"[4] (a term "designed to be broad enough to encompass all the electronic information resources owned or used" by an RIA or Regulated Fund) and Information (defined to encompass any electronic information related to the firm's business)[5] and (2) to identify cybersecurity risks to applicable service providers that handle Information;
- User Security and Access – controls designed to minimize user-related risks and prevent unauthorized access to Information Systems and Information, including on personal mobile devices or when remote work is conducted through unsecured or less secure WiFi;

---

[1] "Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies," Release No. 33-11028 (Feb. 9, 2022), available at https://www.sec.gov/rules/proposed/2022/33-11028.pdf?utm_medium=email&utm_source=govdelivery (the "Proposing Release").

[2] For a Regulated Fund, the board of directors would have to approve cybersecurity policies and procedures. If the Regulated Fund is a unit investment trust, the Proposed Cyber Rules provide that a Fund's principal underwriter or depositor must approve the Fund's policies and procedures and receive the written report describing the Fund's annual cybersecurity review described above.

[3] The Proposed Cyber Rules define "cybersecurity risk" as financial, operational, legal, reputational and other adverse consequences that could result from cybersecurity incidents, threats and vulnerabilities.

[4] The Proposed Cyber Rules define "information systems" to mean the information resources owned or used by the RIA or Regulated Fund, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of Information to maintain or support the firm's operations.

[5] "Information" is defined in the Proposed Cyber Rules as any electronic information related to the RIA's or Regulated Fund's business, including personal information received maintained, created or processed by the RIA or Regulated Fund.

- Information Protection – measures designed to monitor Information Systems and protect Information from unauthorized access or use. Firms would be required to oversee any service provider that handles Information (including, for example, through due diligence and periodic reviews of the service providers) and have written contracts with service providers requiring them to have appropriate measures in place;
- Threat and Vulnerability Management – measures designed to detect, mitigate and remediate any cybersecurity threats and vulnerabilities relating to Information Systems and Information as well as role-specific cybersecurity threat and vulnerability response training; and
- Cybersecurity Incident Response and Recovery – measures designed to detect, respond to and recover from a cybersecurity incident,[6] including policies and procedures that are reasonably designed to ensure: (1) the firm's continued operations; (2) protection of Information Systems and Information; (3) external and internal cybersecurity incident information sharing and communications; and (4) reporting of significant cybersecurity incidents to the SEC on proposed Form ADV-C.

The broad definition of Information puts all business-related electronic communications in scope and, among other things, adds to the challenges firms face when unapproved messaging platforms are used for conducting firm business. The Proposing Release notes that firms should consider issuing firm-issued mobile devices or installing a mobile device manager on employees' personal phones to control work-related content. The SEC also seeks comments regarding what user measures RIAs currently have for mobile devices. Further, as proposed, the rules could impose a significant burden on RIAs and Regulated Funds to vet and monitor the cybersecurity programs of many different types of service providers.[7]

**Annual Review**

RIAs and Regulated Funds would be required to conduct an annual review that assesses the effectiveness of the cybersecurity policies and procedures, including identification of any changes in cybersecurity risk over the time period covered by the review, and prepare a written report that describes the review, assessment and any control tests performed, explains the results, documents any cybersecurity incident that occurred since the date of the last report and discusses any material changes to the policies and procedures since the date of the last report. While the expertise of cybersecurity consultants could be leveraged in conducting the annual review, the SEC expects the review to be overseen by the person responsible for administering the firm's cybersecurity policies. Regulated Funds also would be required to provide the written report to their boards of directors.

**Reporting of Significant Cybersecurity Incidents**

RIAs and Regulated Funds would be required to report significant cybersecurity incidents to the SEC by submitting a proposed Form ADV-C within 48 hours after having a reasonable basis to conclude that a

[6] The Proposed Cyber Rules define a "cybersecurity incident" as an unauthorized occurrence on, or conducted through, Information Systems that jeopardizes the confidentiality, integrity or availability of Information Systems or Information.

[7] Current SEC rules require RIAs and Regulated Funds to address cybersecurity measures in certain circumstances. For example, firms subject to Regulation S-P are required to adopt written policies and procedures that address administrative, technical and physical safeguards for the protection of customer records and information. They must be reasonably designed (1) to protect the security and confidentiality of customer records and information and (2) to protect against any anticipated threats or hazards, unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer. Additionally, firms subject to Regulation SID must develop and implement a written identity theft program that includes reasonable policies and procedures to identify and detect relevant red flags, as well as respond appropriately to red flags so as to prevent and mitigate identity theft.

significant cybersecurity incident has occurred or is occurring. A "significant cybersecurity incident" is a cybersecurity incident, or a group of related incidents, that (1) significantly disrupts or degrades an RIA's or Regulated Fund's ability to maintain critical operations or (2) leads to the unauthorized access or use of Information that results in: (a) substantial harm to the RIA or Regulated Fund or (b) substantial harm to an advisory client or investor whose Information was impacted.

The Proposed Cyber Rule also would require an adviser to amend any previously filed Form ADV-C within 48 hours:

- After information on the form becomes materially inaccurate;
- If new material information about a previously reported incident is discovered; and
- After resolving a previously reported incident or closing an internal investigation pertaining to a previously disclosed incident.

Form ADV-Cs would be confidential.

In the wake of a cyber-incident, it can often take forensic experts some time to assess the extent of the harm and the Information impacted, making it difficult in the first instance to determine when the 48-hour initial notification period has been triggered. Further, a firm could be required to make repeated amendments over the course of a forensic investigation as new information is discovered. The Proposed Cyber Rules also raise the possibility that a cyber-incident that occurred at a service provider may create a significant cybersecurity event for a firm.

Additionally, the recent proposal for amendments to Form PF requires large hedge fund advisers to report within one business day a cyber-incident that results in a significant disruption or degradation of key operations. Taken together, the proposed changes to Form PF and the Proposed Cyber Rules could result in some managers being subject to different reporting requirements (on different timelines) for the same incident.

**Disclosure of Cybersecurity Risks and Incidents**

An RIA would be required to disclose cybersecurity risks that could materially affect its advisory services and how the RIA assesses, prioritizes and addresses such risks on proposed Form ADV Part 2A Item 20. Item 20 also would require an RIA to provide a detailed description of any cybersecurity incident that has occurred within the last two fiscal years that has significantly disrupted or degraded its ability to maintain critical operations, or has led to the unauthorized access or use of Information, resulting in substantial harm to the firm or its clients. The Proposed Cyber Rules also would require an RIA to deliver interim brochure amendments to existing clients promptly if they add disclosure of a cybersecurity incident or materially revise a prior disclosure regarding the incident.

**Recordkeeping**

The Proposed Cyber Rules would require RIAs and Regulated Funds to maintain records of:

- Written cybersecurity policies and procedures that are in effect or at any time within the past five years were in effect;

- Written reports documenting the firm's annual reviews of such policies and procedures within the last five years;
- A copy of any Form ADV-C and amendments filed by the adviser in the last five years;
- Records documenting the occurrence of any cybersecurity incident occurring within the last five years, including records related to any response and recovery from such an incident; and
- Records documenting any cybersecurity risk assessments conducted in the last five years.

*Authored by Marc Elovitz, Kelly Koscuiszka, Meghan Carey, Christopher Avellaneda and Tarik Shah.*

If you have any questions concerning this *Alert*, please contact your attorney at Schulte Roth & Zabel or one of the authors.

Schulte Roth & Zabel
New York | Washington DC | London
www.srz.com