Preparing for the SEC's Cybersecurity Rules for Registered Investment Advisers, Registered Investment Companies, and Business Development Companies

March 13, 2023

In February 2022, the SEC proposed its first-ever cybersecurity rules for registered investment advisers ("RIAs") (including RIAs to private funds) and Funds (which include registered investment companies ("RICs") and closed-end funds that have elected to be treated as business development companies ("BDCs") under the Investment Company Act), which we previously discussed here. The SEC has indicated that it plans to issue final rules in April 2023 (along with new cybersecurity rules for public companies, which we previously discussed here).

The proposed cybersecurity rules for RIAs and Funds impose significant new regulatory burdens, including a new 48-hour cybersecurity incident notification requirement, detailed cybersecurity policies and procedures requirements, and additional disclosure and recordkeeping requirements. This post focuses on how to prepare for compliance with these new SEC rules, which Debevoise's Data Strategy and Security and White Collar and Regulatory Defense Practices will discuss in depth in our March 21 webcast on the topic. The webcast will also discuss the intersection between the proposed cybersecurity rules for RIAs and Funds with the SEC's newly proposed amendments to Reg S-P and the new broker-dealer cybersecurity risk management rule.

Background on the Rule Proposal

On February 9, 2022, the SEC proposed rules on cybersecurity risk management for RIAs and Funds (the "Proposed Rules"). Consistent with Chair Gensler's cybersecurity priorities, the Proposed Rules are the SEC's first-ever requirements specifically obligating RIAs and Funds to adopt and implement cybersecurity controls. The Proposed Rules are consistent with the trend of regulators across industries (including banking, financial services, and critical infrastructure) zeroing in on cybersecurity.

Key Requirements

The Proposed Rules requirements fall into four main categories: (1) cyber incident notification obligations, (2) policies and procedures, (3) disclosure requirements, and (4) books and records requirements.

1) **48-Hour Incident Reporting**: The Proposed Rules impose a new 48-hour cybersecurity incident notification requirement on RIAs. Specifically, RIAs would be required to report significant adviser or fund cybersecurity incidents (including on behalf of a RIC, BDC, or private fund that experiences an incident). The Proposed Rules define a significant cybersecurity incident as an incident or group of related incidents that either (1) "significantly disrupts or degrades" the RIA's or Fund's "ability to maintain critical operations" or (2) "leads to the unauthorized access or use of" RIA or Fund information where that unauthorized access or use results in "substantial harm" to the RIA, Fund, client, or investor in a private fund. Such notifications must be made within 48 hours after "having a reasonable basis to conclude that a significant adviser or fund cybersecurity incident has occurred or is occurring."

   The SEC has proposed that notifications be made by submitting (and updating as material facts change) a Form ADV-C to the SEC. The SEC has stated that such forms will remain confidential.

2) **Cybersecurity Risk Management Policies & Procedures**: The Proposed Rules require RIAs and Funds to implement cybersecurity policies and procedures tailored to the RIA's or Fund's business operations, including its complexity and specific cybersecurity risk. The Proposed Rules recognize that there is no "one-size-fits-all approach" in cybersecurity, and that risk management programs should be appropriately tailored to and evolve with the business. That said, the Proposed Rules require all RIAs and Funds to adopt policies and procedures that address certain elements (*e.g.*, user security and access, information protection, threat and vulnerability management, and incident response and recovery).

   In addition to these elements, RIAs and Funds would be required to review these policies and procedures annually and to prepare a report describing the review, explaining its results, documenting any incident that has occurred since the last report, and discussing any material changes to the policies and procedures since the last report.

   In the case of Funds, the Proposed Rules would also require Funds' boards of directors to review and approve the Fund's cybersecurity policies and procedures.

Funds' boards would also be required to review the annual required written report on cybersecurity incidents and material changes to the Fund's cybersecurity policies and procedures.

The Proposed Rules provide that RIAs and Funds may use third-party cybersecurity risk management services, provided that the service providers are appropriately overseen.

3) **Disclosure Obligations**: The Proposed Rules also require RIAs and Funds to disclose certain cybersecurity risks and incidents to their clients, investors, and other market participants through updated forms (Form ADV Part 2A for RIAs and Forms N-1A, N-2, N-3, N-4, N-6, N-8B-2, and S-6 for Funds).

With respect to RIAs, the updated Form ADV Part 2A would require RIAs to provide information on the cybersecurity risks that could materially impact their services and, in plain English, describe how they plan to assess, prioritize, and address these risks. RIAs would also be required to disclose significant cybersecurity incidents that occurred within the last two fiscal years. RIAs would also be required, under certain circumstances, to update and deliver an interim brochure supplement if there are material changes to the incident disclosures.

The materiality determination for these disclosures is not dependent on whether a risk leads to an actual cyber incident; rather, the SEC is clear in the Proposed Rules that materiality depends on factors like the likelihood and extent to which the cybersecurity risk or incident: (1) could occur and what safeguards are in place to prevent it; (2) could or has disrupted the adviser's ability to provide services; (3) could or has resulted in the loss or compromise of sensitive data; and (4) has or could harm clients.

Funds would also be required to make certain cybersecurity-related disclosures in their registration statements. In particular, Funds would be required to disclose significant cybersecurity incidents from the past two fiscal years. The Proposed Rules also highlight the fact that Funds should consider whether cybersecurity risks warrant disclosure as a "principal risk" in registration statements or as part of the Fund's annual report. The Proposed Rules would also require a Fund to amend its prospectus if a cybersecurity risk or incident results in the prospectus containing an untrue statement of material fact or omitting a material fact necessary to make the disclosure not misleading.

4) **Books and Records**: The Proposed Rules also address books and records obligations, including that RIAs and Funds maintain records related to the

requirements discussed above (*e.g.*, Form ADV-C filings, policies and procedures, annual review reports, records of cybersecurity incidents, and risk assessment documentation).

Getting Ready for Compliance

The SEC has signaled that it plans to issue final rules in April 2023, and we expect that they will likely become effective in late 2023. Given the breadth of new requirements, RIAs and Funds should consider the following steps to prepare for these rules:

1. **Procedures to Meet the 48-Hour Breach Notice Deadline**: The proposed 48-hour notification timeline for cybersecurity incidents will be challenging to meet, particularly without thoughtful and deliberate preparation. RIAs should consider implementing clear protocols for reporting incidents internally, drafting incident notifications, and obtaining the necessary approvals to send out their notifications within the deadline.

   Drawing upon learnings from the banking sector's 36-hour reporting requirement, firms might consider creating protocols regarding (i) which entities (and which systems) are covered by the notification requirement, (ii) who is responsible for making the notification and who must approve such notification, (iii) what types of incidents might trigger the notification requirement and to whom such incidents should be escalated, and (iv) ensuring that a notification template is prepared in advance of an incident so that the notification does not need to be drafted from scratch.

   For RIAs that are also public companies, it will be important to consider the interplay between these proposed rules and the proposed cybersecurity rules for public companies, which propose to require Form 8-K filings for material cybersecurity incidents. Entities for which both rules may apply should consider implementing notification procedures for both Form ADV-C and Form 8-K filings.

2. **Cybersecurity Policies and Procedures**: The Proposed Rules will require RIAs and Funds to establish comprehensive cybersecurity policies and procedures to mitigate cybersecurity risks. Registrants should ensure that the required policies and procedures are implemented or that their current policies and procedures encompass all of the requirements provided in the Proposed Rules. As RIAs and Funds build out their cybersecurity risk management programs, it is important

to remember that not only should these policies and procedures be compliant, but they must also be actionable by the firm.

RIAs and Funds should therefore look to their risk assessment procedures to ensure that they are identifying, categorizing, and prioritizing cybersecurity risks presented by their systems and operations. Absent an effective risk assessment process, RIAs and Funds may not have the information to develop effective and compliant policies and procedures that squarely address potential cybersecurity risks.

As RIAs and Funds are designing and updating policies and procedures, it is also worth considering the annual review process. The cybersecurity threat landscape is constantly evolving, which means that policies and procedures that are effective one year may not be sufficient the next. RIAs and Funds should consider whether their policy and procedure design and review process incorporates not only information about internal systems and operations, but also information about changes in the external threat landscape.

As noted before, external cybersecurity risk management services can be used to implement such policies and procedures, provided that the firm provides adequate supervision. In addition, testing to ensure compliance will likely be important, as the SEC has previously used policy violations as a hook for more sweeping enforcement actions.

3. **Procedures to Meet New Disclosure Obligations**: The Proposed Rules require that RIAs and Funds provide certain disclosures associated with cybersecurity risks or incidents to the SEC as well as to clients, investors, and other market participants. RIAs and Funds should ensure that there are procedures for clear and accurate disclosures. Additionally, RIAs and Funds should have a system by which to update such disclosures as new facts come to light. This will require consideration of what is considered a "material" cybersecurity risk for the firm.

4. **Systems to Maintain Operations in the Event of an Incident**: The SEC emphasizes in the Proposed Rules the importance of continued operations in the event of a cybersecurity incident. Accordingly, RIAs and Funds should consider testing their incident response and business continuity plans through tabletop exercises, to see if they are current and actionable, especially with respect to meeting notification requirements.

5. **Documentation**: It will not be sufficient to have good technical cybersecurity controls — documentation is also necessary, as highlighted by the new recordkeeping obligations. Books and records violations are an easy hook for

SEC examination and enforcement activity when a firm does not have well-documented evidence that its cybersecurity program has been, and remains, compliant.

Debevoise will be holding a webinar on March 21, 2023 to discuss the Proposed Rules, the lessons learned from current SEC cybersecurity exams and enforcement activity and how RIAs and Funds should prepare for the Proposed Rules. The link to register for the webinar is here.

To subscribe to our Data Blog, click here.

* * *

Please do not hesitate to contact us with any questions.

New York

Avi Gesser
agesser@debevoise.com

Erez Liebermann
eliebermann@debevoise.com

Charu A. Chandrasekhar
cchandra@debevoise.com

Suchita Mandavilli Brundage
smbrundage @debevoise.com

Jarrett Lewis
jxlewis @debevoise.com

San Francisco

Kristin A. Snyder
kasnyder @debevoise.com

Washington, D.C.

Luke Dembosky
ldembosky @debevoise.com

Julie M. Riewe
jriewe @debevoise.com