Four Takeaways from the SEC's Proposed Cybersecurity Rules

February 17, 2022

On February 9, 2022, the SEC released its much-anticipated proposed rules relating to cybersecurity risk management, incident reporting, and disclosure for investment advisers and funds. Many of the proposals follow the trends that members of the Debevoise Data Strategy & Security and White Collar & Regulatory Defense practice groups discussed during a November 2021 webcast on the SEC's Cybersecurity Year in Review, as well as in our prior Data Blog posts (here and here).

Chair Gensler recently emphasized that cybersecurity rulemaking in this area is one of his priorities, and placed particular emphasis on establishing standards for cybersecurity hygiene and incident reporting for registrants. The proposed rules, which are the most detailed cybersecurity rules that Chair Gensler's SEC has issued thus far, reflect the SEC's intense attention to cybersecurity risk and its willingness to deploy the full scope of its regulatory authority to promulgate standards that address this risk.

These proposed rules would impose significant new requirements on registered investment advisers and funds, and are generally consistent with cybersecurity requirements imposed on other companies by New York's Part 500 Cybersecurity Regulation and the Federal Trade Commission's updated Safeguards Rule.

Key Requirements under the Proposed Rules

Cybersecurity Risk Management Policies & Procedures

The proposed rules would require advisers and funds to adopt and implement policies and procedures that are "reasonably designed" to address cybersecurity risks. There are several "general elements" that advisers and funds will need to address in their cybersecurity policies and procedures, including risk assessment practices, user security and access, preventing unauthorized access to funds, threat and vulnerability management, and incident response and recovery. The proposed rules require advisers and funds, on an annual basis, to: (1) review and assess the design and effectiveness of their cybersecurity policies and procedures; and (2) prepare a report describing the

review, explaining the 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.

The proposed rules also add requirements relating to board oversight and recordkeeping. Under Proposed Rule 38a-2, registered funds would be required to have their boards, including a majority of its independent directors, (1) approve their cybersecurity policies and procedures, and (2) review the annual report.

Incident Reporting

The proposed rules would also require advisers, "including on behalf of a client that is a registered investment company or business development company, or a private fund" (collectively, "covered clients"), to report any significant cybersecurity incidents, which are defined as any event that (1) "significantly disrupts or degrades the adviser's" or private fund client's "ability to maintain critical operations" or (2) "leads to the unauthorized access or use of adviser information" resulting in substantial harm to the adviser, or substantial harm to a client, or an investor in a private fund, whose information was accessed. Advisers, on behalf of themselves and their covered clients, must report to the SEC within 48 hours from when they have a reasonable basis to believe such an incident has occurred.

Advisers must use the new proposed Form ADV-C for incident notification to the SEC. The notification must include a detailed description of the nature and scope of the incident and any disclosures about it. Advisers will be expected to update any previously submitted Forms ADV-C when there has been a material change in facts. The proposed rule states that submitted Forms ADV-C will remain confidential and not be disclosed to the general public. However, the proposed rules do not address whether the ADV-C filing would be exempt from FOIA.

Disclosure Obligations for Advisers

The proposed rules would also amend Form ADV Part 2A for advisers to include disclosure of cybersecurity risks and incidents that could materially affect the advisory relationship with current and prospective clients. The amendment would require that advisers describe, in plain English, the cybersecurity risks that could materially affect the services they offer and how they plan to assess and address those risks. If adopted, the disclosures must include information about 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.

The proposed amendments would also require advisers to describe any significant cybersecurity incidents that have occurred within the last two fiscal years and require advisers to deliver interim brochure amendments to clients if (1) the adviser was subject to a cybersecurity incident after the dissemination of its brochure, or (2) the information already disclosed in its brochure about an incident materially changes based on new discoveries.

Disclosure Obligations for Funds

Under the proposed rules, changes would be made to Forms N-1A, N-2, N-3, N-4, N-6, N-8B-2, and S-6 for funds to report significant cybersecurity incidents and risks, similar to the required disclosures for advisers. The rules propose amendments to funds' registration forms that would require a description of any significant fund cybersecurity incident that has occurred in its last two fiscal years, and expands the definition of "principal risks" of investing in the fund to include cybersecurity risks and requires disclosure of such in fund registration statements. To the extent that cybersecurity incidents occur after the filing of a fund's registration forms and this alters the material position or risks involved with the fund, the fund must then file a supplement to the Commission.

Key Takeaways

Prepare for 48-Hour Breach Notice Deadline

Advisers may find it challenging to meet the strict 48-hour reporting timeline requirements set out by the proposed rules. Many companies have struggled to meet the longer 72-hour breach notification deadlines under the NYDFS Part 500 and GDPR. Having clear protocols for escalating incidents, drafting the notifications, and obtaining the necessary approvals can make the difference between (1) meeting tight notification deadlines and gaining credibility with the applicable regulator, and (2) missing the deadline and starting off having to explain to the regulator why the notification was late, which can undermine the regulator's view of the overall competence of the response. Advisers can learn from banks that are preparing for the new 36-hour reporting requirement, which have started implementing such protocols, including:

- Who is Covered -- Determining which entities in their group are subject to the new notification deadline, and if it only applies to some entities, assessing which data, information systems, and employees are associated with the covered entities.

- Who is Responsible -- Determining who the person responsible for making the notification, and who else, if anyone, must approve the notification before it is made.

It may be prudent to designate more than one person for each of these roles, in case someone is unavailable.

- Prompt Escalation -- Determining which incidents may trigger the short-deadline notification requirement and therefore should be escalated to the persons responsible for that notification, as well as who should be making that escalation.

- Notification Template -- Creating a sample notification, so that the actual notification does not need to be drafted from scratch during an incident.

Adopt, Implement, and Test Policies and Procedures

The proposed rules expand the policies and procedures obligations for advisers and registered funds. Proposed rules 206(4)-9 and 38a-2 would require advisers and registered funds to establish and implement cybersecurity policies and procedures that are "reasonably designed to mitigate cybersecurity risk," including risk assessment, standards for user security and access, information protection, threat and vulnerability management, and cybersecurity incident response and recovery. The proposed rules also provide very specific guidance on multiple elements of an expected cybersecurity risk and incident response program; while preexisting policies and procedures may include some of these components, they must now include all of them. Moreover, regular testing to ensure sufficient implementation will be crucial to effective compliance with the SEC's objectives of cybersecurity risk mitigation and compliance. Targeting policies and procedures violations has been a longstanding enforcement approach for the SEC (see First American), and the proposed rules provide a clear "hook" for doing so in the SEC's priority area of cybersecurity.

Disclosures and Evidence Preservation

The proposed rules emphasize the importance of clear and accurate disclosures regarding cybersecurity risk and incidents to investors and the SEC, formalizing takeaways from the SEC's 2021 enforcement actions against Pearson and First American as well as the priorities emphasized by Chair Gensler. As it has in the past, we can expect that the SEC will use the proposed rules once enacted to scrutinize cybersecurity-related disclosures and recordkeeping violations through exams and enforcement actions. Companies should ensure that their disclosures are not only accurate, but are also supported by objective evidence and documentation, which will require some thoughtful analysis as to which aspects of the investigation the company wishes to assert privilege.

Incident Response Planning

Through these proposed rules, the SEC has stressed the importance of maintaining continued operations in the event of an incident. Advisers and funds should therefore review their incident response plans and business continuity plans, and consider testing those plans through a tabletop exercises. Given that the proposed rules expand notification obligations of advisers and funds to include incidents affecting private fund and BDC clients' systems or information, these tabletop exercises can test escalation of incidents and engagement of all the relevant players in the incident response process.

We will continue to track and blog on these important updates. Public comments are open until at least April 9, 2022.

* * *

The Debevoise Data Portal is now available for clients to help them quickly assess and comply with their state, federal, and international breach notification obligations, as well as their substantive cybersecurity and AI legal obligations.

To subscribe to our Data Blog, please click here.

The authors would like to thank Linda Lin, a Debevoise law clerk, for her contributions to this post.

Please do not hesitate to contact us with any questions.

NEW YORK

Avi Gesser
agesser@debevoise.com

Charu A. Chandrasekhar
cchandrasekhar@debevoise.com

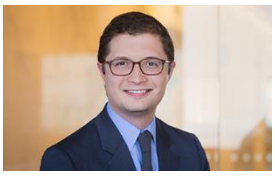
Matthew C. Rametta
mcrametta@debevoise.com

WASHINGTON, DC

Luke Dembosky
ldembosky@debevoise.com

Julie M. Riewe
jriewe@debevoise.com

SAN FRANCISCO



Christopher S. Ford
csford@debevoise.com

H Jacqueline Brehmer
hjbrehmer@debevoise.com