ALSTON & BIRD

WWW.ALSTON.COM

Privacy, Cyber & Data Strategy / Investment Management, Trading & Markets ADVISORY ■

MARCH 11, 2022

SEC Cements Expectations for Investment Advisers' and Investment Companies' Cyber Preparedness and Disclosure

by Blake E. Estes, Katherine Doty Hanniford, Kimberly Kiefer Peretti, and Timothy P. Selby

The U.S. Securities and Exchange Commission (SEC) on March 9, 2022 published in the *Federal Register* a proposed new cybersecurity risk management rulemaking that would establish comprehensive cybersecurity compliance requirements and enhanced reporting and disclosure obligations for registered investment advisers, investment companies, and business development companies (BDCs). The deadline to submit comments is April 11, 2022.

With the recent acceleration of cyber-attacks on the financial sector and the implementation of increasingly prescriptive regulatory requirements by other federal financial regulators, the SEC's new proposed rules would expand its visibility into investment adviser, fund, and BDC cybersecurity preparedness and incident reporting, while also providing fund investors with greater transparency into their current state of security. SEC staff have recently expressed concern that, based on findings from SEC examinations, registered investment advisers and funds may have insufficient or outdated cybersecurity programs in place and have voiced similar concerns about the quality and accuracy of adviser and fund disclosures for cybersecurity risks and cyber-incidents. The proposed rules cement the SEC's previously articulated expectations that advisers and funds tailor their cybersecurity programs to their particular business operations and risks, but they also add prescriptive requirements to ensure policies and procedures are updated in a timely fashion based on the rapidly evolving cyber-threat landscape.

Overview

The proposed rules are a departure from the SEC's existing cybersecurity and data protection rules in three key ways:

(1) Broader Focus Than Protection of Customer Information. The existing rules such as Regulation S-P and Regulation S-ID focus on the protection of customer information pursuant to the Safeguards Rule under the Gramm–Leach–Bliley Act. The proposed rules instead stem from investment advisers' fiduciary obligations under the Investment Advisers Act of 1940 and the Investment Company Act of 1940 and take a more holistic approach to the protection of client interests, which the SEC broadly construes to cover the registrant's information system and operational risks as well as client information, for example, in addition to simply customer information.

(2) Cyber-Incident Reporting. Until this rule release, the SEC adhered to a more flexible, standards-based approach to cybersecurity regulation and was largely silent on cyber-incident reporting. Although the Division of Examinations has previously issued guidance on cybersecurity practices and encouraged the implementation of increasingly specific controls and practices by registered investment advisers, this proposed rulemaking represents the first comprehensive and formal

cybersecurity rules and cybersecurity incident reporting requirements for investment advisers and investment companies subject to SEC regulation through the Advisers Act and Investment Company Act. The rules would require advisers and funds to (1) report "significant cybersecurity incidents" to the SEC within 48 hours; (2) publicly disclose cybersecurity risks and significant cybersecurity incidents that occurred in the last two fiscal years in their brochures and registration statements; (3) submit written reports at least annually to funds' boards of directors; and (4) retain for five years specific supporting documentation that demonstrates compliance with the proposed rules, which presumably will be leveraged by SEC staff in the examinations and investigations contexts.

(3) Cybersecurity Incident Redefined. Consistent with the proposed rules for cybersecurity incident reporting for public companies, the SEC has proposed to broadly define a "cybersecurity incident" as "an unauthorized occurrence on or conducted through [an adviser's or a fund's] information systems that jeopardizes the confidentiality, integrity, or availability of [an adviser's or a fund's] information systems or any [adviser or fund] information residing therein." Although the SEC has intentionally defined this term broadly to encompass incidents that could adversely affect an SEC registrant in a number of ways and harmonizes the definition of a triggering incident across all SEC registrants, this definition differs from how the Federal Trade Commission, Federal Reserve, Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation, and state financial and consumer protection statutes have otherwise and previously defined triggering cybersecurity incidents, which may complicate compliance efforts for SEC registrants that have aligned their cybersecurity program to comply with other regulatory regimes.

Cybersecurity Risk Management Rules

The proposed new Rule 206(4)-9 under the Advisers Act and new Rule 38a-2 under the Investment Company Act would require subject advisers and funds to adopt and implement written policies and procedures reasonably designed to address cybersecurity risks. These include "operational and other risks that could harm advisory clients and fund investors or lead to the unauthorized access to or use of adviser or fund information," including the personal information of their clients or investors.

Under the proposed rule, an adviser's or fund's cybersecurity policies and procedures should continue to be tailored to business operations, including their complexity, and attendant cybersecurity risks. While certain core areas that advisers and funds would be required to address in their cybersecurity policies and procedures are enumerated in the new rules, the SEC continues to recognize that firms need the ability to tailor their cybersecurity policies to their individual characteristics and circumstances. For example, an adviser or fund must empower the administrator of the cybersecurity policies and procedures to make decisions and escalate issues to senior officers as necessary; however, that administrator can be an in-house resource with appropriate knowledge and expertise or a third-party risk management service provider with appropriate oversight.

Risk assessment

As a first step in risk management, the new rules would require advisers and funds to conduct a risk assessment and to periodically reassess, categorize, prioritize, and draft written documentation of the cybersecurity risks associated with their information. Categorizing and prioritizing cybersecurity risks must be based on an inventory of the components of an adviser's or fund's information systems and the information residing therein in light of the firm's particular operations. The risk assessment must also identify service providers that receive, maintain, or process adviser or fund information, or that are permitted access to information systems, and consider the service providers' cybersecurity practices.

Access controls

Reasonably designed policies and procedures would further require access controls designed to minimize user-related risks and prevent the unauthorized access to information and systems. This includes standards of behavior for individuals authorized to access firm information systems, the implementation of multifactor authentication, a comprehensive password policy, access to information only as necessary for individuals to perform their responsibilities and functions on behalf of the adviser or fund, and securing remote access technologies.

System monitoring & oversight

The proposed rule would also require that cybersecurity policies and procedures include the monitoring of information systems and protection of information from unauthorized access or use. Advisers and funds would be required to determine which controls to implement to prevent unauthorized access or use of data based on a periodic assessment that considers several factors, including the sensitivity level and importance of adviser or fund information to its business operations, information systems access controls and malware protection, how information is stored and transmitted, and the potential effect of a cybersecurity incident involving adviser or fund information. The rules require that the cybersecurity policies provide for oversight of any service providers that receive, maintain, or process adviser or fund information or are permitted access to information systems.

Threat & vulnerability management

An adviser's or fund's policies and procedures must also include threat and vulnerability management and cybersecurity incident response and recovery. Firms must detect, mitigate, and remediate cybersecurity threats and vulnerabilities facing adviser or fund information systems. Policies and procedures should be reasonably designed to ensure the continued operations of the adviser or fund, the protection of adviser information systems and the adviser or fund information residing therein, and external and internal cybersecurity incident information sharing and communications.

Incident response & recovery

The proposed rules combine long-standing principles of incident response and business continuity to require policies and procedures to detect, respond to, and recover from a cybersecurity incident. Those policies and procedures should be reasonably designed to ensure the continued operations of the adviser or fund, the protection of the adviser's or fund's information systems and the information residing therein, external and internal information sharing and communications, and reporting significant cybersecurity incidents to the SEC. Consistent with its prior guidance, the SEC cites the NIST framework for incident response and recovery functions, and the proposed rules would require a formal, written documentation of the incident response and recovery actions.

Fund board oversight

As part of proposed Rule 38a-2, a fund's board of directors, including a majority of its independent directors, would be required to initially approve the fund's cybersecurity policies and procedures and to review the at-least annual written report on cyber-incidents and material changes to the fund's cyber-policies and procedures. The accompanying rule release emphasizes that "board oversight should not be a passive activity."

Reporting Significant Adviser Cybersecurity Incidents via New Form ADV-C

Advisers would further be required to notify the SEC about "significant cybersecurity incidents" in a new confidential Form ADV-C filing within 48 hours after having a reasonable basis to conclude that a significant adviser cybersecurity incident or a significant fund cybersecurity incident occurred or is occurring.

The definitions of "significant cybersecurity incident" for advisers and funds are similar and generally include a cybersecurity incident, or a group of related incidents, that (1) significantly disrupts or degrades the adviser's or fund's ability, or the ability of a private fund client of the adviser, to maintain critical operations; or (2) leads to the unauthorized access or use of adviser or fund information that results in substantial harm to the adviser, fund, a client, or an investor in a private fund whose information was accessed. In a footnote, the SEC indicates that it views "critical operations" to include investment, trading, reporting, and risk management of an adviser or fund, as well as operating in accordance with the federal securities laws. Substantial harm would include "significant monetary loss or the theft of personally identifiable or proprietary information."

Within 48 hours, advisers would be required to submit Form ADV-C and provide information that is responsive to both general and specific questions related to the significant cybersecurity incident, such as the nature and scope of the incident and the

adviser's response to the incident, including whether any disclosure has been made to any clients or investors. Form ADV-C would include a series of check-the-box and narrative questions, and it would be filed electronically through the Investment Adviser Registration Depository platform. Advisers need only share information available at the time of filing but would have an ongoing duty to supplement its filing as information becomes available.

Expanded Public Disclosure of Cybersecurity Risks and Incidents

The proposed amendments would require advisers and funds to publicly disclose cybersecurity risks and significant cybersecurity incidents that occurred in the last two fiscal years in their brochures and registration statements.

For advisers, the proposal would amend Form ADV Part 2A to require disclosure of cybersecurity risks and incidents to an adviser's clients and prospective clients. Advisers would be required to describe cybersecurity risks that could materially impact the services they offer. What is deemed "material" would be a factual determination on a case-by-case basis "if there is a substantial likelihood that a reasonable client would consider the information important based on the total mix of facts and information," consistent with well-established case law on materiality. The proposal further amends Rule 204-3(b) under the Advisers Act by requiring advisers to "promptly" deliver interim brochures about the incident to existing clients if it adds a cybersecurity disclosure or materially revises information previously disclosed about an incident.

Funds would also be required to provide a description of any significant fund cybersecurity incidents that have occurred in the last two fiscal years in their registration statements, tagged in a structured, machine-readable data language. Specifically, the proposal would require funds to provide a description of each significant fund cybersecurity incident, including, 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 any other unauthorized purpose; the effect of the incident on the fund's operations; and whether the fund or service provider has remediated or is currently remediating the incident.

Funds that have experienced multiple cybersecurity incidents may need to amend their prospectuses by filing a supplement with the SEC to disclose heightened cybersecurity risk as a principal risk of investing in the fund. The proposal further requires funds to include a general discussion of cybersecurity risks and significant fund cybersecurity incidents in their annual reports if they materially affected performance over the past fiscal year.

New Cybersecurity-Related Recordkeeping Requirements

The proposed rules would also require advisers and funds to adhere to new recordkeeping requirements that are designed to improve the availability of cybersecurity-related information. Specifically, advisers and funds would be required to maintain for five years records of: (1) cybersecurity policies and procedures; (2) annual reviews thereof; (3) documents related to the annual reviews; (4) regulatory filings related to cybersecurity incidents required under the proposed amendments (Form ADV-C filings for advisers and reports pursuant to proposed Rule 38a-2(a)(5) for funds); (5) the occurrence of any cybersecurity incident; and (6) cybersecurity risk assessments.

Key Takeaways

The cumulative effect of the proposed rules is to reinforce the notion of the adviser's and fund's accountability—to boards, to investors, to the SEC—for its overall cybersecurity preparedness, governance, and incident reporting. If adopted in their current form, the rules may be transformative for advisers and funds that may not have formalized their cybersecurity program to the degree required by the proposed rules and may require additional fine-tuning or alignment for firms that have pegged their cybersecurity program to other security standards or regulatory requirements. In addition, the formalized policies, procedures, and disclosures resulting from implementation of these rules may provide staff from the SEC's Examinations and Enforcement Divisions with an ample record to scrutinize and pose increased enforcement and litigation risks to SEC registrants. Nevertheless, in the aggregate, these proposed measures would more closely align the cybersecurity compliance and incident reporting obligations of SEC registrants with other federally regulated financial services companies.

You can subscribe to future ***Privacy, Cyber & Data Strategy*** and ***Investment Management, Trading & Markets*** advisories and other Alston & Bird publications by completing our **publications subscription form**.

If you have any questions or would like additional information, please contact your Alston & Bird attorney or any of the following:

Privacy, Cyber & Data Security Team

Kimberly Kiefer Peretti
202.239.3720
kimberly.peretti@alston.com

Katherine Doty Hanniford
202.239.3725
kate.hanniford@alston.com

Kellen Dwyer
202.239.3240
212.905.9340
kellen.dwyer@alston.com

Amy Mushahwar
202.239.3791
amy.mushahwar@alston.com

Investment Management, Trading & Markets Team

David J. Baum
202.239.3346
david.baum@alston.com

Kristin P. Hinson
704.444.1332
kris.hinson@alston.com

Megan Lau
+44.0.20.3907.1288
megan.lau@alston.com

Martin H. Dozier
404.881.4932
martin.dozier@alston.com

Colby B. Jenkins
704.444.1280
colby.jenkins@alston.com

Dustin J. Littrell
214.922.3475
dustin.littrell@alston.com

Blake E. Estes
212.210.9415
blake.estes@alston.com

Saloni Joshi
+44.020.3823.2197
saloni.joshi@alston.com

Timothy P. Selby
212.210.9494
tim.selby@alston.com

Timothy C. Foley
202.239.3741
timothy.foley@alston.com

Joel Jung
212.210.9564
joel.jung@alston.com

Helena Wong
212.210.9464
helena.wong@alston.com

ALSTON & BIRD

WWW.ALSTON.COM