MILLER CANFIELD

2023 Regulatory Update for Investment Advisers

January 11, 2023

In 2023, Registered Investment Advisers ("RIAs") who are registered with the Securities and Exchange Commission ("SEC") should be prepared for regulatory changes. These include proposed changes to rules governing RIA outsourcing and cybersecurity risk management. Although some key proposed rules are not yet final, RIAs should consider taking preliminary steps to prepare for the new requirements.

1. SEC Proposed Rules on Outsourcing by Investment Advisers

On October 26, 2022, the SEC proposed new rule 206(4)-11 and amendments under the Investment Advisers Act of 1940 (the "Act") to establish oversight obligations for RIAs that are outsourcing "covered functions" to third parties.

The proposed rule defines "covered functions" as functions that are: 1) necessary for the RIA to provide its investment advisory services in compliance with Federal securities laws; and 2) those that, if not performed or performed negligently, would be reasonably likely to cause a material negative impact on the RIA's clients or on the RIA's ability to provide investment advisory services.

The determination of whether an outsourced service provider performs a covered function is dependent on specific facts and circumstances; certain functions may be a covered function for one RIA but not for another. Examples of potentially covered functions may include client services, cybersecurity, investment guideline/restriction compliance, portfolio accounting, pricing, reconciliation, regulatory compliance, trade communication and allocation, and valuation. The proposed rule excludes clerical, ministerial, and general office functions.

The second element has a limiting effect and would require RIAs to assess which functions are reasonably likely to have a material negative impact on clients or the performance of advisory services, such as a material financial loss to a client, or material disruptions in the RIA's operations.

Before outsourcing covered functions, RIAs would be required to identify the nature and scope of the covered function, assess how to mitigate and manage potential risks, determine that the service provider has appropriate competence, capacity, and resources, assess the risks associated with subcontracting arrangements, obtain reasonable assurance that the provider will coordinate to comply with Federal securities laws, and obtain reasonable assurance that the provider has an orderly termination process for the covered functions.

Additionally, the proposed rules would require RIAs to retain specific records of due diligence assessment and monitoring during the term of the engagement and for five years thereafter. The SEC further proposes the addition of a new reporting item to Item 7 of Form ADV Part 1A, which would require RIAs to provide information on the third parties performing covered functions. If an RIA outsources record keeping to a third party, the RIA must ensure that those records can be accessed by the RIA and the SEC and protect the records against loss, alteration and destruction. The RIA may also need to periodically revisit its due diligence with respect to third parties providing covered functions.

2. SEC Proposed Rule on Cybersecurity Risk Management

Continued

In October 2022 the SEC also re-opened the comment period for proposed new Rule 206(4)-9 under the Act, and new Rule 38a-2 under the Investment Company Act of 1940, to require RIAs to implement and adopt written policies and procedures regarding cybersecurity risks.

RIAs would be required to adopt cybersecurity policies and procedures to periodically assess, categorize, prioritize and document cybersecurity risks, implement controls designed to minimize user-related risks and prevent unauthorized access to information and systems, monitor information systems and protect information from unauthorized access or use, detect, mitigate, and remediate cybersecurity threats and vulnerabilities, and detect, respond to, and recover from a cybersecurity incident. RIAs would need to review their cybersecurity policies and procedures at least once a year.

RIAs would also have to maintain certain documents for five years, including a copy of all cybersecurity policies and procedures, reports documenting the annual review of those policies and procedures, any Form ADV-Cs (discussed below), records documenting cybersecurity incidents, and records documenting the RIA's cybersecurity risk assessment.

RIAs would be required to report significant cybersecurity incidents, including on behalf of clients that are registered investment companies or private funds, to the SEC by filing proposed Form ADV-C within 48 hours. A significant cybersecurity incident is an incident that significantly disrupts or degrades the RIA's ability, or the ability of a private fund client to maintain critical operations, or that leads to the unauthorized access or use of client information resulting in substantial harm.

RIAs would be required to disclose information regarding cybersecurity risks and incidents that could materially affect the advisory relationship under new Item 20 of Form ADV Part 2A entitled "Cybersecurity Risks and Incidents." Additionally, RIAs would have to deliver interim brochure amendments to existing clients.

Because complying with the proposed rules, once in their final form, will take considerable effort, RIAs should begin assessing which outsourced functions would be deemed "covered functions" and start performing a risk analysis of pertinent third-party relationships. With respect to cybersecurity rules, RIAs should identify the major risks associated with information systems and start assessing how those risks can be effectively managed and mitigated.

Miller Canfield is prepared to assist RIAs in drafting new compliance policies and the necessary updates to the Policy and Procedures/Compliance Manual and Form ADV.