2024 INVESTMENT ADVISER ASSOCIATION COMPLIANCE CONFERENCE

March 6-8, 2024

Marriott Marquis, Washington, D.C.

OUTSOURCING & VENDOR DUE DILIGENCE

BUILDING A SUSTAINABLE PROGRAM

MICHAEL KOFFLER, PARTNER
CAROLYN A. GARCIA, ASSOCIATE
EVERSHEDS SUTHERLAND (US) LLP

TABLE OF CONTENTS:

I. Introduction

II. The SEC's Proposed Rule on Outsourcing by Investment Advisers

III. Rule 206(4)-7 under the Advisers Act

IV. Regulation S-ID: Identity Theft Red Flags

V. Commission Guidance

VI. Enforcement Cases

VII. Practical Tips

Appendix A – Sample Due Diligence Checklist

Appendix B – Sample Due Diligence Process

I. INTRODUCTION

Investment advisers engage third party vendors for a variety of reasons, including the advisers' limited expertise in performing certain functions, cost or time restrictions, a recognition that certain tasks can be more efficiently provided by a service provider and industry norms. Third party vendors are often utilized by advisers in such areas as finance and audit services, back or middle office services, best execution and quantitative analysis, business continuity planning, client relationship management, compliance, technology and cybersecurity, marketing, AML compliance, performance measurement, reporting, and verification, portfolio accounting and management, research and data, trade order routing and management, trading platform and custody services, trust services, and valuation/pricing.

When an adviser engages a vendor, the act of outsourcing the function to a third party does not relieve the adviser of its responsibility to satisfy the fiduciary obligations it owes to clients or to comply with applicable securities laws and regulations. Instead, when an adviser uses a vendor it "owns" the results achieved by the vendor – those results are, in effect, the adviser's results. Thus, an adviser does not escape liability for poor results that occur as a result of using a vendor.

Accordingly, while vendors can often perform various tasks more quickly, cheaply and efficiently than an adviser can, utilizing vendors subjects an adviser to operational, regulatory, reputational and legal risks. An effective due diligence program is therefore essential to protect an adviser against these risks. While no such program can eliminate these risks, a well-designed due diligence program can track and mitigate risks to a level at which they are acceptable. A well-designed due diligence program should not only seek to ensure compliance with business-oriented service level standards (as part of a Service Level Agreement), but also with the requirements applicable to the adviser under the Advisers Act[1] and other applicable securities laws. It is thus important for advisers to take the time and effort needed to (i) design and specify standards they seek to have vendors comply with and (ii) determine how to ensure vendors comply with such standards. As discussed below, these elements form the backbone of a well-designed due diligence program. Before discussing these elements, however, this outline first reviews some of the key principles and concepts underlying a vendor due diligence program.

II. THE SEC'S PROPOSED RULE ON OUTSOURCING BY INVESTMENT ADVISERS

In 2022, the U.S. Securities and Exchange Commission ("Commission") proposed Rule 206(4)-11 ("Proposed Rule")[2] under the Investment Advisers Act of 1940 ("Advisers Act"), which would prohibit Commission-registered investment advisers from outsourcing certain services or functions to service providers without meeting minimum requirements. The Commission also proposed certain related amendments to Rule 204-2 under the Advisers Act and to Form ADV. In justifying the new rule, the Commission cited concerns about (i) the risks to investors that may arise when an adviser outsources a function necessary for the provision of advisory services without appropriate adviser oversight; (ii) a lack of visibility into advisers'

[1] The Investment Advisers Act of 1940, as amended.
[2] Outsourcing by Investment advisers, IA-6176 (Nov. 16, 2022).

outsourcing practices and therefore into the extent of potential related risks to investors; and (iii) an adviser's improper oversight of third parties with respect to recordkeeping and books and records requirements. Importantly, the Commission stated that in its view, it is a *deceptive* sales practice and *contrary to the public interest and investor protection* for an investment adviser to hold itself out as an investment adviser while outsourcing functions that are necessary to its provision of advisory services to its clients without taking the appropriate steps to ensure that clients are provided the protections the adviser owes under its fiduciary duty and Federal securities laws.

A. Proposed Rule 206(4)-11

- **Covered Functions**: The Proposed Rule would establish an oversight framework across Commission-registered advisers that outsource a "covered function." A "covered function" is a function or service that: (i) is necessary to provide advisory services in compliance with the Federal securities laws, and (ii) if not performed or performed negligently, would be reasonably likely to cause a material negative impact on the adviser's clients or on the adviser's ability to provide investment advisory services. According to the Commission, the first element of this definition is satisfied by functions or services that are related to an adviser's investment decision-making process and portfolio management, such as providing investment guidelines, investment risk software or services, models related to investment advice, custom indexes, portfolio management or trading services or software, portfolio accounting services or sub-advisory services. In the release proposing the Proposed Rule the Commission noted that there is no bright line test as to what is a "covered function" and that certain functions may be covered functions for one adviser but not for another adviser. As a result, certain persons or entities that perform functions on behalf of advisers may be a service provider in the scope of the rule with respect to one adviser but not for another adviser.[3] The definition could include client services cybersecurity, reconciliation, regulatory compliance; trading desk, trade communication, allocation, pricing and valuation among others. Clerical, ministerial, utility, and general office functions or services are explicitly excluded. What is a "material negative impact" depends on the facts and circumstances, and could include a material financial loss to a client or a material disruption in the adviser's operations resulting in the inability to effect investment decisions properly.

- **Service Provider**: An investment adviser would be required to comply with the Proposed Rule if it retains a service provider. A "service provider" is defined as a person or entity that (i) performs one or more covered functions; and (ii) is not a supervised person of the adviser. It can be affiliated with the adviser or a third-party.

[3] For example, one adviser may choose to engage an index provider for the purposes of developing an investment strategy for its clients, which would be a covered function under the proposed rule, while another may license a widely available index from an index provider to use as a performance hurdle, in which case the proposed rule would not apply.

- **Due Diligence**: Before retaining a service provider to perform a covered function, an adviser would be required to reasonably identify and determine, through due diligence, that outsourcing the covered function and selecting that particular service provider is appropriate, considering (i) the nature and scope of the covered function; (ii) potential risks resulting from the service provider performing the covered function, including how to mitigate and manage such risks; (iii) the service provider's competence, capacity, and resources necessary to perform the covered function; (iv) the service provider's material subcontracting arrangements related to the covered function; (v) coordination with the service provider for Federal securities law compliance; and (vi) whether the service provider is able and willing to provide a process for the orderly termination of the performance of the covered function.

- **Monitoring**: The Proposed Rule would require an adviser to monitor its service providers with a manner and frequency such that the adviser reasonably determines that it is appropriate to continue (i) to outsource the covered function and (ii) to outsource to the service provider. According to the Commission, the manner and frequency of an adviser's monitoring would depend on the facts and circumstances applicable to the covered function, such as the materiality and criticality of the outsourced function to the ongoing business of the adviser and its clients.

- **Books and Records Requirements**: The Commission also proposed companion amendments to Rule 204-2 to require advisers to make and keep: (i) a list or other record of covered functions that the adviser has outsourced to a service provider, along with a record of the factors that led the adviser to list it as a covered function; (ii) records documenting the due diligence assessment; (iii) a copy of any written agreement with a service provider; and (iv) records documenting the periodic monitoring of a service provider. These records would be required to be maintained throughout the time period during which the adviser has outsourced a covered function to a service provider and for a period of five years thereafter.

B. Enhanced Oversight of Third-Party Record Keepers

- The Commission proposed to require an adviser that relies on a third-party recordkeeper to maintain books and records to conduct due diligence and monitoring of that third party consistent with the requirements under the Proposed Rule. As proposed, an adviser also would be required to obtain reasonable assurances that the third party will meet four standards, which address the third party's ability to (i) adopt and implement internal processes and/or systems for making and/or keeping records that meet the requirements of Rule 204-2; (ii) make and/or keep records that meet all of the requirements of Rule 204-2 applicable to the adviser; (iii) provide access to electronic records; and (iv) ensure the continued availability of records if the third party ceases operations or its relationship with the adviser ends.

C. Proposed Amendments to Form ADV

- The Commission proposed to amend Item 7 of Part 1A of Form ADV to require an adviser to disclose whether it outsources any covered function, and if so, to provide additional information on Schedule D. The proposed amendments would add Section 7.C. to Schedule D of Part 1A to require advisers to disclose the following for each service provider to which a covered function is outsourced: legal name, primary business name, legal entity identifier (if applicable), whether the service provider is a related person of the adviser, date the service provider was first engaged, location of the service provider's office primarily responsible for the covered function, and the covered function(s) that the service provider is engaged to perform.

D. Industry Comments. Industry participants have expressed concerns over the Proposed Rule.

The Proposal lacks an adequate explanation for a new comprehensive oversight regime

- While the Commission has identified certain potential shortfalls of outsourcing, it has failed to meaningfully identify substantial harms to the public necessitating the Proposal; instead, it bases the weight of its justification on a few examples of failed adherence to existing obligations where a service provider hired by an investment adviser did not properly fulfill its functions.
- The Commission observes in the Proposing Release that "[a]dvisers' fiduciary duty comprises a duty of loyalty and a duty of care, the latter of which includes providing investment advice in the best interest of the client, based on the client's objectives. . . ." And as one Commissioner noted, with respect to one example in the Proposing Release, "there is no discussion of whether and to what extent the mutual funds' investment advisers conducted oversight of the service provider in accordance with their existing obligations, and whether the specified oversight requirements contemplated by the proposed rule would have prevented or mitigated the problem."
- Accordingly, the Proposed Rule is not necessary as the existing regulatory framework under Rule 206(4)-7 already governs outsourcing activity. The Proposal is thus disproportionate to the harms identified by the Commission.

The Commission relies on an unfounded assumption

- The Commission effectively assumes there are greater risks requiring a new oversight regime if an adviser outsources a covered function. However, the reality often is that outsourcing is the *only* viable way an adviser can provide a covered function. Most SEC-registered advisers are small businesses operating from a single office, employing 50 or fewer people (88% in 2021) with the median investment adviser employing eight people. The median investment adviser with 8 employees typically does not have the competence, capacity and resources to provide all covered functions and will have to outsource at least one or some covered functions to a service provider. For many covered functions, the

only real question is which vendor should be selected to provide a covered function, since the adviser has no ability to provide a covered function itself.

The language of the Proposed Rule and the Proposing Release could cause the Commission staff to assess and second guess the merits of outsourcing decisions made by investment advisers

- Rather than state that the Proposed Rule was intended to ensure that investment advisers have a reasonable *process* by which to decide whether to outsource covered functions and to whom it should outsource such functions, the language in the Proposed Rule and the Proposing Release suggests the Commission staff would examine not only the process used by investment advisers to make outsourcing decisions but the *merits* of their decisions as well. For instance, the Proposed Rule would prevent an adviser from outsourcing covered functions unless an adviser "reasonably identifies, and determines that it would be appropriate to outsource the covered function and that it would be appropriate to select that service provider."
- This suggests that even if the process utilized by an adviser satisfies the conditions of the Proposed Rule, an adviser would violate the rule if it were to unreasonably *determine*, in the Commission's view, to outsource a given covered function or to select a given service provider. The language of the rule thus inappropriately requires the Commission staff to second guess the merits of the decisions made by advisers or to substitute its judgment of the outsourcing determinations made by investment advisers in order to conclude whether they are reasonable.

The Proposal's scope is significantly broader than the Proposing Release indicates

- The Proposing Release asserts that "[t]he proposed rule is designed to apply in the context of outsourcing core advisory functions." However, certain of the functions listed in the proposed revisions to Form ADV that are viewed by the Commission as being covered functions, such as client servicing, cybersecurity, portfolio accounting, reconciliation, regulatory compliance clearly fall beyond the plain meaning of "core advisory function."
- An investment adviser is defined in Section 202(a)(11) of the Advisers Act as "any person who, for compensation, engages in the business of advising others, either directly or through publications or writings, as to the value of securities or as to the advisability of investing in, purchasing, or selling securities, or who, for compensation and as part of a regular business, issues or promulgates analyses or reports concerning securities." A "core advisory function" is therefore a function that enables an adviser to (i) advise others as to the value of securities or as to the advisability of investing in, purchasing, or selling securities or (ii) issue or promulgate analyses or reports concerning securities.
- By characterizing such ancillary services (some of which are, in fact, middle office, back office or operational services) as "core advisory services" the Commission has, in a single stroke, materially changed the disclosure obligations of investment advisers such that a failure to provide full and fair disclosure of client servicing, cybersecurity, portfolio accounting, reconciliation, and

regulatory compliance practices (and the like) would constitute a material omission under the instructions of Form ADV and a violation of the anti-fraud provisions of Section 206 of the Advisers Act. Only those functions that relate to the provision of investment advice should be captured.

Violations of the Proposed Rule should not be deemed violations of Section 206(4) of the Advisers Act

- The Proposed Rule would be promulgated under Section 206(4) of the Advisers Act, which prohibits an adviser from engaging in "any act, practice, or course of business which is fraudulent, deceptive, or manipulative." Imposing the proposed oversight regime in reliance upon the anti-fraud rule of Section 206(4) of the Advisers Act means that if an adviser fails to strictly follow any of the Proposed Rule's prescriptions or is deemed to have made an unreasonable determination, the adviser could be deemed to have engaged in fraudulent, deceptive, or manipulative conduct. This would be the case even if the adviser's outsourcing policies and procedures were reasonably designed and even if the adviser was diligent in following those procedures.
- A finding of a violation under Section 206(4) could be catastrophic to an investment adviser; such severe consequences would be disproportionate as compared to the failure of such an adviser. Given the anti-fraud risk faced by advisers, it may be unclear how an adviser could be confident that it has done enough to comply with the Proposed Rule. In addition, the market for outsourced services and the relationships investment advisers have with their service providers will be significantly impacted by the possibility of incurring anti-fraud liability, such that the process of hiring and reviewing service providers will involve much more friction and expense.

The Commission has not sufficiently considered the impact on investment advisers that are themselves performing covered functions for other investment advisers

- Investment advisers performing covered functions for other investment advisers will become subject to more extensive and frequent due diligence requests if they are not excluded from the Proposed Rule.
- As the industry has moved to "open architecture" platforms in recent years, many investment advisers that serve as portfolio managers or model providers for investment strategies have sought to have their strategies and/or model portfolios available on as many investment advisory programs and platforms as possible. Similarly, sponsors of investment advisory programs (e.g., SMA, UMA and wrap-fee programs) and turn-key asset management platforms (commonly referred to as "TAMPs") have sought to increase the number of third party retail firms using the advisory programs available through the TAMP. It will therefore not be unusual to have dozens (or in certain cases, hundreds) of investment advisers conducting due diligence simultaneously on a given portfolio manager, model provider, investment advisory program sponsor or TAMP (collectively, "Platform Advisers").
- While the nature and amount of information requested will vary, it is fair to conclude that the type and amount of information requested under any final rule

will, on the whole, be much more extensive than what is typically requested or provided today, due to the regulatory pressures and risks that advisers conducting due diligence will face under any final rule that is substantially similar to the Proposed Rule.

- Further, the Commission doesn't appear to have considered how its rule would apply when investment advisory responsibilities are spread out over multiple advisers. For example, it's unclear how the Commission's proposal would work in a more complex scenario, such as when a retail adviser ("Adviser 1") hires a Platform Adviser as a service provider ("Adviser 2") to make available on Adviser 2's advisory platform, third party sub-managers and model providers that can be selected by Adviser 1 for Adviser 1's retail clients.

The Proposal creates significant interpretive issues

- The Proposed Rule is vague in a number of important respects. For instance, the scope of the definition of "covered function" is unclear. During the open meeting proposing the rule one Commissioner has observed that "almost any function outsourced by an investment adviser could trigger the numerous oversight functions set forth in the proposed rule," making it hard to distinguish between outsourced functions that fall within the two prongs of the Commission's proposed definition of covered function and those that do not.
- Similarly, because the definition of "service provider" is based on the definition of "covered function," it is similarly deficient. As proposed, the term "service provider" would include certain affiliates that provide certain shared services to the adviser or that operate as part of a single organization but are organized as separate legal entities. The proposed definition also includes other Commission registrants, such as broker-dealers and investment advisers, and financial institutions that are highly regulated by other federal or state regulators, such as broker-dealers, banks, credit unions and insurance companies. Adding an additional overlay of regulation to such registrants would provide little benefit.

The Proposal creates risks for investment advisers and will cause adverse, unintended consequences

- The Commission has sought to address the actions and omissions of service providers not regulated by the Commission and impact their behavior by crafting a rule that shifts liability for their acts or omissions to those entities (i.e., investment advisers registered or required to be registered with the Commission) over which it does have jurisdiction. And in doing so, the Proposed Rule effectively creates a standard of strict liability for investment advisers. Further, there are provisions in the rule text itself (and language in the proposing release) that increase the risk of violations by advisers and exacerbate the risks they will face. For instance, the proposed due diligence provision would require an adviser to obtain reasonable assurance from a service provider that it is able to, and will, coordinate with the adviser for purposes of the adviser's compliance with the Federal securities laws, as applicable to the covered function. A service provider is unlikely willing to revise its template service agreement to enable an adviser to satisfy the proposed reasonable assurance due diligence requirement.

- Because of the potential for liability created by the Proposed Rule, there is a risk that certain investment advisers will seek to provide certain functions themselves in situations where it would be better for that function to be outsourced.

- **The Proposed Rule should allow an exception for emergencies or risk constraining the adviser into breaching its duty of care**
  - Requiring the adviser to conduct all of the due diligence before the replacement service provider is engaged will be tantamount, in many cases, to requiring the adviser to breach its duty of care. If the adviser hires a new service provider immediately in order to prevent a loss of advisory service to its clients, it will violate the Proposed Rule (by failing to requirement to conduct due diligence before a service provider is engaged) and could be deemed to have committed fraud. If it waits to hire a new service provider until the due diligence is conducted, it may not be able to provide advisory services to its clients for an extended period of time and it will be in breach of its duty of care and its investment management agreements and its clients could be materially and irreparably harmed. Either way, the adviser will have violated its fiduciary obligations to its clients. The Proposed Rule should not force advisers to make such a choice. In many cases it simply will not be possible to complete the requisite due diligence for some period of time (and potentially for an extended period of time if the outsourced activity is complex). In such circumstances, if there is no exception for emergencies then the risk of an adviser concluding it cannot act quickly to help its clients (because doing so would trigger an enforcement action under the Proposed Rule) increases greatly if the risk of an enforcement action comes with the risk of a fraud charge.

III. RULE 206(4)-7 UNDER THE ADVISERS ACT[4]

Rule 206(4)-7 makes it unlawful for an investment adviser registered with the Commission to provide investment advice unless the adviser has adopted and implemented written policies and procedures reasonably designed to prevent violation of the Advisers Act and the rules thereunder by the adviser or any of its supervised persons.[5] The Commission has said that advisers should first identify conflicts and other compliance factors creating risk exposure for the adviser and its clients in light of the adviser's operations, and then design policies and procedures tailored to address those risks.[6]

A. Policies and Procedures

[4] See Compliance Programs of Investment Companies and Investment Advisers, 68 Fed. Reg. 74714 (Dec. 24, 2003) ("Adopting Release").

[5] Section 202(a)(25) of the Advisers Act defines "supervised person" to mean any partner, officer, director (or other person occupying a similar status or performing similar functions), or employee of an investment adviser, or other person who provides investment advice on behalf of the investment adviser and is subject to the supervision and control of the investment adviser.

[6] Adopting Release, at 74716.

- Policies and procedures should be designed to prevent violations from occurring, detect violations that have occurred and correct promptly any violations that have occurred.[7]
- Policies and procedures should employ, among other methods of detection, compliance tests that analyze information over time in order to identify unusual patterns.[8]
- Prevention should be a key objective of a firm's compliance policies and procedures.[9]

B. Annual Review

- Each adviser must review its policies and procedures annually to determine their adequacy and the effectiveness of their implementation.[10]
- Advisers should consider compliance matters that arose during the previous year, any changes in the business activities of the adviser or its affiliates, and any changes in the Advisers Act or applicable regulations.[11]
- Advisers should consider the need for interim review in response to significant compliance events, changes in business arrangements, and regulatory developments.[12]

Key Takeaways: The adopting release for Rule 206(4)-7 sets forth certain topics that must be included in investment advisers' policies and procedures, some of which involve products and services that advisers often outsource to third party vendors. As noted, advisers must adopt and implement written policies and procedures reasonably designed to prevent violation of Rule 206(4)-7 and the Advisers Act and this includes activities that are carried out by vendors. Accordingly, advisers that do not properly oversee vendors are subject to at least two regulatory risks (1) violations of the substantive provisions of the Advisers Act and the rules thereunder, such as the Proposed Rule on outsourcing and (2) violation of Rule 206(4)-7 (in addition to other risks such as reputational and operational risks).

IV. REGULATION S-ID: IDENTITY THEFT RED FLAGS

Reg S-ID[13] requires an adviser registered with the Commission to periodically determine whether it offers or maintains "covered accounts."[14] As a part of this determination, the adviser must conduct a risk assessment and take into consideration: (1) methods it provides to open

[7] Id.
[8] Id. at n. 15.
[9] Id. at n. 16.
[10] Id. at 74720.
[11] Id.
[12] Id.
[13] 17 C.F.R. 248.201et seq.
[14] A "covered account" is defined as an account that an investment adviser offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a brokerage account with a broker-dealer or an account maintained by a mutual fund (or its agent) that permits wire transfers or other payments to third parties and any other account that the investment adviser offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the investment adviser from identity theft, including financial, operational, compliance, reputation, or litigation risks. See 17 C.F.R. 248.201(b)(3).

accounts; (2) methods it provides to access accounts; and (3) previous experiences with identity theft. Reg S-ID also requires an adviser that offers or maintains one or more "covered accounts" to develop and implement a written identity theft prevention program that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. The identity theft prevention program must be appropriate to the size and complexity of the adviser and the nature and scope of its activities.

A. Overall Identity Prevention Program Requirements

- The identity theft program must include reasonable policies and procedures to:
  - identify relevant red flags for the covered accounts that the adviser offers or maintains, and incorporate those red flags into its program;
  - detect red flags that have been incorporated into the program of the adviser;
  - respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and
  - ensure the program (and relevant red flags) is updated periodically, to reflect changes in risks to clients and to the safety and soundness of the adviser from identity theft.

B. Reg S-ID Provisions Addressing Service Provider Arrangements

- Reg S-ID requires investment advisers to exercise appropriate and effective oversight of service provider arrangements.
- Relevant guidance explicitly states that firms subject to the rule must update their identity theft programs (and relevant red flags) periodically, to reflect changes in risks to customers or to the safety and soundness of the adviser, based on changes in the business arrangements of the adviser, including service provider arrangements.
- The guidance for Reg S-ID also requires firms subject to the rule to report to its board, an appropriate committee of its board, or a designated employee at the level of senior management, at least annually, on compliance related to Reg S-ID. Importantly, the guidance provides that the report must evaluate service provider arrangements, among other things.
- Whenever a financial institution subject to Reg S-ID engages a service provider to perform an activity in connection with one or more covered accounts the financial institution is expected under relevant guidance to take steps to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft. The guidance provides that a financial institution could require the service provider by contract to have policies and procedures to detect relevant red flags that may arise in the performance of the service provider's activities, and either report the red flags to the financial institution, or to take appropriate steps to prevent or mitigate identity theft

Key Takeaways: In order to comply with Reg S-ID, investment advisers' identity theft prevention programs must properly oversee vendors. Such compliance requires adopting

policies and procedures designed to detect, prevent, and mitigate identity theft that might occur as a result of vendors' activities. In addition, vendor agreements should clearly set forth the parties' responsibilities for managing the risk of identity theft created by the vendors' activities.

V. COMMISSION GUIDANCE

A. Division of Examinations 2024 Examination Priorities (October 16, 2023)[15]

- Areas of examination focus in fiscal year 2024 may include third-party service providers, among other things.
- Cybersecurity remains a perennial focus area. Given the continued elevation of operational disruption risks such as the proliferation of cybersecurity attacks, firms' dispersed operations, intense weather-related events, and geopolitical concerns, the Division will continue to review advisers' practices aimed to prevent interruptions to mission-critical services and to protect investor information, records, and assets. The Division will focus on registrants' policies and procedures, internal controls, oversight of third-party vendors (where applicable), governance practices, and responses to cyber-related incidents, including those related to ransomware attacks. With respect to third-party products and services in particular, the Division will continue to assess how registrants identify and address risks to essential business operations. The Division also will look at the concentration risk associated with the use of third-party providers, including how registrants are managing this risk and the potential impact to the U.S. securities markets.
- Examinations of advisers will continue to look at firms' practices to promote cyber resiliency. Reviews will include firm practices, policies, and procedures to prevent account intrusions and safeguard customer records and information, including personally identifiable information. Additional focus will be on the cybersecurity issues associated with the use of third-party vendors, including registrant visibility into the security and integrity of third-party products and services. The Division will also review whether there has been an unauthorized use of third-party providers.
- Among other items, the Division is also focused on advisers' policies and procedures for selecting and using third-party and affiliated service providers.

B. Division of Examination Risk Alert: Customer Records and Information at Branch Offices (April 26, 2023)[16]

- The Division issued a Risk Alert to highlight the importance of establishing written policies and procedures for safeguarding customer records and information at branch offices, which often lack these written policies despite being subject to the same or similar risks as the firm's main office. The Safeguards Rule of Regulation S-P (the "Safeguards Rule") requires firms to

[15] 2024 Examination Priorities Report located at https://www.sec.gov/files/2024-exam-priorities.pdf.
[16] Risk Alert: Safeguarding Customer Records and Information at Branch Offices (sec.gov).

adopt written policies and procedures addressing administrative, technical, and physical safeguards for the protection of customer records and information. These procedures must be reasonably designed to ensure the security and confidentiality of the same, protect against any anticipated threats or hazards, and protect against unauthorized access to or use of the information that could result in substantial harm or inconvenience to any customer.

- In assessing compliance with the Safeguards Rule, Division staff observed that in many instances, firms did not reasonably ensure that their branch offices performed proper due diligence and oversight of their vendors, or did not provide any guidance to assist branch offices in the selection. As these vendors provide services such as cybersecurity, technology operations, and business applications, this resulted in some weak security settings that put client records or information at risk.
- Similarly, firms often use vendors to provide email services. Division staff observed firms lacking policies and procedures addressing branch office email configurations, and often at the branch level these services were managed without the main office specifying the technical requirements adequate to secure the branch offices' email solution.

C. OCIE Report on Cybersecurity and Resiliency Observations (Jan. 27, 2020)[17]

- OCIE summarized its observations on industry practices and approaches to managing and combating cybersecurity risk and maintaining and enhancing operational resiliency.
- OCIE observed that practices and controls related to vendor management generally include policies and procedures for: (i) due diligence for vendor selection; (ii) monitoring and overseeing vendors and SLA terms; (iii) assessing ongoing risk assessment processes and the level of diligence to conduct on a vendor; and (iv) assessing how vendors protect client information.
- OCIE suggested that advisers: develop vendor management programs to ensure vendors meet security requirements and that appropriate safeguards are implemented; utilize questionnaires based on reviews of industry standards and independent audits; and establish procedures for terminating or replacing vendors.
- OCIE suggested that advisers understand vendor relationships, including understanding contract terms and understanding and managing the risks related to vendor outsourcing (e.g., use of cloud-based services).
- OCIE recommended vendor monitoring and testing. OCIE asserted that advisers should monitor vendor relationships to ensure that vendors continue to meet security requirements and to be aware of changes to vendors' services or personnel.
- Finally, OCIE recommended that advisers establish a vulnerability management program that includes routine scans of software code, web applications, servers

[17] https://www.sec.gov/files/OCIE%20Cybersecurity%20and%20Resiliency%20Observations.pdf.

and databases, workstations, and endpoints within the organization and third party providers.

Key Takeaways: Advisers should make sure that their vendor management practices and controls align with OCIE's cybersecurity observations, including initial and ongoing diligence to understand and manage risks related to vendor outsourcing and ensure that vendors meet advisers' security requirements.

D. OCIE Examination Priorities (Jan. 7, 2020)[18]

- OCIE noted that the footprint of registered entities has become more global and diverse, "often with an increased dependency on services and operations worldwide. The use of third-party service providers and other vendors by firms continues to increase, which can bring improved expertise and effectiveness, but also additional challenges and risks to organizations."
- OCIE stated it will continue to focus on third-party risk management in fiscal year 2020.
- In coordination with other Commission Divisions and Offices, OCIE will engage with firms on these risks, among others, to better assess the impact and compliance challenges.
- OCIE prioritized information security in each of its examination programs. Examinations will focus on, among other things, proper configuration of network storage devices, information security governance generally and retail trading information security.
- For advisers, OCIE focused examinations on assessing advisers' protection of clients' personal financial information. Particular focus areas will include, among other things, vendor management.
- With respect to third-party and vendor risk management:
  - OCIE staff focused on oversight practices related to service providers and network solutions, including those leveraging cloud-based storage.
  - OCIE staff reviewed for compliance with Regulations S-P and S-ID.
  - OCIE focused on the controls surrounding online access and mobile application access to client brokerage account information.
  - OCIE staff examined for the safeguards around the proper disposal of retired hardware that may contain client information and potential network information that could create an intrusion vulnerability.
- OCIE staff prioritized examining firms that utilize the services of third-party asset managers to advise clients' investments to assess, among other things, the extent of these firms' due diligence practices, policies, and procedures.

Key Takeaways: Advisers should be prepared for wide-ranging OCIE examinations regarding third party risk management. Examinations may focus on a host of issues, from proper configuration of network storage devices and information security governance, vendor management to compliance with Regulations S-P and S-ID to online access and mobile

[18] https://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2020.pdf.

application access to client account information to the proper disposal of retired hardware vulnerability. Importantly, OCIE's expectations are ongoing. Gone are the days of one time vendor reviews or "set it and forget it" approaches. Instead, firms would be well to incorporate the Japanese concept of "kaizen" or continuous improvement. Such an approach is premised on conducting ongoing due diligence and monitoring of vendors.

E. OCIE Risk Alert: Safeguarding Customer Records and Information in Network Storage – Use of Third Party Security Features (May 23, 2019)[19]

- During examinations, OCIE staff identified security risks associated with the storage of electronic client records and information by investment advisers in various network storage solutions, including those leveraging cloud-based storage.

- OCIE observed inadequate oversight of vendor-provided network storage solutions. In some cases, advisers did not ensure that the security settings on vendor-provided network storage solutions were configured in accordance with the firm's standards.

- OCIE recommended that firms implement a configuration management program that includes, among other things, vendor oversight to mitigate the risks incurred when implementing on-premise or cloud-based network storage solutions.

- OCIE also recommended that advisers adopt vendor management policies and procedures that include, among other things, regular implementation of software patches and hardware updates followed by reviews to ensure that those patches and updates did not unintentionally change, weaken, or otherwise modify the security configuration.

Key Takeaways: Advisers should actively oversee any vendors they use for network storage solutions to determine whether the service provided by the vendor is sufficient to enable the firm to meet its regulatory responsibilities. Among other things, this requires ongoing monitoring and testing to ensure the vendors: configure their solutions in accordance with the firm's standards; do not implement solutions that create security or other problems for the adviser; and regularly patch software and update hardware in a way that would not adversely impact the adviser's security configuration.

F. OCIE Risk Alert: Investment Adviser and Broker-Dealer Compliance Issues Related to Regulation S-P – Privacy Notices and Safeguard Policies (Apr. 16, 2019)[20]

[19] https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20Network%20Storage.pdf.
[20] https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20Regulation%20S-P.pdf.

- OCIE provided a list of compliance issues related to Regulation S-P that were identified in recent examinations of SEC-registered investment advisers and broker-dealers.

- OCIE staff observed firms with written policies and procedures that did not appear to be implemented or reasonably designed to: (1) ensure the security and confidentiality of client records and information; (2) protect against anticipated threats or hazards to the security or integrity of client records and information; or (3) protect against unauthorized access to or use of client records or information that could result in substantial harm or inconvenience to clients.

- With respect to outside vendors, advisers failed to follow their own policies and procedures for outside vendors. For example, OCIE staff noted that advisers failed to require outside vendors to contractually agree to keep clients' PII confidential, even though such terms were mandated by the advisers' policies and procedures.

Key Takeaways: Advisers must ensure that vendor agreements comply with the advisers' standards, policies and procedures.

VI. ENFORCEMENT CASES

A. In the Matter of Magnus Oppenheim & Co. Inc. (March 13, 2023)[21]

- **Facts:** From 2019 to 2021, Magnus Oppenheim adopted as its written compliance policies and procedures ("Compliance Manual") another investment adviser's compliance manual without removing references to the other adviser and failed to tailor the manual to its own business, including leaving in references to research analysts that it did not employ, and before then, Magnus Oppenheim's written compliance policies and procedures were principally oriented towards broker-dealer activities rather than the investment advisory business. Among other things, these policies and procedures referenced outdated regulatory guidance from the NASD and only mentioned the Advisers Act once. As such, the Compliance Manual did not include policies and procedures reasonably designed to prevent violations of the Advisers Act in areas that were relevant to the firm's business and operations, including policies and procedures involving conducting due diligence of third-party service providers, an area in which Magnus Oppenheim had been previously notified of deficiencies during the 2019 examination.

- Cost: Based on these and other violations, Magnus Oppenheim was ordered to pay $50,000 in civil penalties.

B. In the Matter of Barclays Capital Inc. (May 10, 2017)[22]

[21] E. Magnus Oppenheim & Co. Inc. (sec.gov)
[22] https://www.sec.gov/litigation/admin/2017/33-10355.pdf.

- Facts: From September 2010 through December 2015, Barclays Capital improperly overcharged certain advisory clients for advisory fees. In addition, from September 2010 through December 2014, Barclays Capital falsely represented to advisory clients that it was performing ongoing due diligence and monitoring of certain third-party managers that managed advisory clients' assets, when Barclays was not performing such due diligence. As a result, Barclays Capital improperly charged 2,050 client accounts approximately $48 million in fees for these promised services.

- Cost: Based on these and other violations, Barclays Capital was ordered to pay disgorgement, prejudgment interest, and a civil monetary penalty totaling over $90 million.

Key Takeaways: Adopting and implementing policies and procedures to perform initial and due diligence is not enough. Advisers also must ensure that their practices align with their policies and procedures and internal standards. In addition, advisers may not falsely represent due diligence practices or charge clients for due diligence they do not perform.

C. The "F-Squared Cases" (Aug. 25, 2016)[23]

- Facts: The Commission has announced a series of settlements against more than a dozen investment advisers found to have violated securities laws by disseminating false claims made by an investment adviser concerning the performance of its investment strategy. The Commission found that the advisers accepted and negligently relied on the performance information from F-Squared, and repeated many of F-Squared's claims while recommending an F-Squared strategy to their own clients without obtaining sufficient documentation to substantiate the information being advertised.

- Cost: The penalties assessed against the firms ranged from $100,000 to $500,000.

Key Takeaways: When an adviser uses a third party money manager's performance claims in its advertisements, the adviser has effectively adopted the performance claims as its own. As a result, advisers must perform due diligence on third party money managers and verify third party money managers' performance claims that the advisers plan on using or distributing.

D. In the Matter of Federated Global Investment Management Corp. (May 27, 2016)

[23] See e.g., SEC, Press Release, Commission Charges Investment Manager F-Squared and Former CEO With Making False Performance Claims (Dec. 22, 2014); SEC, Press Release, Mutual Fund Adviser Advertised False Performance Claims (Nov. 16, 2015); SEC, Press Release, Investment Advisers Paying Penalties for Advertising False Performance Claims (Aug. 25, 2016).

- Facts: Federated Global Investment Management Corp. ("FGIMC") served as the sub-adviser to the Federated Kaufmann Funds (the "Funds"). From approximately 2001 to 2010, FGIMC used a third-party consultant who worked closely with FGIMC and periodically provided analysis and buy, sell, and hold recommendations with respect to pharmaceutical and biotechnology stocks for the Funds. During the consulting relationship, the consultant also served on the boards of four public companies without disclosing this information to FGIMC's senior management or compliance department. In addition, the consultant had access to nonpublic information regarding the public companies, as well as information about the holdings of the Funds. While FGIMC had written policies and procedures regarding material nonpublic information and policies and procedures addressing the personal trading activities of individuals who had access to confidential information regarding the Funds, FGIMC did not establish or maintain written policies or procedures for identifying outside consultants who should be subject to oversight and controls carried out by its compliance department. As a result, FGIMC was unable to enforce fully the firm's written policies and procedures with respect to its use of and relationships with outside consultants to prevent the misuse of material nonpublic information and other confidential information.

- Cost: $1.5 million.

Key Takeaways: An investment adviser's policies and procedures should address the circumstances under which outside consultants should be subject to the adviser's oversight and controls as a result of their responsibilities, roles and access to material, nonpublic information or other confidential information of the firm.

E. In the Matter of Calhoun Asset Management, LLC (July 9, 2012)[24]

- Facts: Calhoun touted its due diligence capabilities in marketing materials and provided the materials to prospective and current investors. The materials described: the criteria for selecting managers; past performance; diversification in relation to other managers; assets under management; absence of significant conflicts of interest; overall integrity and reputation; percentage of business time devoted to investment activities; and fees charged. Calhoun also described a network of sources for identifying prospective managers. Calhoun represented that its due diligence included regular monitoring and performance reviews of managers, conducted at least monthly, along with periodic visits to managers. In materials available on its website, Calhoun stated, "we take every precaution necessary to complete thorough due diligence and research on every manager we recommend." Calhoun's actual due diligence was virtually nonexistent. Calhoun outsourced its due diligence obligations to a third party, and did not perform any due diligence on the third party or oversee the services it performed. The Commission found that Calhoun violated Section 206(4) of the Advisers Act and

[24] https://www.sec.gov/litigation/admin/2012/33-9333.pdf.

Rule 206(4)-8 thereunder by making false or misleading statements to, or otherwise defrauding, investors or prospective investors.

- Cost: The Commission assessed a $50,000 penalty and its principal and sole employee was barred from the brokerage and advisory industries.

Key Takeaways: Advisers' must not misrepresent their due diligence practices in marketing materials. Advisers have a duty to oversee any outsourcing of due diligence activities.

F. In the Matter of Morgan Stanley Investment Management, Inc. (Nov. 16, 2011)[25]

- Facts: Morgan Stanley Investment Management (MSIM) was the investment adviser for a closed-end fund. MSIM represented to investors and the fund's board of directors that the fund's sub-adviser was providing certain services that the sub-adviser, in fact, was not providing. As a result, the fund paid approximately $1.8 million to the sub-adviser between 1996 and the end of 2007 for advisory services it did not receive. In addition to violations of the Investment Company Act of 1940, the Commission found that MSIM violated: (1) Section 206(2) of the Advisers Act by representing that the sub-adviser was providing advisory services to MSIM for the benefit of the fund, and providing information to the fund board related thereto, when the sub-adviser was not; and (2) Section 206(4) of the Advisers Act and Rule 206(4)-7 thereunder by failing to adopt and implement reasonable procedures governing its oversight of the sub-adviser's services and its representations and provision of information to the board regarding those services in connection with the investment advisory contract renewal process.

- Cost: MSIM agreed to pay more than $3 million to settle the charges.

Key Takeaways: Advisers are responsible for making sure that sub-advisers provide contracted services.

VII. PRACTICAL TIPS

A. Compliance and Legal

- Check whether your contracts have provisions necessary to protect you, such as reps and warranties, notification of certain events (e.g., cybersecurity breaches), service level standards and consequences, key person provisions, operation and control standards, indemnification, standard of conduct, liquidated damages, provisions requiring the service provider not to disclose or use the protected information for any purpose other than as necessary to perform the subject services, language providing for an orderly transition of services to a third party, termination rights, access to books and records, an audit right etc.

[25] https://www.sec.gov/litigation/admin/2011/ia-3315.pdf.

- Ask yourself what happens if this vendor goes out of business tomorrow? What services and information will I lose access to? What is my back up plan? Am I able to continue to provide my core services to clients? What are my options? How long will it take to select and implement an option?
- Create a risk matrix for each service provider. What information do they have? What functions do they perform? How great is the risk to the firm and to clients if the vendor fails to provide adequate services?
- Create and map policies and procedures to the risk you have identified under your compliance manual. Incorporate vendor due diligence into your reviews under Rule 206(4)-7 under the Advisers Act.
- Take advantage of audit rights built into contracts and check on the performance of service providers. Ask for that policies and procedures are being performed as designed.
- Ensure your policies and procedures address roles and responsibilities for firm staff who supervise vendor activities and diligence and monitoring functions.
- Periodically review and update your firm's vendor management policies and procedures to reflect material changes in the firm's business or business practices.
- Consider whether governance changes may be appropriate for vendors (such as charging an enterprise wide risk management committee with oversight of the vendor management process).
- Periodically run Google searches on key vendors and their management.
- Document your due diligence of service providers. If you want to get the regulatory benefit from what you do, make sure you can demonstrate what you have done.
- If you can conduct reviews of vendors' processes in person, do so. You can often learn many important things from visiting a vendor on site and having them walk through their processes and their quality control efforts as compared to just reviewing documents sent to you via e-mail.
- Periodically review the standards in your SLAs and verify that they continue to be adequate to meet your fiduciary obligations to clients.
- Periodically review your marketing material to ensure such material is consistent with your use of vendors.
- Verify whether vendors' services satisfy your regulatory and contractual obligations under the Advisers Act. The services they provide have to meet your needs (and not merely be convenient for them).
- Ask for and review any reports service providers receive from third parties (e.g. SOC reports, business continuity plans, cybersecurity reports etc.).
- Create vendor-related due diligence forms that can be easily completed, reviewed (with documentation of such review), filed and maintained electronically.
- If operationally feasible, use such forms to obtain and track data points that can be analyzed for conducting trend analysis and scoring vendors.
- Review and make use of rankings of vendors in industry specific magazines, newsletters and rags.
- Run credit checks and BBB checks of vendors.

- Ask for and follow up on references provided by vendors during the due diligence process.

B. Vendor Onboarding

After completing due diligence and selecting a vendor, advisers should put in place a written contract with the vendor that addresses, among other things, both the firm's and the vendor's roles with respect to outsourced regulatory obligations.

Vendor Contracts[26]

- Does your firm document relationships with vendors in a written contract, and if not, under what circumstances?
- In addition to the contractual provisions mentioned above, do your firm's contracts address, when applicable, vendors' obligations with respect to such issues as (i) documentation evidencing responsible parties' and vendors' compliance with Federal securities laws and regulations; (ii) non-disclosure and confidentiality of information; (iii) protection of non-public, confidential and sensitive firm and client information; (iv) ownership and disposition of firm and client data at the end of the vendor relationship; (v) notification to your firm of cybersecurity events and the vendor's efforts to remediate those events, as well as notification of data integrity and service failure issues; (vi) vendor business continuity practices and participation in your firm's BCP testing, including frequency and availability of test results; (vii) disclosure of relevant pending or ongoing litigation; (viii) relationships between vendors, sub-contractors and other third-parties; (ix) firm and regulator access to books and records; and (x) timely notification to your firm of application or system changes that will materially affect your firm.
- Do your firm's contracts with vendors address roles, responsibilities and performance expectations with respect to outsourced activities or functions?

Features and Default Settings of Vendor Tools[27]

- Does your firm review, and as appropriate adjust, vendor tool default features and settings, to limit use of tools to specific firm-approved features, to set the appropriate retention period for data stored on a vendor platform or to limit data access—to meet your firm's business needs and applicable regulatory obligations?

C. Supervision[28]

[26] FINRA Regulatory Notice 21-29 located at https://www.finra.org/sites/default/files/2021-08/Regulatory-Notice-21-29.pdf.
[27] Id.
[28] Id.

Firms may wish to consider the following potential steps in determining how they fulfill their monitoring and oversight obligations:

- Obtaining covenants from the vendor in a contractual agreement that they are conducting self-assessments and undertaking the specific responsibilities identified;
- Requiring vendors to provide attestations or certifications that they have fulfilled certain reviews or obligations;
- Going onsite to vendors to conduct testing or observation, depending on the firm's familiarity with the vendor or other risk-based factors;
- Monitoring and assessing the accuracy and quality of the vendor's work product;
- Investigating client complaints that may be indicative of issues with a vendor and exploring whether there are further-reaching impacts; and
- Training staff to address and escalate red flags at your firm that a vendor may not be performing an activity or function adequately, such as not receiving confirmation that a vendor task was completed.

D. Initial Diligence

- Review the adviser's current policies and procedures to ensure they address the use of third party vendors, including due diligence, SLAs, approval processes, supervision, ongoing monitoring, risk assessment, remediation and termination.
    - **WHAT** functions will be outsourced?
        - Outline functions to be outsourced in policies and procedures.
        - Document criteria used and basis for decision.
        - Periodically review application of process to ensure consistent application of the criteria used.
    - **WHO** will conduct the diligence?
        - Consider whether diligence will be conducted by a single person or a committee of persons.
        - Decide whether the diligence will be outsourced to a third party in order to have an independent review.
        - Consider what internal parties should be involved (e.g., business, compliance, technology, and legal). Who are the relevant stakeholders?
        - Decide who will supervise the diligence process. Who will take "ownership" of the process?
    - **WHEN** will diligence be conducted?
    - **HOW** will diligence be conducted and documented?
        - Consider using a risk assessment that ranks vendors based on their level of risk (e.g., low, medium or high-risk).
        - When vendors are labeled high-risk, consider subjecting them to a more extensive due diligence process.
        - Consider the criteria that will be used to select a vendor.
        - Consider what documents will be requested from the vendor (e.g., policies and procedures, internal control documents,

regulatory forms, disciplinary history, risk assessment reports, organizational charts, financial statements and audits, business continuity plans, internal control reports and other testing results and security audits). Consider asking for and following up with references.
    - Research publicly available information on the vendor, its regulators and the regulatory requirements with which the vendor must comply. Search for complaints, lawsuits and other indications of problems.
    - Consider using background checks, checklists, questionnaires, and standardized forms and/or conducting interviews to find out about the vendor's background, experience, conflicts of interest, resources, data encryption practices, and disaster recovery practices.
    - Consider using third party reports and the reliability of such reports.
    - Request information on: (i) vendor personnel who will have access to the adviser's systems and client information; and (ii) how adviser and client information will be protected and stored.
    - Consider using a non-disclosure agreement ahead of any engagement in which confidential or sensitive information will be disclosed by the adviser to evaluate the vendor's services.
- Conduct due diligence reviews of any third party vendors prior to choosing to engage a vendor, including an assessment of the vendor's experience, reputation, operations, business continuity plan, and compliance programs.
- Visit the vendor to observe its operations and employees and speak with employees.
- Maintain a database of all third party vendors to track important dates, such as receipt of documents, review of documents, completion of diligence, receipt of reports, red flags, and follow-up items.

E. Establishing a Vendor Relationship

- Clearly define the vendor's responsibilities and consequences for breach of the agreement.
- Discuss and negotiate contractual provisions (e.g., data ownership, transference, destruction, audit clauses, inspection rights, use of subcontractors, reporting, confidentiality, technical standards, service levels, tiered penalties for breach, injunction clauses, specific performance provisions, bonuses for exceeding standards, use of escrow accounts, etc.) appropriate to the information and systems the vendor will have access to and the services the vendor will provide.
- Consider requiring (i) certain types of insurance; (ii) notifications of certain events (e.g., breach, loss of a letter of credit, merger or acquisition, filing of bankruptcy); (iii) strong indemnification provisions; (iv) the reporting of regulatory examinations or inquiries, litigation, or client complaints; and (v)

prior written approval for a delegation of duties or for an assignment of the contract to a third party.

- Consider including liquidated damages provisions upon the occurrence of certain events.
- Discuss what type of dispute resolution provision is appropriate.
- Consider including "key man" provisions.
- Consider requesting and reviewing audited financial statements of the vendor.
- Outline controls to ensure vendors are complying with applicable laws and the SLA.
- Specify how failures to satisfy applicable SLA standards will be handled in detail.
- Include supervision and oversight provisions in the SLA.

F. Ongoing Diligence

- Conduct ongoing due diligence reviews on a regular basis.
    - Consider more frequent reviews for critical vendors and those who have access to clients' PII or to critical firm systems.
    - Maintain a log for each vendor to track important dates, such as contract renewal and expiration, receipt of documents, review of documents, completion of diligence, receipt of reports, red flags, and follow-up items.
- Conduct regular vendor risk assessments to identify risks that may develop over time, based on business changes or regulatory changes, and assess how the vendor is managing risks.
- Consider and document the criteria that will be used when determining whether to renew a vendor. Consistently apply such criteria. Periodically assess and modify the criteria used, if appropriate.
- Request updated key documents from the vendor (e.g., policies and procedures, internal control documents, regulatory forms, references, disciplinary history, risk assessment reports, organizational charts, financial statements and audits, descriptions of new technologies, systems or processes, business continuity plans, and security audits).
- Request that the vendor certify that there are no material changes to information provided on questionnaires submitted previously.
- Evaluate (or obtain a copy of internal or external reports that assess) the vendor's compliance with federal securities laws and the SLA, identify any violations (red flags) that have occurred, and promptly address any violations that have occurred.
- Evaluate the vendors' services provided to the firm and its clients, and evaluate SLAs depending on business needs and regulatory requirements.
- Determine how client complaints related to the vendor will be addressed.
- Consider additional visits to the vendor to observe its operations and employees.
- Canvass stakeholders within the firm and ask them to assess the quality of the vendor and to rate the vendor.

- Record the diligence process and outcomes:
    - Document who participated in the process, the steps performed, the conclusions reached, any follow-up to be completed, and how red flags or concerns were addressed.
    - Recommend changes to a vendor's policies and procedures based on diligence process.

G. Review of Diligence Policies and Procedures

- Regularly review and update diligence policies and procedures to strive to improve the process.
- Compare actual practices against requirements set forth in the policies and procedures.
- Address weaknesses as they are detected.

H. Considerations On Terminating a Vendor Relationship

- Retrieving adviser and client data from vendor systems.
- Disposing of adviser and client data on vendor systems.
- Removing vendor software from adviser systems.
- Terminating vendor access to adviser systems.
- Ensuring compliance with Advisers Act recordkeeping rules.

Appendix A – Sample Due Diligence Checklist

- **Background Information**
  - History
  - Mission & philosophy
  - Culture
  - Ownership
  - Capital structure
  - Affiliates (including broker-dealers, investment advisers, custodians, administrators and other financial services companies)
  - Growth objectives
  - Significant changes to operations (mergers, acquisitions, joint ventures, management, new products) in last few years
  - E&O insurance, D&O insurance, fidelity bond insurance
  - Disciplinary history (criminal, civil, regulatory matters, including any pending matters)
  - SEC filings and other regulatory disclosure documents
  - SEC investigations and disqualifications
  - Financial statements (audited)

- **Personnel**
  - Senior management
  - Service provider team dedicated to adviser
  - Description of responsibilities
  - Training and education programs
  - Biographical information (including education, licensing, certifications, experience)
  - Compensation and incentive programs
  - Organizational chart
  - Background checks
  - SEC investigations and disqualifications
  - Recent changes in key personnel (departures or additions)
  - Anticipated changes in key personnel (departures or additions)
  - Major organizational changes
  - Succession plans for key personnel

- **Products and Services**
  - Current products/services offered
  - Compare to competitors
  - Marketing materials
  - Client base overview
  - Top 10 clients
  - Client agreements
  - Client complaints
  - Vendor and service provider agreements and due diligence policies and procedures

- References
- Third party ratings, awards

- **Technology**
  - Policies and procedures
  - Physical controls for technology
  - Security documents, including data flow diagrams, system and network architecture
  - Cybersecurity
    - Policies and procedures to manage and monitor risk environment and operational requirements
    - Information security policy
    - IT Acceptable Use Policy
    - Identified security roles and responsibilities and alignment of internal roles and external partners
    - Governance and risk management processes address cybersecurity risks
    - Incident Response Plan and Recovery Plans
      - Are Incident Response Plans/Recovery Plans tested?
      - Results of tests?
      - Are incident alert thresholds established?
    - Training program
    - Internal controls and protocols for identity theft
    - Access controls
      - Is remote access secure?
      - Is remote access managed?
      - Are access permissions managed?
    - Integration
    - Periodic assessments
    - Experience of IT staff
    - Documented privacy controls
    - Logging/Review
      - Network activity and event logging solution
    - Communications monitoring
    - Data destruction policy
      - Is data destroyed according to policy?
    - Employee termination checklist
    - Are identities and credentials managed for authorized devices and users?
    - Are physical access to assets managed and protected?
    - Is network integrity and data protected?
      - Are integrity checking mechanisms used to verify software, hardware and information integrity?
    - Are backups of information created, maintained and tested periodically?
    - Are removable media protected and their use restricted?
    - Antivirus
    - Encryption
    - Firewalls

        - Intrusion detection systems
            - Are the network, physical environment and personnel activity monitored to detect cybersecurity events (malicious or unauthorized code, unauthorized personnel, connections, devices and software)?
            - Is service provider activity monitored to detect cybersecurity events?
            - Are vulnerability scans performed?
            - Are detection processes tested?
            - Are detected events analyzed and impact determined?
        - Patch management program
        - Web filtering
        - Is a baseline of network operations and data flows for users and systems established and maintained?
        - How does the vendor make it easy for you to monitor their activities on your network?
    - Business continuity plans and records of recent testing

- **Compliance**
    - Chief Compliance Officer (CCO)
        - CCO background and expertise
        - CCO responsibilities and compensation
        - Reporting lines
        - Compliance organizational chart
        - Changes to compliance personnel
        - Independence
    - Compliance resources (staffing, resources)
    - Policies and procedures (including notes on reasons for recent changes and additions)
    - Compliance culture
    - Risk assessments
    - Testing of compliance program, testing, material compliance violations
    - Third party reviews
    - Compliance certifications
    - Internal disciplinary actions
    - Code of Ethics
    - Privacy Policy

Appendix B – Sample Due Diligence Process

A. Document Development & Maintenance

1. Initial Vendor Questionnaire

    a. Development of Initial Vendor Questionnaire: develop vendor questionnaire that addresses key factors to be considered by Due Diligence Team:

        1) Due Diligence Team Chair and team jointly identify issues that should be addressed by the due diligence process.

        2) Due Diligence Team Chair drives development of Initial Vendor Questionnaire, ensuring that intended content will provide the basis for a thorough due diligence review.

        3) Due Diligence Team Chair (with support of Due Diligence Team) reviews Initial Vendor Questionnaire to confirm that it will provide a reasonable framework for gathering necessary information from a vendor.

    b. Continuous Maintenance of Initial Vendor Questionnaire – Due Diligence Team Chair will periodically review and enhance the Initial Vendor Questionnaire to make it more effective and efficient:

        1) Add questions as new factors are identified, industry trends evolve, or regulatory requirements change.

        2) Revise questions to make them clearer.

        3) Eliminate questions that provide little value or cannot be reasonably addressed by vendors.

2. Due Diligence Report Template

    a. The Due Diligence Report Template is intended to provide:

        1) Concise summary of the findings.

            a) Product/Services description

            b) Benefits

            c) Key Risks

        2) Presents key details in an organized manner.

        3) Ensures key issues are considered by Due Diligence Team.

        4) Encourages consistent due diligence analysis.

            a) from vendor to vendor

b) from Due Diligence Team Member to Due Diligence Team Member

5) Checklist to identify topics that may require further investigation.

6) Documentation to show key issues were considered by Due Diligence Team.

7) Format allows reports to be presented and reviewed in a consistent manner.

b. Initial Report Template Development:

1) Due Diligence Team Chair and team jointly identify issues that should be addressed by the due diligence process.

2) Due Diligence Team Chair drives development of the report template, ensuring that all potentially important topics are addressed.

3) Due Diligence Team reviews report template to confirm that it will provide a reasonable framework for reviewing materials and performing a thorough due diligence evaluation.

4) Not all factors identified in the Initial Report Template will be relevant or feasible to address for all products and services so various factors will not be addressed because they are not relevant or reasonably available.

5) Due Diligence Team Member may remove sections from final report template if they do not add value to the analysis and report.

c. Continuous Report Template Maintenance – Due Diligence Team Chair will periodically review and enhance the report template to make it more effective and more efficient:

1) Add sections as new factors are identified, industry trends evolve, or regulatory requirements change.

2) Reformat sections so that they are clearer.

3) Eliminate questions that provide little value or cannot be reasonably addressed by due diligence.

B. Initial Due Diligence

1. Business Unit Leader provides due diligence request and necessary information to Due Diligence Manager:

a. Business Unit Leader addresses key issues and factors relating to proposed vendor.

b. Business Unit Leader discusses priority with Due Diligence Manager to determine priority and reasonable expectations for completion.

c. Business Unit Leader will revise Due Diligence Team priorities as necessary to reasonably meet expectations.

2. Due Diligence Team may provide assistance to Business Unit in assessment of potential vendors, such as:

    a. Provide a template or checklist to help Business Unit evaluate key factors when assessing potential vendor candidates.

    b. Provide brief research to Business Unit summarizing the potential merits and risks of potential vendor candidates.

C. Gathering Due Diligence Information – The Due Diligence Team will:

1. Send Initial Vendor Questionnaire to Vendor Contacts.

    a. Contacts provided by Business Unit.

    b. Due Diligence Team Member may communicate with vendor to set mutual expectations.

    c. Due Diligence Team Member receives completed Initial Vendor Questionnaire and related materials from vendor.

2. Due Diligence Team Member may conduct preliminary review of Initial Vendor Questionnaire and related materials, as necessary.

    a. Review for significant omissions.

    b. Review key topics for completion and clarity of responses.

    c. Share preliminary findings with Business Unit.

        1) Continue as planned.

        2) Re-prioritize.

        3) Cancel diligence if apparent vendor will not meet due diligence or business requirements.

3. Due Diligence Team may submit follow-up questions to vendor when key information has been omitted, responses are not clear or the material provided raises new questions.

4. Due Diligence Team may conduct independent research if necessary to validate key information provided by vendor.

    a. Confirm key pieces of information provided by vendor.

    b. Supplement vendor information with details from independent research.

5. Due Diligence Team may conduct independent investigation, if necessary, to gain further understanding of the vendor and its products/services.

    a. News items, background information, and headline risks.

    b. Regulatory, criminal, and civil events.

c. Key aspects of vendor and its products/services.

d. Competitors and market research.

e. Review of third party reports, if available.

f. Interview references/existing clients of vendor.

D. Reviewing Due Diligence Information

1. Review of due diligence materials:

a. Vendor business model and organizational structure.

b. Infrastructure and resources available.

c. Key leadership and investment personnel:

1) Academics and professional experience

2) Appropriate capacity and experience

3) Succession concerns

4) Turnover

d. Products, services, philosophy and processes:

1) Reasonable philosophy (i.e., is it consistent with business needs?)

2) Reasonable approach

a) Strategies

b) Processes, methodology and implementation

c) Reasonable resources and staffing

d) Financial strength/liquidity/viability

e) Transparency

e. Risk Management

1) Ongoing monitoring

2) Results of testing

f. Performance

1) Reasonable relative to benchmark or peers

g. Back Office

1) Compliance supervision and ethics

2) Operations

2. Key Findings and Risks Identified
    a. Key Findings
    b. Key risks identified or “red flags”
        1) Risks related to vendor type
            a) Compliance
            b) Legal
            c) Reputational
            d) Other
        2) Risks of vendor under review
        3) Risks pertaining to firm infrastructure and viability of vendor
        4) Risks relating to clients
        5) Risks relating to business
        6) Risks from a compliance/supervision perspective
        7) Risks relating to operations
3. Due Diligence Review Process (subject to the discretion of Due Diligence Team Member)
    a. Review of all materials
    b. Additional information & research
        1) Vendor follow-up and information requests
        2) Independent research and analysis, as necessary
    c. Initial Due Diligence Report
        1) Thorough review of all key factors
            a) All key factors addressed
            b) Identify inconsistencies
            c) Irrelevant topics not addressed
            d) Identify factors that require further investigation
        2) Input information into Initial Due Diligence Report
            a) Summarize relevant information and input into Initial Due Diligence Report

b) Indicate whether item was addressed or add detailed information when required for reporting purposes (additional details may be found in vendor file)

c) Indicate "not applicable" if the item is not relevant to vendor

d) Indicate "not available" if item was not provided and may not be reasonably available

3) Review Initial Due Diligence Report

a) Identify topics that have not been adequately addressed and conduct appropriate investigation

b) Identify potential "red flags":

c) Identify key findings and present in Initial Due Diligence Report:

(i) Key vendor attributes

(ii) Key vendor risks

(iii) Potential business concerns

(iv) Other

d) Conduct final review on Initial Due Diligence Report for accuracy & completeness

4) Complete Initial Due Diligence Report

4. Submit completed Initial Due Diligence Report to Business Unit

a. Brief Business Unit Leader with key findings and risks identified

b. Assist with the review of agreements to ensure that they are consistent with due diligence understanding of the vendor, as necessary.

c. Provide insight and support to Business Unit Leader for recommendations and supporting materials to Vendor Management Committee.

d. At the Vendor Management Committee meeting, Due Diligence Team Member may support the Business Unit Leader with technical expertise.

e. Assist with the development of policies & procedures and the development of any other materials, as necessary.

5. Document completed due diligence review

a. Maintain due diligence vendor files, which include:

1) Completed Initial Due Diligence Report

2) Supporting materials

3) Relevant communications and answers to follow up questions

E. Exceptions to Initial Due Diligence Process

1. Exceptions may be made for business reasons, as determined by senior management.
    a. Persons who may request due diligence exception:
        1) President
        2) Vice President of Business Unit requesting vendor diligence
        3) Other
2. Reasons for an exception:
    a. Known vendor
    b. Cost-benefit analysis
3. Due Diligence Exceptions:
    a. Limited due diligence
    b. No due diligence

F. Ongoing Due Diligence

1. Purpose: confirm accuracy of due diligence information previously obtained
2. Identify key changes to vendor since prior due diligence review
    a. Vendor and products/services
    b. Philosophy and processes
    c. Organization and infrastructure
    d. Key personnel
    e. Performance (contracted services and relative to peers/industry benchmarks)
    f. Regulatory developments
    g. Marketplace/industry position
    h. Pricing
    i. Technology/systems
    j. Geographic footprint

3. Frequency: at least annually (may be more frequent depending on vendor's risk profile)

G. Send Ongoing Vendor Questionnaire

1. Similar to Initial Vendor Questionnaire
2. Subject to revision
    a. May be abbreviated
    b. Allow vendors to "cut & paste" static information
3. Sent annually (may be more frequent depending on vendor's risk profile)

H. Review Ongoing Due Diligence Materials

1. Receive & review Ongoing Vendor Questionnaire
    a. Review for significant omissions
    b. Review key topics for completion and clarity of responses
    c. Identify inconsistencies
    d. Identify new issues
    e. Identify red flags
2. Additional follow-up with vendor on particular issues

I. Ongoing Due Diligence Report Template

1. Substantially similar to Initial Due Diligence Report Template
2. Subject to revision
    a. May be abbreviated
    b. Will "cut & paste" static information
3. Completed annually (may be more frequent depending on vendor's risk profile)
    a. Final report provided to Business Unit Leader
    b. Findings presented in summary format to Vendor Management Committee
    c. Maintained in vendor's due diligence file

J. Semiannual Performance Review

1. Performance Request
    a. At least semiannual performance review of vendor based on performance benchmarks may be requested from Business Unit or Vendor Management Committee.

b. Performance information is input into template to determine whether vendor outperformed performance objectives.

c. Summary of performance review is provided to Business Unit or Vendor Management Committee:

    1) Semiannual basis (may be more frequent depending on vendor's risk profile)

    2) Significant findings highlighted to Business Unit or Vendor Management Committee

    3) Maintained in vendor's due diligence file and with Business Unit or Vendor Management Committee notes