

# 2024 / Investment Adviser Compliance Conference

MARCH 6-8 / WASHINGTON, DC

**EFFECTIVE STRATEGIES & BEST PRACTICES**

IAA

## Ethics for Advisers: Compliance with Fiduciary Standards – Part 1

Max Mejiborsky / COMPLY

Kim Versace / National Real Estate Advisors, LLC

Steven A. Yadegari / Chief Executive Officer, FiSolve

A. Valerie Mirko / Armstrong Teasdale LLP (Moderator)

1

IAA

2024 / Investment Adviser  
Compliance Conference

**EFFECTIVE STRATEGIES  
& BEST PRACTICES**

## Agenda

- Fiduciary Duty – 2019 Standard of Conduct Interpretation
- Requirements of Rule 204A-1 and Rule 17j-1
- Operational challenges:
  - Defining Access Persons
  - Households / Held Away Accounts
    - Generic codes
  - Preclearing
  - Recordkeeping
  - Escalation

2



## Investment Adviser Standard of Conduct

The SEC Interpretation (commonly referred to as the Investment Adviser Standard of Conduct) outlines the fiduciary duty into two main components:

- Duty of Care –
  - Duty to provide advice in best interest of the client
  - Duty to seek best execution
  - Duty to provide advice and monitoring
- Duty of Loyalty
  - Clients' interests ahead of the adviser
  - Full and fair disclosure of material facts
  - At minimum, full and fair conflicts disclosure and also consider mitigation or elimination

3



## Rule 204A-1 Requirements

At a minimum, a Code of Ethics must:

1. Include a standard of conduct.
2. Require compliance with federal securities laws.
3. Require personal trading reports by access persons.
4. Require supervised persons to report any violations of the Code.
5. Require certification of compliance by supervised persons.
6. Require access persons to obtain preapproval before acquiring ownership in any security in an initial public offering or in a limited offering.

4



## Rule 17j-1 Requirements

- Like Rule 204A-1, Rule 17j-1 requires funds and each investment adviser and principal underwriter of a fund to “adopt a written code of ethics containing provisions necessary to prevent its Access Persons” from engaging in certain fraudulent, manipulative, and deceptive actions.
- The Fund board of directors/trustees must approve the Code.
- Code must include procedures such as access person reporting, annual reports to the board, report reviews, preclearance, disclosures etc.

5



## Practical Challenge – Identifying Access Persons

“Access person” means supervised persons who either:

- (i) have access to nonpublic information regarding clients’ purchase or sale of securities,
- (ii) are involved in making securities recommendations to clients, or
- (iii) have access to recommendations that are nonpublic.

Directors, officers and partners of an investment adviser whose primary business is giving investment advice are presumed to be access persons.

But what about consultants? Given that “Access Person” is defined as a subset of “Supervised Persons,” can we assume the consultant is not an “Access Person” if that person is not a “Supervised Person”?



6



## Practical Challenge – Households / Held Away Accounts

Access person presumed to have beneficial ownership of securities held by immediate family members residing in the same household.

- Immediate family members include any child, stepchild, grandchild, parent, stepparent, grandparent, spouse, sibling, close in-laws, and adoptive relationships.

What children away at college but legal residence is still at home?

What about interns?

What about new hires living at home?

7



## Practical Challenge – Generic Codes

In a recent action, the SEC staff messaged against an investment management firm for adopting a “*wholesale*,” “*off-the-shelf*” code of ethics from an outside trade organization with no applicability to the firm’s own business.

- How can advisers tailor their Codes to align with their business model?

8



## Practical Challenge – Preclearance

Code must include a requirement that its access persons obtain prior authorization before investing in an IPO or private placement.

- What other transactions should be precleared?
- What ways can an adviser take a more risk-based approach?

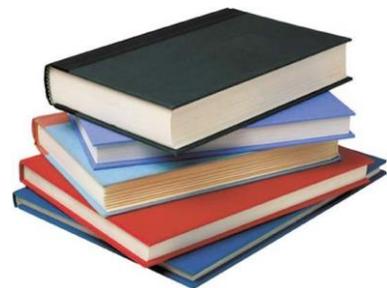


9



## Practical Challenge – Recordkeeping

- Should advisers keep a separate Code of Ethics, or should it be a part of their broader policy manuals?
- At what point should an adviser start implementing software and other systems for tracking purposes?



10



## Practical Challenge – Escalation

- What are the penalties with escalation and what do you do?
- What happens if someone in the C-suite violates the Code?



11



## Other Considerations



- Outside Business Activities.



- Gifts and Entertainment.



- Political Contributions.

12

# 2024 / Investment Adviser Compliance Conference

MARCH 6-8 / WASHINGTON, DC

**EFFECTIVE STRATEGIES  
& BEST PRACTICES**

IAA

# Ethics for Advisers: Compliance with Fiduciary Standards Spotlight on Code of Ethics Requirements

Investment Adviser Association 2024 Compliance Conference, Washington, DC  
March 6-8, 2024

A. Valerie Mirko, Partner &  
Leader, Securities Regulation and Litigation Practice, Armstrong Teasdale LLP<sup>1</sup>

Margaret Mudd, Partner  
Armstrong Teasdale LLP

Noelle Mack, Associate  
Armstrong Teasdale LLP

Rule 204A-1 under the Investment Advisers Act of 1940 (the “Advisers Act”), also known as the Code of Ethics Rule, is a long-standing Securities and Exchange Commission (“SEC”) rule that governs the activities and ethics of associated persons of investment advisers. The SEC adopted Rule 204A-1 to promote compliance with fiduciary standards by advisers and their personnel. At the time, there had been an increasing number of enforcement actions involving violations of fiduciary duties to clients, leading in turn to rulemaking.

Rule 204A-1 specifically requires investment advisers to adopt a code of ethics that sets forth standards of conduct expected of advisory personnel and addresses conflicts that arise from personal trading by advisory personnel. One of the policy goals of Rule 204A-1 is to prevent the possibility of fraud by reinforcing fiduciary principles that govern conduct of investment adviser firms and their personnel. Therefore, as the SEC’s pronouncements on fiduciary principles has evolved through the years, Rule 204A-1 compliance benefits from greater guidance.<sup>2</sup> To this end, we also briefly address in this summary the 2019 Commission Interpretation Regarding Standard of Conduct for Investment Advisers to provide further context relevant to Rule 204A-1 compliance.<sup>3</sup> Furthermore, as with all aspects of long-standing Advisers Act compliance, advisers should review and update code of ethics requirement to respond to both regulatory and market developments. This includes both developments like the Interpretation and emerging areas, such as crypto.<sup>4</sup>

---

<sup>1</sup>This material is provided for informational purposes only and does not constitute legal advice or create an attorney-client relationship. This may qualify as “Attorney Advertising” requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.

<sup>2</sup> The scope of this summary is generally limited to code of ethics requirements. There are other components to fiduciary duties that are important to consider when developing, implementing, and enforcing a code of ethics. For further discussion see A. Valerie Mirko and Margaret Mudd, *Fiduciary Obligations for Identifying, Managing, and Disclosing Conflicts of Interest* (Sept. 1, 2023) (“2023 Conflicts Outline”).

<sup>3</sup> *Commission Interpretation Regarding the Solely Incidental Prong of the Broker-Dealer Exclusion from the Definition of Investment Adviser*, Investment Advisers Act Release No. 5249, 84 FR 33681 (Jul. 12, 2019) (“Interpretation”). Note that the Commission intended this to be a restatement of existing fiduciary principles.

<sup>4</sup> See 2024 Examination Priorities Report, SEC Division of Examinations (Oct. 16, 2023), available at <https://www.sec.gov/files/2024-exam-priorities.pdf>. In our experience, code of ethics deficiencies are often

## 1. Rule 204A-1 Overview and Code Requirements

Under federal law, investment advisers must have policies and procedures in place reasonably designed to prevent the misuse of material nonpublic information by investment advisers and persons associated with the investment adviser.<sup>5</sup> Specifically, Rule 204A-1 requires that all investment advisers registered or required to be registered with the SEC adopt, maintain and enforce a written code of ethics reflecting the adviser’s fiduciary duties to its clients. At a minimum, an adviser’s code of ethics must contain the following:<sup>6</sup>

- A standard (or standards) of business conduct that the investment adviser requires of supervised persons,<sup>7</sup> which must reflect both the investment adviser’s fiduciary obligations and the supervised persons’ fiduciary obligations.
- Procedures requiring supervised persons to comply with applicable federal securities laws.
- Procedures that require all access persons to report,<sup>8</sup> and the investment adviser to review, all personal securities transactions and holdings periodically.
- Procedures requiring supervised persons to report any violations of the code of ethics promptly to the Chief Compliance Officer (“CCO”) or, provided the CCO also receives reports of all violations, to other persons designated in the code of ethics.
- Procedures for distributing copies of the code of ethics and any amendments to each supervised person and requiring supervised persons to provide written acknowledgement of their receipt of the same.

Several provisions of Rule 204A-1 are modeled after Rule 17j-1 under the Investment Company Act. Like its Advisers Act counterpart, Rule 17j-1 requires funds and each investment adviser and principal underwriter of a fund to “adopt a written code of ethics containing provisions necessary to prevent” certain persons affiliated with the fund, its investment adviser or its principal underwriter from engaging in fraudulent, manipulative, and deceptive actions with respect to the fund.<sup>9</sup> Rule 17j-1 further requires that investment companies use reasonable diligence and institute procedures reasonably necessary to prevent violations of the code.<sup>10</sup> Any access person who acquires direct or indirect beneficial ownership of any security as defined in the rule is required to

---

addressed in the SEC exam context, though we note in this document certain recent enforcement actions and key takeaways on those.

<sup>5</sup> 15 U.S.C. § 80b-4a.

<sup>6</sup> 17 C.F.R. § 275.204A-1(a).

<sup>7</sup> “Supervised person” means: (i) a partner, officer, director (or other person occupying a similar status or performing similar functions); (ii) an employee of an investment adviser; or (iii) a person who provides investment advice on behalf of the investment adviser and is subject to the supervision and control of the investment adviser. 15 U.S.C. § 80b-2(a)(25).

<sup>8</sup> Rule 204A-1 defines “access person” as any supervised persons who either (A) have access to nonpublic information regarding clients’ purchase or sale of securities, or (B) are involved in making securities recommendation to clients or have access to such recommendations that are nonpublic. Directors, officers and partners of an investment adviser whose primary business is giving investment advice are presumed to be access persons. 17 C.F.R. § 275.204A-1(e)(1). *See* p. 3 for further discussion.

<sup>9</sup> 17 C.F.R. § 270.17j-1.

<sup>10</sup> 17 C.F.R. § 270.17j-1(c)(2).

report such transaction to their investment company adviser or underwriter.<sup>11</sup> Additional details on each of the Advisers Act code of ethics requirements are set forth below.

### (a) Standard of Conduct Considerations

The code must set forth a minimum standard of conduct for all supervised persons.<sup>12</sup> While Rule 204A-1 does not require a particular standard, the SEC stated in the adopting release – at the time, in 2004 – that a “good code of ethics should effectively convey to employees the value the advisory firm places on ethical conduct and should challenge employees to live up not only to the letter of the law, but also to the ideals of the organization.”<sup>13</sup> This means that the code must be consistent with the firm’s fiduciary obligations to clients and “premised upon the fundamental principles of openness, integrity, honesty and trust.”<sup>14</sup>

Furthermore, pursuant to Rule 204A-1 text adopted in 2004, investment advisers should consider specifying that supervised persons are not permitted, in connection with the purchase or sale, directly or indirectly, of a security held or to be acquired by a client to:

- Defraud clients in any manner.
- Mislead clients (including an omission of material facts).
- Engage in any act, practice or course of business which operates or would operate as a fraud or deceit upon clients.
- Engage in any manipulative practice with respect to clients.
- Engage in any manipulative practice with respect to securities (including price manipulation).<sup>15</sup>

In adopting Rule 204A-1, it is clear that the SEC intentionally drafted the rule broadly enough so as to provide advisers the flexibility to tailor their code to existing trading policies and varied business models. At the time, the 2019 Interpretation was 15 years away and the SEC had not been as active in specifying the contours of Advisers Act fiduciary principles as it subsequently became. Over the years we have seen exam deficiencies, enforcement settlements and ultimately the Interpretation.

It is helpful and instructive to read the above requirements of Rule 204A-1 in conjunction with the Interpretation. The Interpretation consolidated many – but not all – principles of Advisers Act fiduciary duty in a single Commissioner-approved release. To this end, the Interpretation provides a discussion of both the duty of care and the duty of loyalty, as well as the overarching duty to act in the best interest of clients. The duty of care discussion focuses largely on (i) the duty to provide advice that is in the best interest of the client, (ii) the duty to seek best execution of a client’s

---

<sup>11</sup> 17 C.F.R. § 270.17j-1(d).

<sup>12</sup> 17 C.F.R. § 275.204A-1(a)(1).

<sup>13</sup> *Investment Adviser Code of Ethics*, Advisers Act Release No. 2256 (July 9, 2004) (hereinafter “Adopting Release”) at Section II.A, available at <https://www.federalregister.gov/documents/2004/07/09/04-15585/investment-adviser-codes-of-ethics>.

<sup>14</sup> *Id.*

<sup>15</sup> See 17 C.F.R. § 270.17j-1(b).

transactions where the adviser has the responsibility to select broker-dealers to execute client trades, and (iii) the duty to provide advice and monitoring over the course of the relationship.<sup>16</sup> The duty of loyalty discussion in the Interpretation is instructive with regard to conflict disclosure and mitigation.<sup>17</sup>

The Interpretation purported to consolidate and reaffirm aspects of the fiduciary duty investment advisers owe their clients under Section 206 of the Advisers Act, while at the same time highlighting that it is not intended to be the sole authority on fiduciary duty. Rule 204A-1 is one of those additional authorities on fiduciary duty and among the reasons the Interpretation cannot be the sole authority. Therefore, Rule 204A-1 should be read in conjunction with the Interpretation – particularly the section on conflicts – when an adviser seeks to update its code of ethics program. Advisers should tread carefully to ensure their practices, procedures, and policies outlined in their codes of ethics align with standard of care developments as well as their business model. We note that the Interpretation’s discussion on the duty of loyalty and conflicts management is particularly relevant to a code of ethics analysis.

There is no one size fits all solution to a code of ethics and an adviser should adopt a code that properly reflects its respective business and fiduciary obligations. In failing to include the required provisions or tailoring to the scope of the business, an adviser runs the risk of costly—and potentially reputationally embarrassing—disciplinary action. For example, in a recent action, the order specifically focused on why advisers cannot just over-rely on a code of ethics template. The order noted that this investment adviser had adopted a code of ethics, word for word, from an outside trade organization with no applicability to the firm’s own business.<sup>18</sup> According to the order, “[the firm’s] Code of Ethics, as *adopted wholesale* from the Professional Organization’s Code of Ethics. . . failed to include any. . . requirements.” The order goes on further to say that “in adopting this *off-the-shelf* code of ethics from the Professional Organization’s Code of Ethics, [the firm] failed to meet the requirements of Section 204A and Rule 204A-1 thereunder.” A key takeaway is that advisers are expected to be deliberate and thoughtful in implementing a code of ethics.

### **(b) Reporting Requirements for Access Persons**

A code of ethics must address personal trading and require access persons to periodically report their personal securities holdings and transactions to the CCO or other designated persons.<sup>19</sup> In evaluating who is an access person, Rule 204A-1 defines “access person” to include supervised persons who either (i) have access to nonpublic information regarding clients’ purchase or sale of securities, (ii) are involved in making securities recommendations to clients, or (iii) have access to recommendations that are nonpublic.<sup>20</sup> This includes clerical, accounting, and information technology personnel who have access to client recommendations.

---

<sup>16</sup> *Id.* at 33672-33674.

<sup>17</sup> See [2023 Conflicts Outline](#) for additional detail.

<sup>18</sup> See *In the Matter of Two Point Cap. Mgmt., Inc., & John B. McGowan*, Advisers Act Release No. 6199 (Dec. 5, 2022), available at <https://www.sec.gov/files/litigation/admin/2023/ia-6413.pdf> (emphasis added).

<sup>19</sup> *Id.*

<sup>20</sup> 17 C.F.R. § 275.204A-1(e)(1).

On the other hand, access persons do not generally comprise employees of service providers or related persons, even though they may have access to such information. In such situations, however, advisers should consider access and level of risk.<sup>21</sup> Directors, officers and partners of an investment adviser whose primary business is giving investment advice are presumed to be access persons.<sup>22</sup>

### **i. Holdings Reports**

Access persons must submit a securities holdings report no later than ten days after becoming an access person and once a year thereafter.<sup>23</sup> All information submitted in the reports must be current as of a date no more than 45 days prior to the individual becoming an access person (with respect to the first report) or not more than 45 days prior to the date the report is submitted (with respect to subsequent reports).

At a minimum, each holdings report must contain the following:

- The title and type of security, the exchange ticker symbol or CUSIP number (as applicable), the number of shares, and principal amount of each reportable security<sup>24</sup> in which the access person has any direct or indirect beneficial ownership;<sup>25</sup>
- The name of any broker, dealer or bank with which the access person maintains an account in which any securities are held for the access person's direct or indirect benefit; and
- The date the access person submits the report.

---

<sup>21</sup> Note that the SEC has found violations where the investment advisers did not properly establish or maintain policies and procedures for identifying whether outside consultants involved in portfolio management should be subject to the adviser's policies or procedures, including the code of ethics. *See In the Matter of Federated Global Investment Management Corp.*, Advisers Act Release No. 4401 (May 27, 2016), available at: <https://www.sec.gov/litigation/admin/2016/ia-4401.pdf>.

<sup>22</sup> 17 C.F.R. § 275.204A-1(e)(1); *see also* 17 C.F.R. § 270.17j-1(a)(1) (“If an investment adviser’s primary business is advising Funds or other advisory clients, all of the investment adviser’s directors, officers, and general partners are presumed to be Access Persons of any Fund advised by the investment adviser. All of a Fund’s directors, officers, and general partners are presumed to be Access Persons of the Fund.”).

<sup>23</sup> 17 C.F.R. § 275.204A-1(b)(1); *see also* 17 C.F.R. § 270.17j-1(d)(i).

<sup>24</sup> Rule 204A-1 treats all securities—as broadly defined in Section 202(a)(18) of the Advisers Act—as “reportable securities” though it specifically excludes from its purview: (i) transactions and holdings in direct obligations of the U.S. government; (ii) certain bank instruments, commercial paper and agreements; (iii) shares of money market funds; (iv) transactions and holdings in shares of other types of mutual funds, unless the adviser or a control affiliate acts as the investment adviser or principal underwriter for the fund; and (v) transactions in units of a unit investment trust if the unit investment trust is invested exclusively in unaffiliated mutual funds. *See* 17 C.F.R. § 275.204A-1(e)(10); Adopting Release, *supra* note 13 at Section II.C.6. Note, Rule 17j-1 requires access persons of investment companies to report holdings or transactions in securities held or to be acquired by the investment company, but it does not require access persons to report holdings or transactions in shares of open-end funds, including mutual funds they manage. 17 C.F.R. § 270.17j-1(a)(4)(iii).

<sup>25</sup> Beneficial ownership is defined by reference to Rule 16a-1(a)(2) under the Exchange Act, which presumes an access person to have beneficial ownership of securities held by his or her immediate family members residing in the same household. 17 C.F.R. § 275.204A-1(e)(3). Thus, these securities holdings must be reported as well. Immediate family members include any child, stepchild, grandchild, parent, stepparent, grandparent, spouse, sibling, mother-in-law, father-in-law, son-in-law, brother-in-law, or sister-in-law, and adoptive relationships. 17 C.F.R. § 240.16a-1(e).

## ii. Transaction Reports

An adviser's code of ethics must require that access persons submit quarterly transaction reports of all personal securities transactions no later than 30 days after the end of the calendar quarter.<sup>26</sup> Each report must contain, at a minimum, the following information about each transaction involving a reportable security in which the access person had, or acquired, any direct or indirect beneficial ownership:

- The date of the transaction, the title, and as applicable the exchange ticker symbol or CUSIP number, the interest rate and maturity date, number of shares, and principal amount of each reportable security involved;
- The nature of the transaction (i.e., purchase, sale or any other acquisition or disposition);
- The execution price of the security;
- The name of the broker, dealer or bank by or through which the transaction was executed; and
- The date the access person submits the report.

## iii. Exceptions to Reporting Requirements

Rule 204A-1 permits three exceptions to reporting personal securities. First, access persons are not required to submit reports with respect to securities held in accounts over which the access person had no direct or indirect influence or control.<sup>27</sup> Before relying on this exception, the SEC has recommended that investment advisers take steps to establish a reasonable belief that an access person actually had no direct or indirect influence or control, as opposed to a third-party manager simply having discretionary investment authority. In doing so, the SEC suggests an investment adviser consider, for example:

- obtaining information about a trustee or third-party manager's relationship to the access person;
- obtaining periodic certifications by access persons and their trustees or discretionary third-party managers regarding the access persons' influence or control over the account;
- providing access persons with the exact wording of the reporting exception and a clear definition of "no direct or indirect influence or control" that the investment adviser consistently applies to all access persons; and
- on a sample basis, requesting reports on holdings and/or transactions made in the account to identify transactions that would have been prohibited pursuant to the adviser's code of ethics, absent reliance on the reporting exception.<sup>28</sup>

---

<sup>26</sup> 17 C.F.R. § 275.204A-1(b)(2); *see also* 17 C.F.R. § 270.17j-1(d)(1)(ii).

<sup>27</sup> 17 C.F.R. § 275.204A-1(b)(3)(i); *see also* 17 C.F.R. § 270.17j-1(d)(2)(i).

<sup>28</sup> *See* Investment Management Guidance Update, Personal Securities Transactions Reports by Registered Investment Advisers: Securities Held in Accounts Over Which Reporting Persons Had No Influence or Control, No. 2015-03 (June 2015), available at <https://www.sec.gov/investment/im-guidance-2015-03.pdf>.

Moreover, access persons are not required to submit a transaction report (1) with respect to transactions effected pursuant to an automatic investment plan, or (2) if the report would duplicate information contained in broker trade confirmations or account statements that are received no later than 30 days after the end of the applicable quarter.<sup>29</sup>

#### **iv. Report Reviews**

Once submitted, securities transactions and holding reports must be reviewed by the CCO or other designated person to identify potential conflicts of interests and prevent misconduct.<sup>30</sup> The SEC has stated that such person should, among other things, “compare the personal trading to any restricted lists” and “assess whether the access person is trading for his own account in the same securities he is trading for clients, and if so whether the clients are receiving terms as favorable as the access person takes for himself.”<sup>31</sup>

#### **(c) Pre-Clearance Requirements**

An investment adviser’s code of ethics must also include a requirement that its access persons obtain prior authorization before investing in an initial public offering (“IPO”) or private placement, which would include most investments in hedge funds or other private funds.<sup>32</sup> Because most people do not have the opportunity to invest in IPOs or private placements, the issues that often arise with respect to an access person’s purchase of these securities include whether the employee should have first offered the opportunity to clients, or whether a portfolio manager is receiving a personal benefit for directing client business.<sup>33</sup>

Beyond this base-level requirement, many advisers may wish to adopt policies requiring that its access persons obtain prior approval for all personal securities transactions and that duplicate confirmations for personal securities transactions be provided to and reviewed by a designated senior person (some advisers require all access persons to trade through designated firms that automatically provide the adviser with duplicate confirmations). The SEC strongly recommended too that such policies and systems provide for automated or computerized analysis of trading patterns.<sup>34</sup> According to the SEC, this practice aims to prevent gaming the restrictions, such as placing personal trades on the day before or after “blackout” periods begin or end. Advisers with robust policies and procedures around preclearance – as opposed to a more bare minimum framework – further mitigate their enforcement risk by showing a reasonable, thoughtful and thorough effort to meet the rule’s requirements. Demonstrating such an effort is helpful in an exam and enforcement setting, and can have significant impact on the adviser’s liability in the event of

---

<sup>29</sup> 17 C.F.R. § 275.204A-1(b)(3)(ii)-(iii). No-action relief has been provided to permit an investment adviser not to treat an access person’s transactions and holdings in a 529 Plan as reportable securities if the adviser or its control affiliate does not manage, distribute, market, or underwrite the 529 Plan or the investments and strategies underlying the 529 Plan. Wilmer Hale, LLP, SEC No-Action Letter (July 28, 2010), available at <https://www.sec.gov/divisions/investment/noaction/2010/wilmerhale072810.htm>.

<sup>30</sup> 17 C.F.R. § 275.204A-1(a)(3); *see also* 17 C.F.R. § 270.17j-1(d)(3).

<sup>31</sup> Adopting Release, *supra* note 13 at Section II.G.

<sup>32</sup> 17 C.F.R. § 275.204A-1(c); *see also* 17 C.F.R. § 270.17j-1(e).

<sup>33</sup> *See* Adopting Release, *supra* note 13 at n.50.

<sup>34</sup> *See* Adopting Release, *supra* note 13.

an employee engaging in fraudulent and deceitful conduct by intentionally concealing transactions and falsifying internal reports.<sup>35</sup>

## **2. Reporting Violations and Maintaining the Code of Ethics**

A code of ethics must require all supervised persons to promptly report any violations of the code to the investment adviser's CCO or other designated person.<sup>36</sup> Should an investment adviser designate someone other than the CCO to receive reports of violations, the adviser must still have procedures requiring that the CCO receives periodic reports of all violations. Furthermore, all violations of the code of ethics should be handled appropriately and consistently across all staff. This includes the imposition of fines or other similar sanctions for repeated violations.

In its adopting release, the SEC cautioned investment advisers that it is the adviser's responsibility to foster an environment in which individuals feel comfortable and encouraged to report violations.<sup>37</sup> Safeguards should be in place to protect and prevent retaliation against supervised persons who report violations. For example, advisers may choose to permit anonymous reporting, or decide that retaliation constitutes a further violation of the code.<sup>38</sup>

### **(a) Adviser Enforcement of the Code of Ethics**

An investment adviser's code of ethics should be maintained, enforced, and frequently reviewed. The authority to enforce the code often lies with the CCO, or others designated under his or her authority.

As mentioned above, part of enforcing the code includes an adviser reviewing access persons' personal securities reports. The CCO or designated person should, among other things: (1) review whether the access person followed proper internal procedures, such as pre-clearance; (2) periodically analyze the access person's trading for patterns that may indicate abuse, including market timing; and (3) investigate any substantial disparities between the percentage of trades that are profitable when the access person trades for his or her own account and the percentage that are profitable when he or she places trades for clients.<sup>39</sup>

---

<sup>35</sup> See *In re Geoffrey Brod*, Advisers Act Release No. 2673 (Oct. 24, 2007).

<sup>36</sup> 17 C.F.R. § 275.204A-1(a)(4). Whether the reviews are conducted by the CCO or other designated person generally depends on the size of the investment adviser.

<sup>37</sup> Adopting Release, *supra* note 13 at Section II.E.

<sup>38</sup> Section 21F of the Securities Exchange Act of 1934 and Rules 21F-1 through 21F-17 thereunder are designed to protect whistleblowers by creating incentives for investment adviser employees to report violations of the federal securities laws. While outside the scope of this outline, some investment advisers incorporate such rules into their codes of ethics, prohibiting advisers and their personnel from deterring, or retaliating against, an employee who reports. Note, in September 2023, the SEC brought an enforcement action against an investment adviser for requiring employees to sign agreements that prohibited them from disclosing "Confidential Information" to anyone outside of the firm unless authorized by the firm or required by law, without any exception for voluntary communications with the SEC concerning possible securities laws violations. See *In the Matter of D.E. Shaw & Co, L.P.*, Exchange Act Release No. 98641 (Sept. 29, 2023), available at <https://www.sec.gov/files/litigation/admin/2023/34-98641.pdf>.

<sup>39</sup> Adopting Release, *supra* note 13 at Section II.G.

### **(b) Educating Employees About the Code of Ethics**

An adviser's code of ethics must require that each supervised person is provided a copy of the codes of ethics and any amendments.<sup>40</sup> The code must also require each supervised person to acknowledge, in writing, his or her receipt of those copies.<sup>41</sup>

Though not required, many advisers provide periodic employee training to highlight the types of conflicts of interest that may arise. The SEC recommends that investment advisers train employees on the principles and procedures of their codes, in addition to holding sessions with new and existing employees to remind them of their obligations under the code.<sup>42</sup>

Procedures such as requiring supervised persons to annually certify that they have read and understood the code and providing annual hands-on trainings help to reinforce the code's principles. Moreover, it provides supervised persons with an opportunity to ask questions and to gain a better understanding for the consequences of non-compliance. The point is to make the trainings meaningful. For example, advisers should explain the rationale behind the rules and use real-life scenarios and fact patterns to make it memorable for the employees. Advisers can additionally ask employees to bring to the training any ethical dilemmas they have experienced.

### **3. Recordkeeping Requirements**

An adviser's code of ethics must require that the adviser keep copies of the code, records of violations of the code, and any actions taken against violators of the code. Advisers must also maintain copies of each supervised person's acknowledgement of receipt of a copy of the code and any amendments.<sup>43</sup> Moreover, Rule 204-2(a)(13) requires investment advisers to keep a record of the names of their access persons, the holdings and transaction reports made by access persons, and records of decisions approving access persons' acquisition of securities in IPOs and limited offerings.<sup>44</sup>

The standard retention period required for most records is five years. The records must be kept in an easily accessible place, and the first two years of which the records must be in an appropriate office of the investment adviser.<sup>45</sup> The five years is measured per the following:

- Codes of ethics must be kept for five years after the last date they were in effect.
- Supervised person acknowledgements of the code must be kept for five years after the individual ceases to be a supervised person.
- The list of access persons must include every person who was an access person at any time within the past five years, even if some of them are no longer access persons of the investment adviser.

---

<sup>40</sup> 17 C.F.R. § 275.204A-1(a)(5).

<sup>41</sup> *Id.*

<sup>42</sup> Adopting Release, *supra* note 13 at Section II.F.

<sup>43</sup> 17 C.F.R. § 275.204-2(a)(12); *see also* 17 C.F.R. § 270.17j-1(f).

<sup>44</sup> 17 C.F.R. § 275.204-2(a)(13).

<sup>45</sup> 17 C.F.R. § 275.204-2(e).

Although not expressly required in the rules, the SEC has stated that investment advisers also will likely need to maintain electronic records of access persons' personal securities reports in order to meet their obligations with respect to reviewing the records and monitoring compliance with their codes of ethics.<sup>46</sup>

While some may find recordkeeping burdensome, the goal is to ensure that all documentation or other output generated substantiates the adviser's efforts in obtaining all related information in a timely, accurate, and complete manner.

#### **4. Common Compliance Issues and SEC Division of Examination Observations**

We acknowledge that the provisions of Rule 204A-1 are not overtly complicated, but note that in our experience, in practice the details may get lost in the shuffle of day-to-day firm operations. An adviser's code of ethics, however, is one of the initial documents the SEC will request and review during a typical examination of an adviser.<sup>47</sup> Noncompliance with the code of ethics is thus a quick and easy area for the SEC to uncover possible violations.

Pursuant to a Risk Alert issued on April 26, 2022 (the "2022 Risk Alert"),<sup>48</sup> staff from the Division of Examinations noted the following recurrent deficiencies associated with Rule 204A-1 during the Exams process:

- Identification of Access Persons. Advisers failed to identify and supervise certain employees as access persons in accordance with Rule 204A-1. Moreover, many codes of ethics did not properly define "access persons" or accurately identify which employees were access persons.
- Pre-Clearance for Certain Investments. Access persons failed to obtain the requisite pre-approval before purchasing direct or indirect ownership in IPOs and private offerings, and codes failed to include such requirements.
- Personal Securities Transactions and Holdings. Access persons failed to report personal securities transactions and holdings, and ones that did contained deficiencies. For example, some advisers: (1) failed to produce evidence of supervisory review of holdings and transaction reports; (2) did not assign to another employee or officer the review of a CCO's reporting, thereby permitting the CCO to self-review his or her own reports; and (3) did not include in their codes provisions requiring access persons to submit reports, or include in such reports all of the information required by Rule 204A-1, such as private placements.
- Written Acknowledgment of Receipt of Code. Advisers failed to provide supervised persons with a copy of the code or amendments to the code, and in turn, supervised persons failed to provide written acknowledgement of the same.

---

<sup>46</sup> Adopting Release, *supra* note 13 at Section II.H.

<sup>47</sup> See Division of Examinations Risk Alert, Investment Advisers: Assessing Risks, Scoping Examinations, and Requesting Documents (Sept. 6, 2023), available at <https://www.sec.gov/files/risk-alert-ia-risk-and-requesting-documents-090623.pdf>.

<sup>48</sup> See Division of Examinations Risk Alert, Investment Adviser MNPI Compliance Issues (Apr. 26, 2022), available at <https://www.sec.gov/files/code-ethics-risk-alert.pdf>.

- Trading Investments on Restricted List. Employees traded in securities of issuers that were on the adviser’s restricted securities list.
- Allocation of Investment Opportunities. Employees failed to follow policies and procedures regarding the allocation of investment opportunities (e.g., an adviser or its employee purchased securities at a better price, or ahead of the adviser’s clients and in contravention of the adviser’s own code of ethics).

The 2022 Risk Alert serves as a reminder that advisers should consistently and meaningfully review their practices, policies, and procedures regarding the topics listed above to ensure they comply with the Advisers Act and the rules thereunder. First and foremost, advisers should review their codes to confirm that they provide for all elements required by Rule 204A-1. All relevant definitions should be consistent with the rule and all records or lists should be up to date and accurately reflect the current status and activities of the adviser. Policies and procedures for regularly updating the code and relevant materials should also be in place and routinely followed.

The 2022 Risk Alert also notes that “advisers should consider incorporating procedures to ensure that investment opportunities must first be offered to clients before the adviser or its employees may act on them.”<sup>49</sup> This observation concerns potential breaches of an adviser’s fiduciary duties and reinforces the notion that compliance personnel must remain vigilant when preclearing employee trades involving securities that may relate to existing investor or fund strategies.

Furthermore, advisers should remind access persons of their obligations to: (1) submit transaction and holdings reports; (2) submit written acknowledgements on a timely basis and otherwise in accordance with the code; and (3) obtain pre-approval prior to making IPO and limited offering purchases. Advisers should also evaluate whether their recordkeeping procedures are sufficient to demonstrate that transaction and holdings reports are reviewed and that any omissions or violations by access persons are addressed appropriately.

## **5. Additional Considerations**

Potential conflicts of interest may arise in other areas not enumerated in Rule 204A-1. As such, advisers have the option to implement higher ethical standards when developing and enforcing a code of ethics. In doing so, certain risks and advantages must be considered. For example, including additional content reduces the risk of noncompliance with other fiduciary obligations under the Advisers Act. At the same time, it broadens the possibility for violations and may increase the administrative burden with respect to documenting the same.

Nevertheless, common additions to a code of ethics are discussed in greater detail below.

### **(a) Outside Business Activities**

While not required by the rule, many advisers include in their code of ethics provisions regarding other business activities of their supervised persons to prevent conflicts with such person’s

---

<sup>49</sup> *Id.*

fiduciary duties. Supervised persons' conflicts may affect their ability to make proper decisions on behalf of clients and are attributed to the adviser.

Activities like serving on a nonprofit board, while common in the industry, can present potential conflicts that need monitoring. Other examples of potentially conflicted outside business activities include forming an entity for personal business activities or receiving compensation from a person or entity other than the adviser and its affiliates. Advisers could either prohibit such activities or implement policies requiring prior authorization.

### **(b) Gifts, Contributions, and Entertainment**

Accepting gifts or entertainment may implicate other violations of the law outside of Rule 204A-1. Accordingly, the SEC has indicated that the receipt of gifts or entertainment by investment advisers should be addressed in the adviser's compliance manual or as a stand-alone policy. A properly implemented policy helps shield employees from improper influence and thus protects the interests of the adviser and its clients. When developing such a policy, advisers should consider requirements to report gifts given or received over a de minimis amount (an amount which should reasonably reflect the adviser and its clientele).

### **(c) Insider Trading**

Beyond warning investment advisers to review their codes of ethics, the 2022 Risk Alert discussed above also noted the additional scrutiny on advisers for lacking appropriate policies concerning material nonpublic information ("MNPI").<sup>50</sup> Section 204A of the Advisers Act requires investment advisers to establish, maintain and enforce written policies and procedures reasonably designed to prevent the misuse of MNPI by the adviser or any of its associated persons.<sup>51</sup> Many provisions required in a code of ethics may serve a dual purpose in preventing the receipt and misuse of MNPI, but they are likely insufficient, standing alone, and thus need to be supplemented.

### **(d) Anti-Bribery**

Advisers may also wish to incorporate anti-bribery policies that address compliance issues related to the Foreign Corrupt Practices Act and doing business outside the United States.

## **6. Update on SEC Enforcement Actions**

The last time there was a string of settlement orders focusing on Rule 204A-1 dates back to 2015. We note, however, based on recent orders, that the Division of Enforcement shows no signs of retreating. Furthermore, the more recent orders show that investigations and recommendations for resolution are following a consistent position similar to about a decade ago. Below is a sampling of settlement orders.

---

<sup>50</sup> *Id.*

<sup>51</sup> 15 U.S.C. § 80b-4a.

- *In the Matter of Mortg. Indus. Advisory Corp.*, Advisers Act Release No. 6413 (Sept. 11, 2023). Despite receiving a deficiency notice during an examination in 2006, MIAC failed to properly establish, maintain, and enforce a written code of ethics until 2022—which was only after a subsequent 2021 examination raised the same issues.
- *In the Matter of Parallax Invs., LLC, John P. Bott, II, & F. Robert Falkenberg*, Advisers Act Release No. 4159 (Aug. 6, 2015). For two years after registration with the Commission, Parallax failed to adopt proper policies and procedures as well as perform annual reviews of the adequacy and effectiveness of such policies.
- *In the Matter of Du Pasquier & Co., Inc.*, Advisers Act Release No. 4004 (Jan. 21, 2015). Du Pasquier adopted a code of ethics but failed to indicate how personal transactions would be reviewed, and thus Du Pasquier did not assess whether a given access person had traded in his own account in the same security he was trading for clients.
- *In the Matter of Thomas E. Meade*, Advisers Act Release No. 3855 (June 11, 2014). As CCO of PCM, Inc., Thomas Meade failed to adequately collect and review required reports. Furthermore, Meade overly relied on other employees to self-report violations and failed to assess the adequacy or effectiveness of the firm’s policies and procedures on an annual basis as required by said policies and procedures.

# 2024 Investment Adviser Compliance Conference

MARCH 6-8 / WASHINGTON, DC

EFFECTIVE STRATEGIES & BEST PRACTICES

## Cybersecurity for Smaller and Medium Firms

**Gordon Eng**, SKY Harbor Capital Management, LLC

**Christian Kelly**, CISSP, Xantrion

**Joseph Mannon**, Vedder Price P.C. (MODERATOR)

1

1



2024 Investment Adviser  
Compliance Conference

EFFECTIVE STRATEGIES  
& BEST PRACTICES

## Disclaimer

This presentation is intended for educational and discussion purposes only, and nothing stated today whether in writing or verbally shall constitute legal advice.

The content of this presentation and comments expressed by the moderator and each panelist are solely their personal perspectives, views, and opinions and do not represent the perspectives, views, opinions or policies of their affiliated entities.

2

2



2024 Investment Adviser  
Compliance Conference

EFFECTIVE STRATEGIES  
& BEST PRACTICES



## Agenda

- SEC's Proposed Cybersecurity Risk Management Rules
- Recent Division of Examinations Risk Alerts and Division of Enforcement cases
- Reasonably Designed Cybersecurity Policies and Procedures
- Practical Practice Pointers

3

3



2024 Investment Adviser  
Compliance Conference

EFFECTIVE STRATEGIES  
& BEST PRACTICES



## Cybersecurity: why all the fuss?

Only a matter of time before Threat Actors will see smaller and medium sized financial firms as easier targets than the big banks/firms that have substantial cybersecurity budgets and employ large staffs of technologists.

4

4



## Cybersecurity: an existential threat

Significant Cyber Incidents can result in:

- Significant financial and operational harm (regulatory sanctions, fines, lawsuits, remediation expenses, increased cyber insurance premiums)
- Reputational Harm can be irreparable for smaller and medium size firms
- Loss of client confidence in firm's ability to act as fiduciary of client assets

5

5



## The CIA of Cybersecurity

No presentation of Cybersecurity would be complete without a reminder that, the essential core of the cybersecurity is data security, which in turn rests on three pillars:

- Confidentiality
- Integrity
- Availability

Every aspect cybersecurity touches one or more to these three pillars directly or indirectly, and keeping these pillars in mind while traveling through the topic may be a helpful focal point.

6

6



**2024** Investment Adviser  
Compliance Conference

**EFFECTIVE STRATEGIES  
& BEST PRACTICES**



## The Proposed Rule

Published in the Federal Register on March 9, 2022, vol. 87, No. 46, at 13524 entitled: Cybersecurity Risk Management for Investment Adviser, Registered Investment Companies, and Business Development Companies. The Proposed Rule has not yet been enacted.

7

7



**2024** Investment Adviser  
Compliance Conference

**EFFECTIVE STRATEGIES  
& BEST PRACTICES**



## Scope of the Proposed Rule

- RIAs (and their private funds), Registered Funds and BDCs
- Adopt and implement written cybersecurity policies and procedures reasonably designed to address cybersecurity risks and reviewed no less frequently than annually
- Required to report promptly to the SEC but not less than 48 hours after a “significant cybersecurity incident(s)” has occurred or is occurring
- New IAA and ICA Disclosure Forms and Recordkeeping Rules

8

8



## Proposed Rule Reporting Obligation

Advisers would be required to report significant cybersecurity incidents to the Commission, including on behalf of a client that is a RIC, or a BDC, or a private fund (each a “covered client”) that experiences a significant cybersecurity incident.

Any RIA or any adviser required to be registered with the SEC as an investment adviser would be required to report on proposed Form ADV-C promptly, but in no event more than 48 hours, after having a *reasonable basis* to conclude that a significant adviser cybersecurity incident or significant fund cybersecurity incident had occurred or is occurring. (emphasis added)

9

9



## Confidential Treatment (for now)

The SEC acknowledged in the Proposed Rule that public disclosure of an adviser’s significant cybersecurity breach “harm an adviser’s or fund’s ability to mitigate or remediate the cybersecurity incident, especially if it is ongoing.

“Accordingly, our preliminary view is that Form ADV– C should be confidential given that public disclosure is neither necessary nor appropriate in the public interest or for the protection of investors.” Proposed Rule at 13539.

10

10

## Follow Up Reporting Obligation

Proposed rule 204–6 would also require advisers to amend any previously filed Form ADV–C promptly, but in no event more than 48 hours, after information reported on the form becomes materially inaccurate; if new material information about a previously reported incident is discovered; and after resolving a previously reported incident or closing an internal investigation pertaining to a previously disclosed incident.

11

11

## What Is A Significant Cybersecurity Incident?

Under the proposed rule, “a significant adviser cybersecurity incident is a cybersecurity incident, or a group of related incidents, that significantly disrupts or degrades the adviser’s ability, or the ability of a private fund client of the adviser, **to maintain critical operations** [broadly defined in FN 60], or leads to the unauthorized access or use of adviser information, where the unauthorized access or use of such information results in: **(1) Substantial harm to the adviser, or (2) substantial harm to a client, or an investor in a private fund, whose information was accessed.**”

12

12



## The SEC's Concerns

- The “staff continues to observe that certain advisers and funds show a lack of cybersecurity preparedness, which puts clients and investors at risk.”
- The staff is “concerned that clients and investors may not be receiving sufficient cybersecurity-related information, particularly with respect to cybersecurity incidents to help ensure they are making informed investment decisions.”

The Proposed Rule at 13525

13

13



## Cybersecurity as a Fiduciary Duty

The proposed Cybersecurity Rule if enacted will be promulgated under 17 CFR 275.206(4)-9 of the IAA and under 17 CFR 270.38a-2.

As a reminder, the proposed rule is promulgated under Section 206 of the IAA, Prohibited Transactions by Registered Investment Advisers, which imposes a fiduciary duty on RIAs by operation of law per the 1963 SCT case SEC v. Capital Gains Research Bureau, Inc.

14

14



2024 Investment Adviser  
Compliance Conference

EFFECTIVE STRATEGIES  
& BEST PRACTICES



## Current Legal and Regulatory Framework

“An adviser’s fiduciary obligation to its clients includes the obligation to take steps to protect client interests from being placed at risk because of the adviser’s inability to provide advisory services,” which “include steps to minimize operational and other risks that could lead to significant business disruptions or a loss or misuse of client information,” . . . “Thus, advisers should take steps to minimize cybersecurity risks in accordance with their fiduciary obligations.” Proposed Rule at 13526.

15

15



2024 Investment Adviser  
Compliance Conference

EFFECTIVE STRATEGIES  
& BEST PRACTICES



## SEC Resources

16

16



**2024** Investment Adviser  
Compliance Conference

**EFFECTIVE STRATEGIES  
& BEST PRACTICES**



- OCIE Cybersecurity and Resiliency Observations (2019)
  - <https://www.sec.gov/files/OCIE%20Cybersecurity%20and%20Resiliency%20Observations.pdf>
- Observations from Cybersecurity Examinations (2017)
  - <https://www.sec.gov/files/observations-from-cybersecurity-examinations.pdf>
- SEC Announces Three Actions Charging Deficient Cybersecurity Procedures
  - <https://www.sec.gov/news/press-release/2021-169>

17

17



**2024** Investment Adviser  
Compliance Conference

**EFFECTIVE STRATEGIES  
& BEST PRACTICES**



## Reasonably Designed Cybersecurity Policies and Procedures

18

18



## What the SEC believes:

“We believe that advisers and funds should be required to adopt and implement policies and procedures that **address a number of elements** to increase the likelihood that they are prepared to face a cybersecurity incident (whether that threat comes from an outside actor or the firm’s personnel), and that investors and other market participants are protected from a cybersecurity incident that could significantly affect a firm’s operations and lead to significant harm to clients and investors.” (emphasis added)  
Proposed Rule at 13527.

19

19



## NB: What California believes:

In February 2016, then-California Attorney General Kamala D. Harris wrote in the 2016 California Data Breach Report:

“The 20 [now 18] controls in the [CIS’s] Critical Security Controls identify a *minimum* level of information security that all organizations that collect or maintain personal information should meet. The *failure to implement all the Controls* that apply to an organization’s environment *constitutes a lack of reasonable security.*” (emphasis added)

20

20



## Accountability

P&P should designate the person(s) who shall implement and oversee the effectiveness of the firm's cybersecurity policies and procedures. CCO's extra job?

The Proposed Rule permits the use of third-party cybersecurity risk management services ("MSPs"), but Investment Advisers are responsible to exercise appropriate oversight. What does appropriate oversight look like?

21

21



## Liability Considerations

Will CCOs or COOs of small and medium firms embrace the added role of CISO after recent enforcement action against the former SolarWinds CISO?

Is the paradigm of CCO liability portable to the CISO role? See Vedder Price PC, Nov. 24, 2023, comment on CCO Liability

(affirmatively participate in misconduct, mislead regulator, wholesale failure to perform)

22

22



## Duty of Oversight

- Most smaller and medium size firms outsource cybersecurity to Managed Service Providers (“MSP”), but you should have sufficient knowledge to exercise reasonable oversight.
- Review closely your contracts, MSAs, and SOWs and understand each component of your MSP’s services and tools employed to address cybersecurity concerns.
- Ask your MSP how your current network and cybersecurity infrastructure reflects the principle of “Defense-in-Depth”?

23

23



## Cybersecurity: Getting Up to Speed

- Regulatory involvement in managing cybersecurity risk, now more than ever, merits the attention of executive management and the Boards of both public and private companies.
- Either upstream or downstream relationships with public companies can trigger an incident response and/or regulatory reporting obligation, which may implicate or directly involve a private company.
- Education, Awareness, and Training: many available resources

24

24



## Essential First Steps

- Conduct a Threat Vulnerability Assessment
- Rank the Risks (probability of occurrence and impact of occurrence)
- Allocate Resources and establish Partnerships (internal and external)
- Build consensus among senior management and internal stakeholders and balance risk management with business priorities

25

25



## Risk Frameworks and Assessment Methodologies

- Prepare the firm to deal with and categorize cyber risks
- Select Controls – NIST pub. 800-53 ver. 5; Center for Internet Security Critical Security Controls v.8; ISO/IEC 27001
- Implement and Assess Controls
- Authorize and drive accountability
- Monitor and adjust accordingly (consider KPIs)

26

26



## KEY Elements in Cybersecurity P&P

- Risk Assessment
- Data Protection (privacy)
- Secure Configuration of Enterprise Assets and Software
- Account Management
- Access Control Management
- Continuous Vulnerability Management
- Audit Log Management
- Email and Web Browser Protection
- Malware Defense
- Data Recovery
- Source: Center for Internet Security Critical Security Controls V. 8

27

27



## And there's more!

- Network Infrastructure Management
- Network Monitoring and Defense
- Security Awareness and Skills Training – a culture of cybersecurity awareness and vigilance
- Service Provider Risk Management
- Application Software Security
- Incident Response
- Penetration Testing

28

28



## Center for Internet Security Critical Controls

The foregoing series of Key Elements of Cybersecurity P&P comprise virtually all 18 controls\* (formerly 20 Controls in Version 7 until May 2021) set forth in the Center for Internet Security (“CIS”) Critical Security Controls, Version 8, a widely-recognized and accepted cybersecurity risk framework.

\*The CIS’s “Inventory and Control of Enterprise Assets” and “Inventory and Control of Software Assets” were compressed as “Risk Assessment” in the prior slide.

29

29



## Key Cybersecurity Principles

- Defense-in-depth
- Least privilege or Zero Trust Network Access (“ZTNA”)
- Understand your firm’s “Attack Surface” by inventorying and controlling all endpoints, especially if you are an all or hybrid distributed workforce (WFH) business model.
- Continuous Vulnerability Management
- Robust and resilient Incident Response

30

30

## National Institute of Standards and Technology

NIST Cybersecurity Framework (“CSF”) five core functions:

- Identify
- Protect
- Detect
- Respond
- Recover

See also NIST publication 800-53 Rev 5, Security and Privacy Controls for Information Systems and Organizations available at: <https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final>. Last visited: Feb. 7, 2024, sets forth 20 “families” of cybersecurity controls including P&P, specific controls, control enhancements, and detailed discussion.

31

31

## A closer look at Vulnerability Analysis

Vulnerability analysis consists of a tools to detect, mitigate, and remediate cybersecurity threats and vulnerabilities:

- Endpoint Detection and Response Systems (“EDR”)
- Network Detection and Response Systems (“NDR”)
- Intrusion Detection Systems (“IDS”) and Intrusion Prevention System (“IPS”)

32

32



2024 Investment Adviser  
Compliance Conference

EFFECTIVE STRATEGIES  
& BEST PRACTICES



## Looking up to the Cloud

Size notwithstanding, our industry is undergoing a digital transformation, and much of it is led by migrating significant IT and Communication infrastructure to “the cloud” (e.g., AWS, Azure, Google, or private clouds).

With pandemic legacy WFH or hybrid structures, centralized cybersecurity command and controls are now a necessary part of a firm’s cybersecurity infrastructure.

33

33



2024 Investment Adviser  
Compliance Conference

EFFECTIVE STRATEGIES  
& BEST PRACTICES



## Centralized Command and Control

The former model of a physical office defended by a physical or electronic/firewall perimeter protecting all those inside from outside threats is an outdated and arguably a dangerously obsolete cybersecurity model.

A firm (or its MSP) must be able to remotely configure, maintain, patch and update security protocols to multiple endpoints (located anywhere and everywhere) simultaneously and in a timely way.

34

34



## Weaving in SIEMS and SOCs

- Security Information and Event Management Systems (SIEMs) – a single pane of glass to monitor the attack surface with automated alerts
- Security Operations Center (SOC) – a team to detect, respond and recover
- Data Loss Prevention Systems – detect potential exfiltration
- Network Traffic Analysis – detect DDoS attacks

35

35



## Intrusion Detection Frameworks

MITRE ATT&CK (Adversarial Tactics, Techniques and Common Knowledge), is a structured matrix of tactics, techniques, and procedures (“TTPs”) used by threat actors to find, infiltrate, and impact networks and data by impairing, damaging or destroying the confidentiality, integrity and availability of a firm’s data. See <https://attack.mitre.org/matrices/enterprise/>

36

36



## What is a Significant Cybersecurity Event?

Factors in the Calculus Determining a Significant Cybersecurity Incident:

- Did the data breach put the firm or any employees or clients at risk?
- Severity, Scope, and Impact on CIA data privacy triad
- Nature of the Compromised Data (PII, PCI-DSS, IP, bank a/c)
- Regulatory, Legal and Insurance Considerations
- Disclosure Obligations: regulators, law enforcement, stakeholders, public
- Financial Impact/Business Impairment

37

37



## Severity, Scope and Impact

- Duration of Incident (still ongoing? How long until discovered? APT? Time needed to determine significance?)
- Nature of the data breach? Quality and Quantity, Exfiltrated, altered or corrupted Impaired Availability (Ransomware)
- Impact on operating business (degree of impairment or impediments to trading, investing, reporting, sales, back-office operations, risk management, marketing, or compliance functions? Will major business units be taken offline? For how long?)

38

38



## Nature of Compromised Data

- PII notice obligations to affected individuals – each state has its own laws and rules
- Unclassified Controlled Information – subject to applicable law, regulation, and government policies although not classified
- Was the data encrypted? If so, how secure was the cypher used?

39

39



## Regulatory, Legal, and Insurance

- Have any statutory or regulatory mandates been violated? (e.g., GLBA, CCPA, HIPAA, GDPR)
- Have any contractual obligations been triggered requiring disclosure? (e.g., NDAs covering another party's confidential information)
- Has a claim been filed under a claims made cyber insurance policy? Should a filed claim be presumed significant?

40

40



## A Reasonable Basis to Report

The Proposed Rule highlights that the 48-hour reporting obligation is triggered as soon the RIA has a “reasonable basis” to conclude that a significant adviser or fund cybersecurity incident has occurred or is occurring with respect to itself or any of its clients that are covered clients.

“In other words, an adviser must report within 48 hours after having a reasonable basis to conclude that an incident has occurred or is occurring, and not after definitively concluding that an incident has occurred or is occurring. The 48-hour period would give an adviser time to confirm its preliminary analysis and prepare the report while still providing the Commission with timely notice about the incident.” Proposed Rule at 13537.

41

41



## Financial Impact: ex ante and ex post

- Ex ante public disclosure: what is the financial impact on the business in containing and remediating the incident?
- Ex post financial consequences of disclosing to external stakeholders and the public? Loss of market share, client assets, redemptions; public relations, legal, insurance fees in handling public fallout
- Ransomware and other threats to release confidential data

42

42



## External Experts

- Financial impact of retaining forensic, legal, accountants, and other consultants?
- Is an internal investigation needed? If so, who should conduct it? What will be its scope? Who will be data custodians targeted for discovery? Written or oral report? Employee sanctions within scope?
- Maintaining and preserving attorney client privilege – consider off band communication channel if your client is a publicly-owned entity with statutory obligations to disclose internal communications

43

43



## Additional Reporting Considerations

### Law Enforcement

- Report Ransomware attacks to the FBI's Internet Crime Complaint Center (IC3)
- Cybersecurity & Infrastructure Security Agency – incident reporting system
- U.S. Secret Service

44

44



## Practical Practice Pointers - Policies

- Before embarking on writing your firm's Cybersecurity Policies and Procedures consider starting with a template.
  - The IAA has Cybersecurity Policies and Procedures templates available to its members!
- Review and revise BCP-DR Policies and Procedures as part of the exercise of adopting and implementing written cybersecurity policies and procedures

45

45



## Practical Practice Pointers - Vulnerability Management

- Enforce centralized and timely patch management on endpoints and servers
- Update firmware on all devices and network appliances
- Require your tech staff or MSP to provide vulnerability reports using the Common Vulnerability Scoring System (CVSS)
- Critical or High CVSS scores should be addressed in a timely fashion (e.g., could be false positives) or remediated
- Retain a qualified service provider reasonably independent of your MSP to perform a Penetration Test at least annually

46

46



## Practical Practice Pointers - Identity

- Employ Multi-Factor Authentication on **all** critical apps
- Utilize Single Sign On to secure and centralize logins
- Monitor and alert on abnormal identity behavior
- Practice least privilege and strictly limit privileged access to sensitive servers and data bases (e.g., active directory). SQL data bases should be configured “read only” for general use and availability with only limited privileged users able to read and write data.
- Practice Defense-in-depth: backup data frequently and backup the backup
- Label data according to degree of confidentiality and treat accordingly

47

47



## Practical Practice Pointers - Email

- Exercise caution upon receipt of unsolicited, unexpected or suspicious emails; inquire if your email servers have installed DKIM, DMARC, and SPF.
- Install a strong spam filter with advanced phish and spoof protection
- BOLO for sophisticated phishing attempts and social engineering
- Utilize a security awareness training and phish testing program

48

48



## Practical Practice Pointers - Network

- Configure Firewalls according to your risk appetite
- If feasible, consider establishing network segmentation to segregate sensitive company-related network traffic from other less sensitive (e.g., DMZ) or non-company traffic
- Be aware that IoT devices can be vulnerability vectors (e.g., printers, webcams, remote thermostats)

49

49



## Practical Practice Pointers - Web

- Always be sure you're on the intended site before entering any information.
- Be cautious about websites that do not have a valid certificate issued by a trusted authority, which means information (such as passwords or credit cards) will be securely sent to the site and cannot be intercepted. How can you tell?
- Exercise extreme caution of Microsoft Office attachments that prompt users to enable macros
- Apply symmetric encryption whenever possible (e.g., password protect sensitive documents when transmitting over the internet)

50

50



## Practical Practice Pointers - Endpoints

- Before discarding old computers ensure that all data on the equipment is professionally wiped
- Unless you can afford in-house expertise, ensure that your MSSP is able to remotely maintain, monitor, configure, patch, access, re-boot, and if needed, wipe data on all your employee endpoints
- Always Log out of company workstations when done or when absent

51

51



## Practical Practice Pointers - Vendor Due Diligence

- Service Providers: inquire and request summary of their BCP-DR policies and procedures; critical suppliers should submit an annual SOC audit report covering internal controls and cybersecurity readiness
- Any service provider with access to your network must be thoroughly and regularly vetted and comply with the same company policies and procedures that apply to employees

52

52



## Practical Practice Pointers - Cyber insurance

- Review and update your firm's point of contact with your cybersecurity insurer and be ready to contact and notify the carrier and insurance broker in case an incident warrants filing a claim
- Cyber insurers often provide additional services and features to mitigate risks – read the policy and take advantage of them
- Unless you have in-house expertise, leverage your insurance broker to help you to fully understand the coverage, the retention amounts, and especially the exclusions
- Review and update your firm's point of contact with your MSP and be prepared to respond in the event of a cyber incident (i.e., BCP-DR).

53

53



## Questions?

54

54

# 2024 / Investment Adviser Compliance Conference

MARCH 6-8 / WASHINGTON, DC

**EFFECTIVE STRATEGIES  
& BEST PRACTICES**

IAA

IAA Investment Adviser Compliance Conference

March 6-8, 2024

**Cybersecurity for Medium and Smaller Firms**

*I. SEC's Proposed Cybersecurity Risk Management Rules*

a. Regulation

- i. SEC's Proposed Cybersecurity Risk Management Rules Recent Division of Examinations Risk Alerts and Division of Enforcement cases Reasonably Designed Cybersecurity Policies and Procedures Practical Practice Pointers

<https://www.sec.gov/files/rules/final/2023/33-11216.pdf>

- ii. SEC's Proposed Cybersecurity Risk Management Rules Recent Division of Examinations Risk Alerts and Division of Enforcement cases Reasonably Designed Cybersecurity Policies and Procedures Practical Practice Pointers

<https://www.sec.gov/files/rules/final/2023/33-11216.pdf>

1. Investment Adviser Cybersecurity Incident Report

b. Relevant Comment Letters

- i. IAA Comment Letter to SEC Regarding Adviser Proposals

<https://www.investmentadviser.org/resources/iaa-comment-letter-to-sec-regarding-adviser-proposals/>

- ii. ICI Comment Letter on SEC's Cybersecurity Risk Management

<https://www.ici.org/letters/23-cl-sec-cyber-proposal>

*II. Recent Division of Examinations Risk Alerts and Division of Enforcement cases*

- a. OCIE Cybersecurity and Resiliency Observations (2019)

<https://www.sec.gov/files/OCIE%20Cybersecurity%20and%20Resiliency%20Observations.pdf>

- b. Observations from Cybersecurity Examinations (2017)

<https://www.sec.gov/files/observations-from-cybersecurity-examinations.pdf>

- c. SEC Announces Three Actions Charging Deficient Cybersecurity Procedures  
<https://www.sec.gov/news/press-release/2021-169>
- d. SEC Proposes New Requirements to Address Cybersecurity Risks to the U.S. Securities Markets  
<https://www.sec.gov/news/press-release/2023-52>
- e. Risk Alert: Investment Adviser and Broker-Dealer Compliance Issues Related to Regulation S-P - Privacy Notices and Safeguard Policies  
<https://www.sec.gov/ocie/announcement/ocie-risk-alert-regulation-s-p>
- f. Cybersecurity Risk Governance, SEC Agency Rule List – Spring 2023  
<https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202304&RIN=3235-AM89>

### III. *Reasonably Designed Cybersecurity Policies and Procedures*

- a. National Institute of Standards and Technology - Framework  
<https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final>
- b. Security Information and Event Management Systems (SIEMs) – a single pane of glass to monitor the attack surface with automated alerts
- c. Security Operations Center (SOC) – a team to detect, respond and recover
- d. Data Loss Prevention Systems – detect potential exfiltration
- e. Network Traffic Analysis – detect DDoS attacks

### IV. *Practical Practice Pointers*

- a. NIST Self Testing Tool  
[https://expel.com/expel-self-scoring-tool-for-nist-csf/?utm\\_medium=sem&utm\\_source=google&utm\\_campaign=dgt-comm-mident-ent-mofu-bofu-nist-go-mofu-dtb-nist&utm\\_content=marketing-content-nist-csf-tool&bt=499708119833&bk=nist%20framework&bm=b&bn=g&bg=568941875](https://expel.com/expel-self-scoring-tool-for-nist-csf/?utm_medium=sem&utm_source=google&utm_campaign=dgt-comm-mident-ent-mofu-bofu-nist-go-mofu-dtb-nist&utm_content=marketing-content-nist-csf-tool&bt=499708119833&bk=nist%20framework&bm=b&bn=g&bg=568941875)

[27&gad\\_source=1&gclid=CjwKCAiA\\_tuuBhAUEiwAvxkgTtHcs8ohrVrDs4VbUx5VxoDR8UX8afV6T3c3jOQUtaEismC6kaegFRoCZaQQAvD\\_BwE](https://www.acaglobal.com/our-solutions/cybersecurity-privacy-risk)

b. ACA Vantage – Cybersecurity Self Assessment

i. <https://www.acaglobal.com/our-solutions/cybersecurity-privacy-risk>

# 2024 Investment Adviser Compliance Conference

MARCH 6-8 / WASHINGTON, DC

EFFECTIVE STRATEGIES & BEST PRACTICES

## Cyber Programs: Larger Firms

Katie Gorham / Capital Group

Kathryn Mellinger / Vanguard

E.J. Yerzak / SalusGRC

Charu Chandrasekhar / Debevoise & Plimpton

1



2024 Investment Adviser Compliance Conference

EFFECTIVE STRATEGIES & BEST PRACTICES

## RIAs and Funds

Proposed Rules would require:

- New 48 hour incident notification requirement on Form ADV-C
- Cybersecurity risk management policies and procedures
- Annual review and written reports
- New disclosure and recordkeeping requirements



2



## BDs and Other “Market Entities”

Proposed Rules would require:

- Immediate incident notification to SEC for all entities and additional 48 hour incident notification for “Covered Entities” (“CEs”)
- Public disclosure of risks and incidents for CEs
- Cybersecurity program requirements, with additional requirements for CEs
- New recordkeeping requirements



3



## Amendments to Reg S-P

Proposed Rules would require:

- 30 day Customer incident notification
- Incident response plan
- Expansion of Safeguards and Disposal Rules
- Recordkeeping
- Privacy notice amendments



4

**IAA** 2024 Investment Adviser Compliance Conference **EFFECTIVE STRATEGIES & BEST PRACTICES**

## SEC 2024 EXAMS Priorities

1. Information security and operational resiliency
2. Reg S-ID policies and procedures
3. Firmwide cybersecurity, across branch offices
4. Vendor and third-party risk management
5. AI risks

5

**IAA** 2024 Investment Adviser Compliance Conference **EFFECTIVE STRATEGIES & BEST PRACTICES**

## Cybersecurity Trends

 Ransomware	 Risks from AI
 Third Party Risks and Supply Chain Attacks	 Attacks Targeting Sensitive Financial Events
 Targeting of Individual Executives	 Nation State Attacks

6

IAA 2024 Investment Adviser Compliance Conference EFFECTIVE STRATEGIES & BEST PRACTICES

## Cybersecurity Risks of Generative AI

### Risks to AI Systems

- Increased attack surface for data breach or misuse
- Adversarial attacks to bypass controls
- Model poisoning

### Risks Caused by AI Systems

- Deepfakes
- Automating social engineering
- Generating malicious code
- Evading detection systems

7

IAA 2024 Investment Adviser Compliance Conference EFFECTIVE STRATEGIES & BEST PRACTICES

## Proposed Outsourcing Rule

- ✓ Due diligence
- ✓ Monitoring
- ✓ Recordkeeping

- ✓ Disclosures and census-type information  
(Form ADV, Part 1A)
- ✓ Third-Party recordkeeping

8



9

ARTIFICIAL INTELLIGENCE

## The SEC's 2024 Examination Priorities: Continued Scrutiny of Cybersecurity Policies and Procedures

BY: CHARU CHANDRASEKHAR, LUKE DEMBOSKY, AVI GESSER, KRISTIN SNYDER, EREZ LIEBERMANN,  
MATT KELLY AND MENGXI XU - OCTOBER 18, 2023



On October 16, 2023, the SEC's Division of Examinations ("EXAMS") issued its 2024 Examination Priorities (the "2024 Priorities"). The 2024 Priorities reflect the Commission's continued scrutiny of information security and operational resiliency at registrants and the risks posed by third-party service providers, as well as new attention to artificial intelligence and other forms of so-called emerging financial technology.

- 1. Information Security and Operational Resiliency:** EXAMS stated that "[o]perational disruption risks remain elevated due to the proliferation of cybersecurity attacks," among other factors. Accordingly, cybersecurity remains a "perennial focus area" for registrant examinations, and EXAMS will continue to review registrants' practices to protect "mission-critical" services and to protect investor

data and assets. The Division will additionally focus on registrants' policies and procedures, internal controls, oversight of third-party vendors, governance practices, and responses to cyber-related incidents, including those related to ransomware attacks.

2. **Reg S-ID Policies and Procedures:** In connection with such exams, EXAMS will consider staff training regarding Regulation S-ID (the Identity Theft Red Flags Rule) and the adequacy of policies and procedures to protect customer records and information.
3. **Firmwide Cybersecurity Across Branch Offices:** Because many registrants have a main office and multiple other offices, EXAMS will continue to look at practices to prevent account intrusions and safeguard customer records and information (such as personally identifiable information) across multiple offices.
4. **Vendor Risk Management:** EXAMS will continue to review vendor and third-party cybersecurity risk management, considering several different topics, including: the cybersecurity risks posed by third-party vendors; the security and integrity of vendor products and services; how registrants identify and assess vendor-related risks to essential business operations; and the unauthorized use of such providers. Consistent with its policy mandate, the Division will examine the concentration risk associated with third-party vendors, including how registrants are managing this risk and the potential U.S. securities marketplace impact.
5. **Artificial Intelligence:** In the context of crypto assets and emerging financial technology products ("fintech"), the Division will continue to examine new products and services and sales practices with an emphasis on technological compliance and marketing features for online accounts. In this context, the Division "remains focused on certain services, including automated investment tools, artificial intelligence, and trading algorithms or platforms, and the risks associated with the use of emerging technologies and alternative sources of data."

## Takeaways

The continued focus in the 2024 Priorities on cybersecurity issues suggests that the Staff expects firms to continue demonstrating proactive efforts to reduce both the frequency and magnitude of cybersecurity incidents.

In previous posts regarding the SEC's cybersecurity priorities (including [here](#) and [here](#)), we identified multiple takeaways for firms based on SEC enforcement actions and guidance. These included: (1) Close Out Major Issues, (2) Prepare for the Need to Respond to and Recover from Ransomware, (3) Support and Document Senior-Level Engagement, (4) Perform Tabletop Exercises, (5) Provide Role-Based Employee Training, (6) Take Steps to Mitigate Risks from Credential Stuffing, (7) Enhance Programmatic Vendor Management, (8) Adhere to Cybersecurity Plans and Policies, (9) Revisit and Enhance Disclosure Controls, Where Necessary, and (10) Prepare for Supply-Chain and other Vendor Attacks.

The 2024 Priorities underscore the importance of these same measures, to the extent not already addressed, and they suggest firms should also consider the following:

1. **Revisit Business Continuity and Resiliency Preparations.** Firms should consider whether there are additional steps that they can and should take to prepare for, and minimize the impact of, business disruptions caused by cybersecurity incidents. Given the evolving tactics of threat actors, who often work to compromise the viability of recovery options in the course of executing an attack, various backup strategies may be less resilient and less helpful than anticipated in the event of a live incident. Steps to consider therefore include re-assessing the timeliness, security, and availability of backups, as well as the availability of fail-over systems that could be used to continue or restore operations, if needed.
2. **Reconsider Identity Theft Prevention Program Design and Implementation.** In light of the Staff's continued focus on firms' safeguarding and Reg S-ID obligations, firms should consider whether they have in place written policies and procedures reasonably designed to detect and address red flags of identity theft. They also should consider whether they conduct effective and appropriate training for employees to support the firm's compliance with obligations regarding customer accounts and information.
3. **Analyze Differences Between and Among Branches and Home Offices.** Firms should consider whether there are significant differences between the application of their cyber- and information-security policies, procedures, and controls between and among their various branches and offices. Any such differences should be examined carefully to ensure they are reasonable in light of the circumstances, and (if necessary) remediated.
4. **Vendor Risk Management.** Firms should consider the design and effectiveness of their third-party and vendor risk management programs. Among other risk areas to consider, firms should contemplate both (a) the risk of supply-chain and hub-and-spoke attack strategies, through which threat actors seek to compromise firm environments by taking advantage of third-party and vendor connectivity, and (b) the risk to sensitive or strategically important information held by third parties and vendors. Firms also may want to revisit the extent and prioritization of vendor diligence and oversight to test for compliance with cybersecurity-related terms and conditions, as well as the adequacy of documentation and records reflecting these efforts.

To subscribe to the Data Blog, please [click here](#).

The [Debevoise Artificial Intelligence Regulatory Tracker](#) ("DART") is now available for clients to help them quickly assess and comply with their current and anticipated AI-related legal obligations, including municipal, state, federal, and international requirements.

The cover art used in this blog post was generated by DALL-E.

AI

AI COMPLIANCE

AI REGULATION

CYBERSECURITY

SEC





### **Charu Chandrasekhar**

Charu A. Chandrasekhar is a litigation partner based in the New York office and a member of the firm's White Collar & Regulatory Defense and Data Strategy & Security Groups. Her practice focuses on securities enforcement and government investigations defense and cybersecurity regulatory counseling and defense.



---

### **Luke Dembosky**

Luke Dembosky is a Debevoise litigation partner based in the firm's Washington, D.C. office. He is Co-Chair of the firm's Data Strategy & Security practice and a member of the White Collar & Regulatory Defense Group. His practice focuses on cybersecurity incident preparation and response, internal investigations, civil litigation and regulatory defense, as well as national security issues. He can be reached at [ldembosky@debevoise.com](mailto:ldembosky@debevoise.com).



---

### **Avi Gesser**

Avi Gesser is Co-Chair of the Debevoise Data Strategy & Security Group. His practice focuses on advising major companies on a wide range of cybersecurity, privacy and artificial intelligence matters. He can be reached at [agesser@debevoise.com](mailto:agesser@debevoise.com).



---

### **Kristin Snyder**

Kristin Snyder is a litigation partner and member of the firm's White Collar & Regulatory Defense Group. Her practice focuses on securities-related regulatory and enforcement matters, particularly for private investment firms and other asset managers.



---

### **Erez Liebermann**

Erez is a litigation partner and a member of the Debevoise Data Strategy & Security Group. His practice focuses on advising major businesses on a wide range of complex, high-impact cyber-incident response matters and on data-related regulatory requirements. Erez can be reached at [eliebermann@debevoise.com](mailto:eliebermann@debevoise.com)

---

## Matt Kelly

Matthew Kelly is a litigation counsel based in the firm's New York office and a member of the Data Strategy & Security Group. His practice focuses on advising the firm's growing number of clients on matters related to AI governance, compliance and risk management, and on data privacy. He can be reached at [makelly@debevoise.com](mailto:makelly@debevoise.com)



---

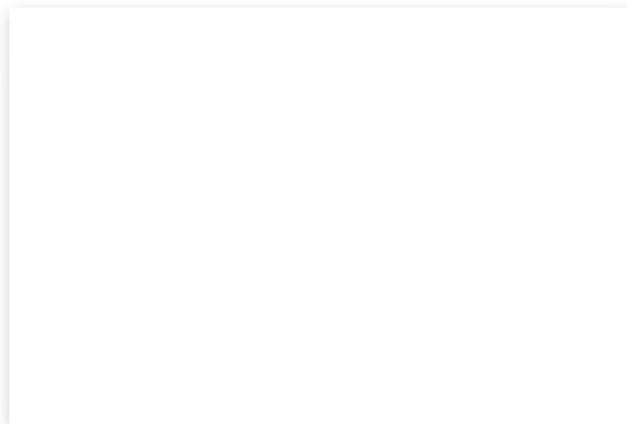
## Mengyi Xu

Mengyi Xu is an associate in Debevoise's Litigation Department and a Certified Information Privacy Professional (CIPP/US). As a member of the firm's interdisciplinary Data Strategy & Security practice, she helps clients navigate complex data-driven challenges, including issues related to cybersecurity, data privacy, and data and AI governance. Mengyi's cybersecurity and data privacy practice focuses on incident preparation and response, regulatory compliance, and risk management. She can be reached at [mxu@debevoise.com](mailto:mxu@debevoise.com).



---

## Related Posts



**Risk of AI Abuse by Corporate Insiders Presents Challenges for Compliance Departments**

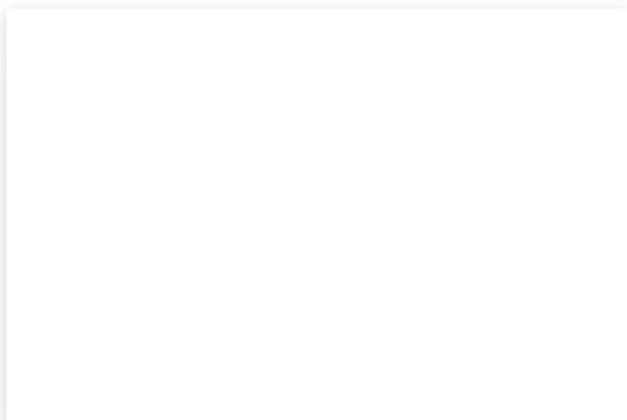
FEBRUARY 19, 2024

---



## **DOJ Announces Initiative to Combat AI-Assisted Crime**

**FEBRUARY 16, 2024**



## **Webcast: NYDFS AI Requirements for Insurers Using AI or External Data**

**FEBRUARY 5, 2024**

# SEC Adopts New Cybersecurity Rules for Issuers

July 27, 2023

On July 26, 2023, the SEC adopted the long-anticipated final rules on cybersecurity risk management, strategy, governance, and incident disclosure for issuers. The new rules are part of the SEC's larger efforts focused on cybersecurity regulation with a growing universe of rules aimed at different types of SEC registrants, including: (i) its proposed cybersecurity rules for [registered investment advisers and funds](#) and [market entities, including broker-dealers](#), (ii) its proposed [amendments to Reg S-P](#) and [Reg SCI](#) and (iii) existing cybersecurity obligations under SEC regulations, including Reg S-P, Reg S-ID, and the recently amended Form PF.

## KEY REQUIREMENTS

The rules introduce three new types of disclosure requirements relating to: (1) material cybersecurity incidents, (2) cybersecurity risk management processes and (3) cybersecurity management and governance.

- **Current Disclosure of Material Cybersecurity Incidents.** The rules require registrants to disclose certain information about a material cybersecurity incident under new Item 1.05 of Form 8-K ("Item 1.05") within four business days of determining that a cybersecurity incident it has experienced is material. The determination of materiality is to be made "without unreasonable delay," as opposed to "as soon as reasonably practical" as was proposed.
  - *Materiality Analysis:* The final rules revise the materiality analysis in the proposed rules, and require disclosure of the material aspects of the nature, scope, timing of the incident and the material impact or reasonably likely material impact of the incident on the registrant (including its financial condition and results of operations), to the extent the information is known at the time of the Form 8-K filing. A registrant need not disclose specific or technical information about its planned response to the incident or its cybersecurity systems, related networks and devices, or potential system

---

vulnerabilities in such detail as would impede the registrant's response or remediation of the incident.

- *Form 8-K Amendment:* Notably, to the extent any required information is not determined or is unavailable at the time of the required filing, registrants are required to include a statement to this effect in the Form 8-K and then file a Form 8-K amendment containing such information within four business days after the registrant determines such information or within four business days after such information becomes available. This is a departure from the proposed rules that would have required registrants to update incident disclosures in Forms 10-K or 10-Q.
- *Series of Related Unauthorized Occurrences:* The rules adopt a definition of "cybersecurity incident" that extends to "a series of related unauthorized occurrences." Accordingly, if a registrant determines that it has been materially affected by a series of related cyber intrusions, Item 1.05 may be triggered even if the material impact or reasonably likely material impact of each individual intrusion is by itself immaterial. This replaces the proposed rule which would have required disclosure when a series of previously undisclosed individually immaterial cybersecurity incidents became material in the aggregate.
- *National Security and Public Safety Delay Provision:* The final rules introduce a very narrow national security and public safety delay provision, such that disclosure of a cybersecurity incident may be delayed, initially for up to 30 days, if the United States Attorney General determines that immediate disclosure would pose a substantial risk to national security or public safety and notifies the Commission of such determination in writing. Two subsequent delay periods of 30 days and 60 days (in extraordinary circumstances) each may be sought in a similar fashion. If the Attorney General indicates that further delay is necessary beyond the final 60-day delay, the Commission will consider additional requests for delay and may grant such delay through a Commission exemptive order.
- *Foreign Private Issuers:* The rules amend Form 6-K to require foreign private issuers ("FPIs") that are required to furnish such reports, to disclose on Form 6-K material cybersecurity incidents that they disclose or otherwise publicize in a foreign jurisdiction, to any stock exchange or to security holders, promptly after the material contained in the report is made public.
- *Safe Harbors:* Consistent with the proposed rules, the final rules provide for certain limited safe harbors, including from liability under Exchange Act

---

Section 10(b) and Rule 10b-5 thereunder and protection against loss of Form S-3 eligibility, in each case for filing failures related to Item 1.05 of Form 8-K.

A comparison of the final version of Item 1.05 of Form 8-K with the proposed version is [here](#).

- **Periodic Disclosure of Cybersecurity Risk Management Processes.** Registrants will be required to make several disclosures related to cybersecurity risk management programs in their Forms 10-K and 10-Q, including whether and how registrants assess, identify and manage material risks, whether the registrant engages any third-parties, auditors or consultants in connection with such processes and whether the registrant has processes in place to oversee and identify third-party risk, which represents a more streamlined disclosure requirement when compared to the rules as proposed. Notably, the final rules substitute disclosure of “policies and procedures” for the term “processes,” which the SEC believes more fully encompasses registrants’ cybersecurity practices. Registrants will need to describe whether any risks for cybersecurity threats, current or previous, have materially affected or are likely to materially affect business strategy, operations or financial conditions. Parallel requirements apply to FPIs in respect of their Form 20-F filings.
- **Cybersecurity Management & Governance.** Registrants, including FPIs, will be required to describe the board’s oversight of and management’s role in assessing and managing risks posed by cybersecurity threats in their Forms 10-K, 10-Q and 20-F, as applicable. The final rules streamline the enumerated disclosure elements initially proposed. With respect to management’s role, registrants must address, to the extent applicable, which management positions or subcommittees are responsible for assessing and managing such risks, including the relevant expertise of such persons; the process by which management or their committees are informed about and monitor the prevention, detection, mitigation and remediation of cybersecurity incidents and whether such person or committees report information about such risks to the board or a subcommittee of the board. Registrants are required to disclose whether members of management have prior work experience, education, or knowledge, skills or other background in cybersecurity; to the extent they are involved in cybersecurity risk management. This is a departure from the proposed rules, which would have required similar information in respect of directors. If applicable, registrants will be required to identify the board committee or subcommittee responsible for overseeing cybersecurity risks and describe the process by which they are informed of cybersecurity risks.
- **Effective Date.** With respect to Item 1.05 and the new Form 6-K requirements, registrants other than small reporting companies must begin complying on the later

---

of 90 days after the date of publication or December 18, 2023. Smaller reporting companies will have an additional 180 days and must begin complying with Form 8-K Item 1.05 on the later of 270 days from the effective date of the rules or June 15, 2024. With respect to the disclosures required in Form 10-Q and 10-K and the comparable requirements in Form 20-F, registrants must provide disclosures beginning with annual reports for fiscal years ending on or after December 15, 2023. Inline XBRL tagging must begin one year after initial compliance with the related disclosure requirement.

The final rules are available [here](#).

We will publish a more detailed analysis of the impact of the new rules in the coming weeks.

To subscribe to the Data Blog of our Data Strategy and Security practice, please click [here](#).

\* \* \*

Please do not hesitate to contact us with any questions.

---

**NEW YORK**



Charu A. Chandrasekhar  
cachandrasekhar@debevoise.com



Avi Gesser  
agesser@debevoise.com



Matthew E. Kaplan  
mekaplan@debevoise.com



Erez Liebermann  
eliebermann@debevoise.com



Benjamin R. Pedersen  
brpedersen@debevoise.com



Paul M. Rodel  
pmrodel@debevoise.com



Steven J. Slutzky  
sjslutzky@debevoise.com



Matt Kelly  
makelly@debevoise.com



Kelly Donoghue  
kgdonoghue@debevoise.com



John Jacob  
jjacob@debevoise.com



Amy Pereira  
apereira@debevoise.com



Chris Duff  
ceduff@debevoise.com

**WASHINGTON, D.C.**



Luke Dembosky  
ldembosky@debevoise.com

**SAN FRANCISCO**



Mengyi Xi  
mxu@debevoise.com

# Hackers Turned Whistleblowers: SEC Cybersecurity Rules Weaponized Over Ransom Threat

November 20, 2023

On November 7, 2023, the prolific ransomware group AlphV (a/k/a “BlackCat”) reportedly breached software company MeridianLink’s information systems, exfiltrated data and demanded payment in exchange for not publicly releasing the stolen data. While this type of cybersecurity incident has become increasingly common, the threat actor’s next move was less predictable. AlphV filed a whistleblower tip with the U.S. Securities and Exchange Commission (the “SEC”) against its victim for failing to publicly disclose the cybersecurity incident. AlphV wrote in its complaint:<sup>1</sup>

We want to bring to your attention a concerning issue regarding MeridianLink’s compliance with the recently adopted cybersecurity incident disclosure rules. It has come to our attention that MeridianLink, in light of a significant breach compromising customer data and operational information, has failed to file the requisite disclosure under Item 1.05 of Form 8-K within the stipulated four business days, as mandated by the new SEC rules.

As we have previously [reported](#), the SEC adopted final rules mandating disclosure of cybersecurity risk, strategy and governance, as well as material cybersecurity incidents. This includes new Item 1.05 of Form 8-K, which, beginning December 18, will require registrants to disclose certain information about a material cybersecurity incident within four business days of determining that a cybersecurity incident it has experienced is material. Though AlphV jumped the gun on the applicability of new Item 1.05, its familiarity with, and exploitation of their target’s public disclosure obligations is a further escalation in a steadily increasing trend of pressure tactics by leading ransom groups.

---

<sup>1</sup> A copy of the submission was shared by the threat actor with DataBreaches on November 15, 2023 and is available [here](#).

---

### WHY WOULD A THREAT ACTOR BLOW THE WHISTLE ON THEIR OWN CRIME?

The percentage of companies that now make extortion payments to recover access to encrypted systems or stop stolen data from being posted publicly is on the decline.<sup>2</sup> Threat actors are accordingly resorting to increasingly aggressive harassment techniques to extract such payments from victims. This move is an extension of those aggressive pressure tactics. Large threat groups, like BlackCat/AlphV, are sophisticated and aware of regulatory, financial and other company pressures, and have in the past threatened to alert regulators or otherwise have taken to social media or other public outlets to pressure victims to pay. In this instance, the threat actor is attempting specifically to leverage the SEC's regulations to its advantage by increasing the cost to their targets of refusing to pay ransom—namely, by increasing the likelihood that the regulator will investigate the cybercrime victim, which can be incredibly costly, time consuming and damaging to a company's reputation and business.

### HOW WILL THE SEC RESPOND?

Unsurprisingly, the SEC has not yet issued a statement regarding the AlphV whistleblowing complaint, and it is not yet clear how the SEC will handle whistleblower complaints by threat actors. However, this move could arguably result in an increase in the filing of such whistleblower tips by such threat actors and, accordingly, could more generally trigger increased investigative scrutiny into companies that fall victim to cybercrime, including investigations of whether their public disclosures or disclosure controls were deficient in connection with the cybersecurity incident. This will become increasingly true as the new rules come into effect and require timely disclosure of material cybersecurity incidents.

### WILL THE THREAT ACTOR BE ENTITLED TO A WHISTLEBLOWER AWARD UNDER THE SEC'S RULES?

Probably not. Rules 21F-6 and 21F-16 under the Securities Exchange Act of 1934 provide for a reduction in whistleblower awards based on culpability and other factors, assuming that there is an enforcement action resulting from the tip exceeding \$1 million in monetary remedies.

In any event, to be eligible for payment, a whistleblower must be a natural person and must disclose their identity on form WB-APP. (This would be true even if the applicant initially submitted their complaint on an anonymous basis. See §§ 240.21F-7(b) and

---

<sup>2</sup> *Ransom Monetization Rates Fall to Record Low Despite Jump in Average Ransom Payments*, COVEWARE (July 21, 2023), <https://www.coveware.com/blog/2023/7/21/ransom-monetization-rates-fall-to-record-low-despite-jump-in-average-ransom-payments>.

---

240.21F-10(c).) As such, even if a threat actor were otherwise entitled to an award as a matter of law, the procedural requirements for recovery make it unlikely that they would ever seek payment, given their interest in avoiding personal liability for the underlying criminal conduct. Therefore, it is less likely that a threat actor would file a complaint with the hope of recovering an award and more likely that they would view the filing simply as further means of supporting their extortion of current and future victims.

### HOW SHOULD PUBLIC COMPANIES PREPARE TO RESPOND?

Stand by your disclosure controls and materiality determination, and be prepared to respond to regulators, customers and other stakeholders from a crisis communications standpoint. With the compliance date for the new SEC cybersecurity rules looming, public companies should ensure their cybersecurity incident response plan and disclosure controls and procedures are ready. Documenting a thorough and deliberative materiality determination, at each point in a cybersecurity incident response at which significant new facts become available, will be of paramount importance to support Item 1.05 disclosure decisions. Lowering the bar for Item 1.05 disclosure—or, worse, paying a ransom in response to this type of threat—will ultimately set a dangerous precedent for future 8-K disclosures.

For more information about the SEC's cybersecurity rules, see our prior updates:

- [SEC Adopts New Cybersecurity Rules for Issuers](#)
- [SEC Adopts New Cybersecurity Rules for Issuers – Part 2 Key Takeaways.](#)

We will continue to monitor developments in this area.

To subscribe to the Data Blog of our Data Strategy and Security practice, please click [here](#).

\* \* \*

Please do not hesitate to contact us with any questions.



**Andrew J. Ceresney**  
Partner, New York  
+1 212 909 6947  
aceresney@debevoise.com



**Charu A. Chandrasekhar**  
Partner, New York  
+1 212 909 6774  
cchandrasekhar@debevoise.com



**Luke Dembosky**  
Partner, Washington, D.C.  
+1 202 383 8020  
ldembosky@debevoise.com



**Avi Gesser**  
Partner, New York  
+1 212 909 6577  
agesser@debevoise.com



**Matthew E. Kaplan**  
Partner, New York  
+1 212 909 7334  
mekaplan@debevoise.com



**Erez Liebermann**  
Partner, New York  
+1 212 909 6224  
eliebermann@debevoise.com



**Benjamin R. Pedersen**  
Partner, New York  
+1 212 909 6121  
brpedersen@debevoise.com



**Steven J. Slutzky**  
Partner, New York  
+1 212 909 6036  
sjslutzky@debevoise.com



**Jonathan R. Tuttle**  
Partner, Washington, D.C.  
+1 202 383 8124  
jrtuttle@debevoise.com



**Matt Kelly**  
Counsel, New York  
+1 212 909 6990  
makelly@debevoise.com



**Kelly Donoghue**  
Associate, New York  
+1 212 909 6145  
kgdonoghue@debevoise.com

# SEC Adopts New Cybersecurity Rules for Issuers – Part 2 Key Takeaways

August 7, 2023

On July 26, 2023, the SEC adopted long-anticipated [final rules](#) on cybersecurity risk management, strategy, governance and incident disclosure for issuers (“Final Rules”). We summarized the key obligations under the Final Rules, and changes from the Proposing Release,<sup>1</sup> in our [July 27, 2023 update](#). In this companion update, we discuss key takeaways across three areas for issuers to consider:

- (1) Disclosure of material cybersecurity incidents: The Final Rules create a four-business-day obligation to disclose material incidents. Issuers should consider developing a well-informed and deliberative process to support the materiality analysis well before an incident occurs; adherence to internal practices and disclosure controls and procedures will aid issuers in establishing good faith compliance with the disclosure obligation.
- (2) Cybersecurity risk management and strategy: The Final Rules require issuers to disclose more granular details of their cyber risk management than is common among issuers at present. Issuers should review their cybersecurity processes, how these processes are integrated with the issuer’s overall risk management program, and how these relate to the issuer’s cybersecurity risk profile to consider how the required disclosure will appear in the face of greater public scrutiny.
- (3) Cybersecurity governance: The disclosure of senior management’s and the board’s roles in managing and overseeing cybersecurity will up the ante on expectations for cybersecurity oversight, including attracting, developing and retaining cybersecurity talent. Ensuring that both senior management and the board are informed and that their involvement is well-documented will be more important than ever.

---

<sup>1</sup> 87 Fed. Reg. 16590 (Mar. 23, 2022).

---

## Disclosure and Amendment of Material Cybersecurity Incidents

Domestic issuers are required to disclose certain information about a material cybersecurity incident under new Item 1.05 of Form 8-K (“Item 1.05”) within four business days of determining that a cybersecurity incident it has experienced is material. Cybersecurity incident disclosures should include a description of “the material aspects of the nature, scope, and timing of the incident, and the material impact or reasonably likely material impact on the issuer, including its financial condition and results of operations.” The determination of materiality is to be made “without unreasonable delay” (as opposed to “as soon as reasonably practical,” as was proposed). Foreign private issuers (“FPIs”) that are required to furnish a Form 6-K must disclose on Form 6-K material cybersecurity incidents that they disclose or otherwise publicize in a foreign jurisdiction, to any stock exchange or to their security holders, promptly after the material contained in the report is made public.

- **Review the incident response plan and procedures to ensure that the materiality analysis is appropriately sequenced alongside other incident response activities and that materiality determination protocols are well-informed, deliberative and documented.** The Final Rules changed the required timing of the materiality determination from “as soon as reasonably practicable” to “without unreasonable delay.” In doing so, the Commission acknowledged that materiality determinations may take time and require “an informed and deliberative process.” However, it warned that “though the determination need not be rushed prematurely, it also cannot be unreasonably delayed in an effort to avoid timely disclosure.”<sup>2</sup>

Taken together, an issuer should consider: (1) carefully reviewing its incident response plan and procedures to ensure that the materiality determination is appropriately sequenced alongside incident fact finding, in accordance with the nature and scope of any given incident (e.g., earlier if involving key systems and information or if a large volume of important data are implicated); (2) ensuring that its incident response resources are allocated such that any need for early information sharing with third-party stakeholders would not result in unreasonable delay of the materiality analysis; and (3) ensuring that there are well-reasoned bases for any changes to the incident response plans—including as it relates to any contemplated revisions to (a) incident severity assessment time, (b) criteria for escalation to management or board committees in charge of public disclosures or (c) materiality

---

<sup>2</sup> Rule Release, 37. The Commission’s cited examples in the Rule Release are instructive on this point: For instance, for incidents that (1) impact key systems and information (“crown jewels”) and (2) involve unauthorized access to or exfiltration of large quantities of particularly important data, the materiality determination should not be delayed because the issuer does not have complete information, is not able to determine the full extent of the incident, or needs to continue to investigate. The Commission also specifically warned against an issuer revising its existing incident response policies and procedures to support a delayed materiality disclosure.

determination protocols and processes, which should be well-informed and deliberative.

- **Develop a disclosure analysis framework that incorporates both qualitative and quantitative factors, that accounts for the broadened definition for “cybersecurity incident,” and does not disclose information that would impede incident response and remediation.** The Commission noted in the Rule Release accompanying the Final Rule (“Rule Release”) that the focus of the Item 1.05 disclosure should be “primarily on the impacts of a material cybersecurity incident, rather than on [...] details regarding the incident itself.”<sup>3</sup> The Commission also underscored the importance of considering both *qualitative* and *quantitative factors*, and both immediate and longer-term effects, in making such an assessment.<sup>4</sup> The Commission emphasized that a “lack of quantifiable harm does not necessarily mean an incident is not material,”<sup>5</sup> and that a cybersecurity incident involving foreseeable future harms may be material, even if the incident has not yet caused actual harm.

The Final Rules and Rule Release embrace an expansive definition of “cybersecurity incident,” which includes “a series of related unauthorized occurrences,”<sup>6</sup> and “an accidental occurrence [...] even if there is no confirmed malicious activity.”

To satisfy these new disclosure requirements, issuers should consider developing a framework to structure and guide materiality and disclosure analysis and decisions for each incident, accounting for potential serial unauthorized occurrences and accidental occurrences. Such a framework may be incorporated into the issuer’s existing disclosure controls and procedures, and should facilitate a well-informed and deliberative analysis of the incident, such as by mapping to enumerated qualitative and quantitative factors for actual and likely harm.

Issuers should also consider Instruction 4 to Item 1.05 when developing incident disclosures, which provides that issuers “need not disclose specific or technical information about its planned response to the incident or its cybersecurity systems,

---

<sup>3</sup> Rule Release, 29.

<sup>4</sup> Rule Release, 80. The Commission provided certain *illustrative* materiality assessment factors, including: (1) harm to an issuer’s reputation, customer or vendor relationships, and competitiveness (Rule Release, 29); (2) possibility of litigation or regulatory investigations or actions (including by state, Federal authorities, and non-U.S. authorities) (Rule Release, 29-30); (3) data theft (and resulting scope or nature of harm to individuals, customers, or others) (Rule Release, 37), asset loss, IP loss (Rule Release, 29-30); and (4) financial impact (Rule Release, 32).

<sup>5</sup> Rule Release, 37.

<sup>6</sup> Rule Release, 76. (Noting that a series of related unauthorized occurrences could take place and be considered material in the aggregate where (1) “the same malicious actor engages in a number of smaller but continuous cyberattacks related in time and form and against the same company” or (2) multiple actors exploit the same vulnerability and collectively impede the company’s business.)

related networks and devices, or potential system vulnerabilities in such detail as would impede the [issuer's] response or remediation of the incident.”

- **Review policies and procedures regarding the triage and escalation of third-party cybersecurity incidents to enable prompt materiality analysis, where appropriate.** The Commission specifically declined in the Rule Release to exempt “registrants from providing disclosures regarding cybersecurity incidents on third-party systems they use” or to provide “a safe harbor for information disclosed about third-party systems.”<sup>7</sup> As a result, issuers should be prepared to promptly conduct an independent materiality analysis upon becoming aware of a third-party cybersecurity incident, as “disclosure may be required by both the service provider and the customer (registrant), or by one but not the other, or by neither.”<sup>8</sup> To address this requirement, issuers should consider integrating any third-party cybersecurity incident notification and internal escalation processes into their materiality determination protocol and disclosure controls and procedures. The Commission advised that an issuer should only disclose based on information available to it, and that an issuer is not required to conduct additional inquiries outside of its regular channels of communication with third-party service providers pursuant to its contracts and in accordance with the issuer’s disclosure controls and procedures.
- **Track any missing required information in the initial Form 8-K filing and establish a cadence to review ongoing material incidents.** Instruction 2 to Item 1.05 of Form 8-K allows issuers to omit disclosure of otherwise required information from an initial Form 8-K filing where such information is not determined or available at the time. An issuer is required to include a statement to this effect in the initial filing and must provide such information in a Form 8-K amendment within four business days of determining such information, without unreasonable delay, or of such information becoming available. Issuers should therefore (1) closely track any gaps in required elements in the initial Form 8-K filing; (2) establish a cadence for reviewing ongoing material incidents for any of the initially missing information; and (3) when such information is identified, disclose them in an amended Form 8-K.

Note that issuers remain subject to the separate obligation to correct any prior disclosure that is subsequently discovered to be untrue (or to have contained material omissions) *at the time the disclosure was made* (the so-called “duty to correct”). Issuers should also be mindful of the need to update a disclosure that becomes materially inaccurate after it is made (the so-called “duty to update”).<sup>9</sup> The Rule Release acknowledges that issuers do not have a general continuous disclosure

---

<sup>7</sup> Rule Release, 31.

<sup>8</sup> Rule Release, 31.

<sup>9</sup> Rule Release, 52.

obligation, but suggested that issuers “should consider whether they need to revisit or refresh previous disclosure, including during the process of investigating a cybersecurity incident,” particularly in the context of newly required Form 10-K and Form 20-F disclosure, as further described below.

---

## Cybersecurity Risk Management & Strategy

Issuers, including FPIs, will be required to describe on Forms 10-K, 10-Q,<sup>10</sup> and 20-F, as applicable, their cybersecurity risk assessment and management processes and whether risks from cybersecurity threats have materially affected or are reasonably likely to materially affect the issuer. Issuers should review their cyber risk assessment processes and consider how they will appear alongside industry benchmarks and peer issuers’ disclosures.

- **Consider steps to align cybersecurity risk management processes with industry standards.** According to the Rule Release, issuers are expected to disclose “whatever information is necessary, based on their facts and circumstances, for a reasonable investor to understand their cybersecurity processes.”<sup>11</sup> To help position their processes and related disclosure favorably in an established context, issuers should consider benchmarking their cybersecurity risk management processes against industry standards such as the NIST and ISO frameworks. Be prepared to bridge any gaps accordingly.
- **Consider engaging outside vendors to augment cybersecurity capabilities, as appropriate.** Many issuers already outsource elements of their risk management, risk assessment, or monitoring and response to cyber events (e.g., Security Operations Center, Managed Security Service Provider, or incident response vendors, among others). New Item 106(b)(ii) of Regulation S-K requires disclosure of “[w]hether the registrant engages assessors, consultants, auditors, or other third parties in connection with [the firm’s cybersecurity] processes.” Issuers should consider how their disclosures regarding the use of internal versus third-party resources will compare to those of industry peers. Issuers should also take steps to ensure that internal documentation of services provided is consistent with the description of those services in periodic disclosures.

---

<sup>10</sup> While the Final Rule does not contain affirmative Form 10-Q disclosure obligations, the Rule Release references the 2018 Interpretive Release, wherein “the Commission reiterated that registrants must provide timely and ongoing information in periodic reports (Form 10-Q, Form 10-K and Form 20-F) about material cybersecurity risks and incidents that trigger disclosure obligations.” Rule Release, 113-14.

<sup>11</sup> Rule Release, 63.

- **Consider enhancing oversight of third-party service providers and management of cybersecurity risks presented by third-party servicers.** New Item 106(b)(iii) of Regulation S-K requires issuers to disclose “[w]hether the registrant has processes to oversee and identify [material cybersecurity] risks from cybersecurity threats associated with its use of any third-party service provider.” Issuers that do not have existing third-party diligence and oversight processes should consider how their disclosures will compare to those of their peers on this topic. Firms with existing diligence and oversight processes should consider whether there are any gaps in execution or opportunities for enhancement.

---

## Cybersecurity Governance: Management Responsibilities & Board Oversight

Issuers, including FPIs, will be required to describe the board’s oversight of and management’s role and expertise in assessing and managing material risks posed by cybersecurity threats in their Forms 10-K, 10-Q and 20-F, as applicable. Though the Final Rules’ governance requirements are less prescriptive and granular than initially proposed, the Rule Release makes clear that the Commission expects issuers to consider several of the previously prescribed elements — including the frequency of board discussions of cybersecurity risks and designation of CISO — in their disclosures, to the extent material.

- **Consider documenting board discussions with management on cybersecurity.** The Final Rules require issuers to describe the processes by which the board is informed of cybersecurity risks. The Commission noted that discussion of the frequency of board discussions may be relevant to the description of the board processes, and issuers should thus consider inclusion of this information. Issuers should consider instituting a regular cadence (*e.g.*, quarterly) for such reporting where appropriate and should document management presentations to the board to support the disclosure of the board’s oversight processes and the required disclosure under Item 106(c)(2)(iii) for management’s reporting of information to the board.
- **Consider how best to describe management’s cybersecurity expertise and training.** The Final Rules provide a non-exclusive list of items for issuers to consider when describing management’s role in assessing and managing the issuer’s material risks from cybersecurity threats. This list includes, as its first item, identifying the management positions or committees “responsible for assessing and managing such risks,” and identifying “the relevant expertise of such persons or [committee] members in such detail as necessary to fully describe the nature of the expertise.” Issuers should therefore consider how to accurately and effectively describe the experience of members of management who are responsible for cybersecurity. The

Final Rule provides a list of examples of expertise, including “[p]rior work experience in cybersecurity; any relevant degrees or certifications; [and] any knowledge, skills or other background in cybersecurity.” To the extent necessary, firms also should consider how to support or supplement that expertise.

Compliance obligations for the majority of issuers begin after the later of 90 days from the date of publication (which is still forthcoming) or December 18, 2023. Smaller reporting issuers are given a longer period to come into compliance, with obligations effective after the later of 270 days from the effective date of the rules or June 15, 2024. For disclosures required in Forms 10-Q and 10-K and the comparable requirements in Form 20-F, issuers must begin providing disclosures with annual reports for fiscal years ending on or after December 15, 2023. Issuers must begin using Inline XBRL tagging one year after initial compliance with the related disclosure requirement.

The Final Rules are available [here](#).

To subscribe to the Data Blog of our Data Strategy and Security practice, please click [here](#).

\* \* \*

Please do not hesitate to contact us with any questions.

#### NEW YORK



Charu A. Chandrasekhar  
cchandrasekhar@debevoise.com



Avi Gesser  
agesser@debevoise.com



Matthew E. Kaplan  
mekaplan@debevoise.com



Erez Liebermann  
eliebermann@debevoise.com



Benjamin R. Pedersen  
brpedersen@debevoise.com



Paul M. Rodel  
pmrodel@debevoise.com



Steven J. Slutzky  
sjslutzky@debevoise.com



Matt Kelly  
makelly@debevoise.com



Kelly Donoghue  
kgdonoghue@debevoise.com



Chris Duff  
ceduff@debevoise.com



John Jacob  
jjacob@debevoise.com



Amy Pereira  
apereira@debevoise.com

**WASHINGTON, D.C.**



Ned Terrace  
jkterrac@debevoise.com



Luke Dembosky  
ldembosky@debevoise.com

**SAN FRANCISCO**



Mengyi Xu  
mxu@debevoise.com

# A Late Winter Blizzard of SEC Cybersecurity Rulemaking: the Proposed BD Cybersecurity Rules and Expanded Reg S-P and Reg SCI Obligations

March 20, 2023

On March 15, 2023, the U.S. Securities and Exchange Commission (the “SEC”) released a suite of proposed new rules (the “Proposed Rules”) that include:

- [Proposed new cybersecurity rules](#) for broker-dealers, security-based swap dealers, major security-based swap participants, transfer agents, a variety of market infrastructure providers (national securities exchanges, clearing agencies, and security-based swap data repositories), and securities SROs (collectively, “Market Entities”) that would impose new policies and procedures requirements and incident notification obligations (“BD Cyber Proposal”);
- [Amendments to Regulation S-P \(“Reg S-P”\)](#) that would require the implementation of an incident response program, including a new customer notification obligation; expand the scope of the existing requirements relating to the safeguarding of “customer” information and the disposal of “consumer” information relating to individuals (the “Safeguards and Disposal Rules”); and impose new recordkeeping requirements (“Reg S-P Proposal”); and
- [Amendments to Regulation SCI \(“Reg SCI”\)](#) to expand the scope of covered entities to cover certain broker-dealers without an ATS and security-based swap data repositories and to update requirements relating to policies and procedures, incident notification, and other compliance obligations (“Reg SCI Proposal”).

The Proposed Rules follow the SEC’s February 9, 2022 proposed cybersecurity rules for [registered investment advisers and registered funds](#) (“IM Cyber Proposal”) and March 9, 2022 cybersecurity rules for [issuers](#) (“Issuer Cyber Proposal”). The SEC also [reopened the public comment](#) period for the IM Cyber Rules in light of potentially overlapping obligations with these proposed new rules relating to policies and procedures, incident response, SEC notification, public disclosure, and recordkeeping.

Because the SEC’s proposed rules have overlapping requirements, it will be important for firms to assess how these competing requirements would interact and impact their

incident response and compliance programs, as well as their regulatory notification and disclosure obligations.

In this Data Blog post, we outline the key requirements of the Proposed Rules and offer key takeaways to help firms navigate and prepare for the likely adoption of a version of these complex regulations. We will also be discussing these issues during our [live webcast on March 21, 2023, as well as in subsequent blog posts](#).

---

## Key Requirements under the BD Cyber Proposal

The BD Cyber Proposal would create new cybersecurity obligations for sell-side financial institutions and various market infrastructure providers. For broker-dealers, the BD Cyber Proposal differentiates between (i) those for which a significant cyber event might pose higher risk to the market, which—along with all of the other types of covered institutions—would be defined as “Covered Entities” and (ii) more limited broker-dealers that would be subject to a smaller set of requirements. “Covered Entities” would include all (1) carrying broker-dealers; (2) introducing broker-dealers; (3) broker-dealers with regulatory capital equal to or exceeding \$50 million; (4) broker-dealers with assets equal to or exceeding \$1 billion; (5) broker-dealers that operate as market makers; and (6) entities that operate an alternative trading system (“ATS”). All other broker-dealers are excluded from this “Covered Entities” category (collectively, “Other Broker-Dealers”) and would be subject to fewer requirements.

The BD Cyber Proposal would create requirements for Covered Entities and Other Broker-Dealers related to incident response and notification, disclosure, and policies and procedures, including:

- **Immediate Incident Notification:** All Covered Entities and Other Broker-Dealers would be required to provide immediate written electronic notification to the SEC upon having a “reasonable basis to conclude that a significant cybersecurity incident has occurred or is occurring.” For this purpose, a “significant” incident would be one that significantly disrupts or degrades critical operations of the target or leads to unauthorized access that results, or is reasonably likely to result, in substantial harm to the target or any other person that interacts with the target.

Covered Entities would also be required to report additional information about the incident by filing Part I of proposed Form SCIR on EDGAR “promptly, but no later than 48 hours” after having a reasonable basis to conclude that a significant cybersecurity incident has occurred or is occurring. Covered Entities would also need to amend Part I of proposed Form SCIR no later than 48 hours after (1) determining

that previously reported information has become materially inaccurate; (2) learning new material information related to the previously reported incident; (3) resolution of the significant cybersecurity incident; or (4) conclusion of an internal investigation relating to the significant cybersecurity incident. Part I would not be public.

- **Public Disclosure of Risks and Incidents:** A Covered Entity would be required to make (and update in the case of material changes) two categories of cybersecurity disclosures on Part II of proposed Form SCIR (filed on EDGAR), as well as on an easily accessible section of its public website: (1) a summary description of cybersecurity risks that could materially affect the Covered Entity's business and operations (including how the Covered Entity "assesses, prioritizes, and addresses those cybersecurity risks"); and (2) "a summary description of each significant cybersecurity incident that occurred during the current or previous calendar year."
- **Cybersecurity Program:** Both Covered Entities and Other Broker-Dealers would be required to implement written policies and procedures that are reasonably designed to address their cybersecurity risks taking into account the size, business, and operations of the firm. These policies and procedures would need to be reviewed annually to "assess the design and effectiveness of the cybersecurity policies and procedures," including to address evolving cybersecurity risk. Covered Entities would need to document the annual review in a written report and would also be subject to more specific policies and procedures requirements, which would need to address "(1) risk assessments; (2) user security and access; (3) information protection; (4) cybersecurity threat and vulnerability management; and (5) cybersecurity incident response and recovery."
- **Books and Records:** New recordkeeping requirements would also be introduced for Covered Entities and Other Broker-Dealers that would cover, as applicable, the required policies and procedures, incident notification, Form SCIR disclosures, risk assessments, and annual reviews.

---

## Proposed Amendments to Regulation S-P

As we've discussed in our prior Data Blog posts ([here](#) and [here](#)), Reg S-P has been an active area for SEC enforcement activity. Key proposed amendments in the Reg S-P Proposal include:

- **Incident Response Program:** Would require broker-dealers, registered investment advisers, registered funds, and transfer agents (collectively, "Covered Institutions")

to implement an incident response program that is reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer information. The program would need to cover the risk of harm posed by security compromises at third-party service providers, as well as the Covered Institution itself.

- **Customer Notification:** Would generally require Covered Institutions to notify affected customers as soon as practicable, but no later than 30 days, of becoming aware that an incident involving unauthorized access to or use of “sensitive customer information” has occurred or is reasonably likely to have occurred. “Sensitive customer information” would be defined to mean any customer information alone or in conjunction with any other information, the compromise of which could create a reasonably likely risk of substantial harm or inconvenience to the individual identified. The Reg S-P Proposal contains an “affirmative presumption” of customer notice: notice would be required, unless the Covered Institution determines after a “reasonable investigation” of the incident that the sensitive customer information has not been or is reasonably unlikely to be used to cause substantial harm or inconvenience.
- **Expansion of Safeguards and Disposal Rules:** Would expand the Safeguards and Disposal Rules to cover all “customer information” in the possession of the Covered Institution regardless of whether it has a customer relationship with the relevant individual(s) and extends the applicability of the preexisting Safeguards and Disposal Rules to all transfer agents, including *both* those registered with the SEC and those registered with another regulatory agency.
- **Recordkeeping:** Would require the maintenance of written records documenting compliance with the Safeguards and Disposal Rules; amend recordkeeping provisions under the Investment Company Act of 1940, Investment Advisers Act of 1940, and the Securities Exchange Act of 1934; and add a recordkeeping requirement for investment companies not registered under the Investment Company Act.
- **Exception for Annual Privacy Notice:** Would conform Reg S-P’s existing annual privacy notice requirement to be consistent with the GLBA exception to the annual notice delivery requirements for financial institutions that meet certain requirements.

Reg S-P does not apply to private funds (either directly or as institutional clients of registered investment advisers) that rely on an exemption from registration under Sections 3(c)(1) or 3(c)(7) of the Investment Company Act of 1940, and the Reg S-P proposal does not suggest any change to this approach. The Reg S-P proposal provides a proposed compliance date 12 months after the effective date of the final amendments.

---

## Proposed Amendments to Regulation SCI

The Reg SCI Proposal includes amendments relating to (1) scope of covered entities subject to the regulation; (2) systems classification and lifecycle management; (3) third-party/vendor management; (4) cybersecurity; (5) the SCI review; (6) the role of current SCI industry standards; and (7) recordkeeping and related matters. Key proposals include:

- **Expansion of the Definition of “SCI Entities”:** The definition of SCI entity would be expanded to include certain large broker-dealers, registered security-based swap data repositories; and exempt clearing agencies. Broker-dealers would become subject to the full set of requirements if (i) their total assets in at least two of the previous four calendar quarters exceed 5% of the “total assets of all security broker-dealers” (as reported by the FRB); or (ii) their transaction volume over a slightly longer quarterly look-back period in any of four categories (NMS stocks, listed options, U.S. Treasuries, or U.S. Agency securities) exceeds 10% relative to the reported market.
- **Enhanced Policies and Procedures Requirements (with a focus on third-party providers):** An SCI entity’s policies and procedures would be required to include programs that address inventory, classification, and lifecycle management for SCI systems and indirect SCI systems; management and oversight of third-party providers (including cloud service providers) that provide or support SCI or indirect SCI systems; BC/DR plans that address the unavailability of certain third-party providers (and any resulting material impact); unauthorized access to SCI systems and information therein; and identification of current SCI industry standards with which each such policy and procedure is consistent.
- **More Frequent Penetration Testing:** Would increase the scope and the required frequency of penetration testing by SCI entities to at least annually, rather than once every three years.
- **Expanded Definition of “Systems Intrusion”:** Would amend the definition of “systems intrusion” to include two more cyber events: (1) any cybersecurity event that disrupts, or significantly degrades, the normal operation of an SCI system (e.g., DDOS attacks, remote command-and-control attacks, supply-chain attacks); and (2) any significant attempted unauthorized entry into the SCI systems or indirect systems of an SCI entity as determined by the SCI entity pursuant to established reasonable written criteria. Such events would also require SEC notification under Reg SCI’s existing notification framework.

---

## Key Takeaways

- **The SEC’s Comment Process.** Given the number of overlapping and significant proposed regulatory obligations, consider submitting comments to the Proposed Rules.
- **Cross-Functional Risk Assessment Mapped to the Rules.** Consider a risk assessment that assesses both policies and procedures, as well as technical cybersecurity controls, and that maps onto the proposed rules (as well as other applicable regulatory frameworks). Cross-enterprise teams or committees that include members of the business, internal audit, and compliance can ensure that compliance obligations are not missed by working with security teams on these assessments. While the applicability of privilege for such assessments is subject to debate, some of our clients have found it helpful to use outside counsel together with a technical vendor to assist with these.
- **Review Applicability of Each Rule under Expanded Scope and Definitions.** As the SEC itself recognizes, the Proposed Rules have overlapping requirements because a single entity will potentially be bound by multiple sets of rules. For instance, certain SCI entities are also “Covered Entities” under the BD Cyber Proposal and would separately also be subject to requirements under Reg S-P. Likewise, registered investment advisers (which are already subject to Reg S-P) would also be subject to the IM Cyber Proposal. A first step for registrants to consider is identifying and assessing the full range of potentially new or heightened obligations. For some firms that are covered by the Proposed Rules, it may take significant time and resources to fully implement these requirements, and accordingly, they may want to start early.
- **An Integrated Approach.** The SEC also recognizes that registrants can likely comply with the proposed new obligations through a global framework for policies and procedures and incident response. Consider taking a holistic view of covered areas such as incident response, policies and procedures, notification, and recordkeeping.

**Compliance with Notification and Reporting Obligations.** The different proposed regulatory frameworks have different notification timelines, obligations, and formats for notification. Consider preparing a decision matrix for assessing cybersecurity events under each notification trigger, including the factors to consider when determining whether a particular cybersecurity event would qualify as “significant” for reporting purposes.

Please do not hesitate to contact us with any questions.

To subscribe to the Data Blog, please click [here](#).

The [Debevoise Data Portal](#) is now available for clients to help them quickly assess and comply with their various state, federal, and international breach notification obligations.

**NEW YORK**



Avi Gesser  
agesser@debevoise.com



Erez Liebermann  
eliebermann@debevoise.com



Jeff Robins  
jlrobin@debevoise.com



Charu A. Chandrasekhar  
cchandrasekhar@debevoise.com



Sheena Paul  
spaul@debevoise.com



Suchita Mandavilli Brundage  
smbrunda@debevoise.com

**WASHINGTON, D.C.**



Michael R. Roberts  
mrroberts@debevoise.com



Ned Terrace  
jkterrace@debevoise.com



Luke Dembosky  
ldembosky@debevoise.com

**SAN FRANCISCO**



Marc Ponchione  
mponchione@debevoise.com



Julie M. Riewe  
jriewe@debevoise.com



Kristin A. Snyder  
kasnyder@debevoise.com

**SAN FRANCISCO**



Mengyi Xu  
email@debevoise.com

# SEC Cybersecurity Rules: FBI, DOJ and SEC Publish Guidance on Disclosure Delays

December 18, 2023

The SEC's [new cybersecurity rules](#) for public companies became effective on December 18, 2023. The rules require disclosure of a cybersecurity event within four business days of a [determination that it is material](#). They also provide that such disclosure may be delayed for up to 30 days if the United States Attorney General (or per DOJ guidelines, the Attorney General's authorized designees) determines that immediate disclosure would pose "a substantial risk to national security or public safety, and notifies the SEC of such determination in writing." Two subsequent delay periods of 30 days and 60 days (in extraordinary circumstances) may also be sought.

The FBI and the DOJ recently issued guidelines for companies seeking such delays. In this post, we discuss the logistics of making a delay request and offer [several tips](#) for companies to prepare for potentially material cybersecurity incidents that may involve making such a request.

**FBI's Guidance and Policy Notice.** On December 6, the FBI, in coordination with the DOJ, published [guidance](#) and a [Policy Notice](#) on how victimized companies can request disclosure delays for national security or public safety reasons. First, the FBI recommends that public companies establish a relationship with the cyber squad at their local FBI field office before any potentially material cyber incident occurs. Second, during an incident, the FBI "strongly encourages" victims to engage with the FBI directly (or through U.S. Secret Service (the "USSS"), the Cybersecurity and Infrastructure Security Agency (the "CISA") or another sector risk management agency ("SRMA")) *prior* to making a materiality determination. Third, the FBI warns that if it does not receive a delay request "concurrently" with the materiality determination, it will not process the request.

As outlined in the Policy Notice, the FBI is responsible for: (1) intaking delay requests on behalf of the DOJ, (2) documenting those requests; (3) coordinating checks of U.S. government national security and public safety equities, including consulting with the USSS, CISA and SRMAs as appropriate; (4) referring the request forms to the DOJ; (5) conducting follow-up victim engagement, as appropriate; and (6) coordinating and

---

documenting requests for additional delay referrals. The FBI will also soon provide a dedicated email address for initial reporting delay requests and delay extension requests.

The FBI's guidance lists 10 items that must be included in each delay request:

- The name of the company;
- The date when the cyber incident occurred;
- Details (date, time and time zone) regarding when the victim company determined that the cyber incident was material such that it would require disclosure on Form 8-K or Form 6-K under the SEC's final cyber disclosure rules. *The FBI explains that failure to report this information immediately upon determination will cause a delay-referral request to be denied.*
- Whether the victim company is already in contact with the FBI or another U.S. government agency regarding this incident (and, if so, the names and field offices of the FBI points of contact or information regarding the applicable U.S. government agency);
- A description of the cyber incident in detail that includes, at a minimum:
  - What type of incident occurred;
  - What are the known or suspected intrusion vectors, including any identified vulnerabilities if known;
  - What infrastructure or data were affected (if any) and how they were affected;
  - What the operational impact on the company is, if known;
- Whether there is any confirmed or suspected attribution of the cyber actors responsible;
- The current status of any remediation or mitigation efforts;
- The location where the cyber incident occurred (including street address, city and state);
- The company's points of contact for the matter (including name, phone number and email address of personnel the company wants the FBI to contact to discuss the request); and

- 
- Whether the company has previously submitted a delay referral request or if this is the first time. If the company has previously submitted a delay request, the victim company should include details about when the DOJ made its last determination(s), on what grounds and for how long the DOJ granted a delay (if applicable).

**DOJ's Guidelines.** On December 12, the DOJ [issued](#) its [departmental guidelines](#) for material cybersecurity incident delay determinations. The guidelines explain that the “primary inquiry” for the DOJ is “whether the *public disclosure* of a cybersecurity incident threatens public safety and national security, not whether the incident itself poses a substantial risk to public safety and national security.” The guidelines outline four categories of “limited circumstances” in which the DOJ believes the disclosure of some or all of the information required by new Item 1.05 of Form 8-K (“Item 1.05”) could pose a substantial risk to national security or public safety:

- A cybersecurity incident involves a technique for which there is not yet a well-known mitigation (*e.g.*, zero-day vulnerability), and the disclosure required by Item 1.05 could lead to more incidents.
- The cybersecurity incident primarily impacts a system operated or maintained by a registrant that contains sensitive U.S. government information (*e.g.*, information regarding national defense or research and development performed pursuant to government contracts), and public disclosure required by Item 1.05 would increase vulnerability to further exploitation by illicit cyber activity.
- The registrant is conducting remediation efforts, and any disclosure required by Item 1.05(a) revealing that the registrant is aware of the incident would undermine those remediation efforts.
- Circumstances in which the U.S. government, rather than a registrant, is likely to be aware of a substantial risk to national security or public safety and in which the government has made the registrant aware of the circumstances.

For the fourth category, the DOJ anticipates that relevant scenarios may be those: (i) where disclosure would risk revealing a confidential source, information relating to U.S. national security or law enforcement sensitive information; (ii) where the U.S. government is prepared to execute, or is aware of, an operation to disrupt ongoing illicit cyber activity; and (iii) where the U.S. government is aware of or conducting remediation efforts for any critical infrastructure or critical system. In these instances, the government might try to obtain the registrant's agreement to delay a disclosure.

---

**Steps to Consider.** Given the publication of these resources, as well as the FBI's and the DOJ's comments at the recent [2023 Aspen Institute Cyber Summit](#), companies should consider the steps outlined below.

- **Consider updating incident response plans to incorporate relevant factual predicates from, and ensure timely compliance with, the guidelines.** It is important to confirm that cyber incident response plans and procedures ensure timely assessment of whether the disclosure of an incident may present substantial risks to national security or public safety, and therefore be considered for a notification delay from the DOJ. Such plans and procedures should favor early reporting to law enforcement in any situation where these issues have the potential to be relevant in the incident. The guidelines include several examples of cybersecurity incidents (*e.g.*, zero-day vulnerability exploits) and key factual questions that companies should include in their plans in order to inform their analysis.
- **Consider enhancing relationships with applicable FBI local field offices, including points of contact on the FBI cyber squads.** The FBI will play a central role in the DOJ's determinations regarding disclosure delay requests. Having established direct or indirect (*e.g.*, through cyber counsel) relationships with FBI contacts and promptly initiating contact with the FBI about an incident will be critical, as a failure to report a cyber incident immediately upon determination of materiality will cause a delay-referral request to be denied. Additionally, the FBI's guidance emphasizes reporting to the FBI early is important in order to manage the lead time necessary to make a disclosure delay determination.
- **Consider reviewing and updating disclosure analysis and escalation procedures to incorporate the FBI and the DOJ guidelines, as well as interpretations recently issued by the SEC.** The SEC made clear in recently issued [compliance and disclosure interpretations](#) that requesting a delay alone does not toll the registrant's filing obligation. Importantly, the SEC confirmed that if the Attorney General declines to make a determination whether disclosure of the incident poses a substantial risk to national security or public safety or does not respond before the Form 8-K otherwise would be due, the registrant must file the Item 1.05 Form 8-K within four business days of its determination that the incident is material (or within four business days of end of the initial delay period, if the request relates to a delay extension). Registrants should therefore ensure that their disclosure analysis and escalation procedures align with best practices from the guidelines and ensure timely outreach to the FBI and the DOJ. The director of the SEC's Division of Corporation Finance also reiterated, in a [recent speech](#), that a decision to contact the FBI or the DOJ about a cybersecurity incident does not trigger a materiality determination. However, this will only be relevant prior to submitting a request for delay, as the

---

request form requires an indication of when the incident was determined to be material.

\* \* \*

Please do not hesitate to contact us with any questions.



**Charu Chandrasekhar**  
Partner, New York  
+1 212 909 6774  
cchandrasekhar@debevoise.com



**Luke Dembosky**  
Partner, Washington, D.C.  
+1 202 383 8020  
ldembosky@debevoise.com



**Avi Gesser**  
Partner, New York  
+1 212 909 6577  
agesser@debevoise.com



**Erez Liebermann**  
Partner, New York  
+1 212 909 6224  
eliebermann@debevoise.com



**Benjamin R. Pedersen**  
Partner, New York  
+1 212 909 6121  
brpedersen@debevoise.com



**Matt Kelly**  
Counsel, New York  
+1 212 909 6990  
makelly@debevoise.com



**Alice Gu**  
Associate, New York  
+1 212 909 6057  
agu@debevoise.com



**Paul D. Lowry**  
Associate, New York  
+1 212 909 6198  
pdlowry@debevoise.com



**Michael R. Roberts**  
Associate, New York  
+1 212 909 6406  
mrroberts@debevoise.com

## **IAA Investment Adviser Compliance Conference**

Private Equity Fund Advisers: Hot Topics in SEC Examinations Panel

Outline

March 8, 2024

Jason Brown, Partner, Ropes & Gray LLP

Letti de Little, Chief Compliance Officer, Grain Management

Sean Murphy, Senior Vice President, Chief Compliance Officer, EIG Partners

### **I. Preparing for an Exam**

#### **A. Criteria for choosing which advisers are examined**

1. As of 2023, there were over 15,000 registered investment advisers, and the SEC was able to examine about 15% of registered investment advisers annually.
2. To determine which advisers are examined, the SEC has stated it applies a risk-based approach, which is based on both adviser disclosures and information obtained from third parties.
3. Examples of risks considered include:
  - a) Firms with supervisory concerns (i.e., disciplinary history relating to the adviser's personnel);
  - b) Firms with complex business models where the adviser is co-investing with clients;
  - c) Firms which have not been examined in a long period of time;
  - d) Newly registered firms;
  - e) Firms with material changes in leadership or ownership;
  - f) Firms with access to client assets;
  - g) Firms with recently identified issues relating to compliance programs disclosure documents, or marketing materials.

#### **B. Composition of SEC personnel on exam**

1. Local office vs. not
2. Private Funds Unit vs. regional
3. Lawyer vs. not
4. Enforcement vs. EXAMS only

#### **C. Exam process**

1. EXAMS usually calls adviser informing it of upcoming exam.
2. EXAMS then generally sends a formal letter, including an initial request list.
  - a) Number of requests varies widely, but usually includes 30-35 requests (but can exceed 80 requests). Examples of materials/subject matter include:
    - (1) Trade blotters;
    - (2) Compliance manuals and records of infractions;
    - (3) Fund documents;
    - (4) Schedule of fees and expenses;

- (5) Marketing and advertising materials;
    - (6) Investor complaints;
    - (7) Any threatened or pending litigation.
  - b) Initial production of requests is usually due within two weeks.
- 3. Once an initial request is responded to, the process for an exam and the timing for an exam often vary, but they usually include further requests and/or interviews.
  - a) Examiners generally interviews key employees/departments, such as finance, portfolio managers, and compliance.
  - b) Typically, there are multiple rounds of written follow-up requests.
  - c) Exams typically last around 6-9 months, but many are shorter or longer.
- 4. Exam may result in no findings, deficiencies, or a referral to enforcement.
  - a) No findings (infrequent)
  - b) Deficiency letter (most common)
    - (1) Identifies a variety of deficiencies depending on the nature of the firm's business.
    - (2) 30 days to respond in writing.
  - c) Referral to SEC Enforcement Division (infrequent)

#### **D. Preparing for an exam**

1. It is most critical to ensure the adviser has a well-run compliance program on an ongoing basis.
  - a) This includes having the adequate documentation of each aspect of the program.
  - b) Mock examinations, whether done by an outside party or internally, can be a useful tool in preparing for an SEC exam.
2. Consider who on the team, whether internal or external, is going to be responsible for certain portions of the exam process, ideally with backups.
  - a) For example, who will be the person tasked with coordinating internally and tracking the gathering of documents to respond to each item? Who might be tasked with coordinating with outside counsel to gather fund documents?
3. Consider what might be expected from an initial request list and begin gathering those materials to the extent possible.
  - a) In particular, prepare certain materials that the SEC has the expectation that the adviser is maintaining and updating in the regular course, such as a violations log, a risk matrix, or a trade blotter.
  - b) Obtain a list of the types of requests you might expect and start getting ready to fill those in from regulatory counsel or compliance consultants.
4. Similarly, prepare a "Day One" deck in advance with the expectation that it may need to be updated based on the actual requests, as we will discuss in more depth shortly.

**E. “Day One” / “First Day” Deck**

1. Outlines, among other things, the manager’s organizational structure, investment process, expense allocation procedures and compliance function.
2. Items to consider include:
  - a) Firm overview including ownership and history;
  - b) Firm affiliates (include org chart if complex);
  - c) Key personnel (functional org chart);
  - d) Types of clients/products;
  - e) Types of services including investment strategies offered;
  - f) Overview of marketing, compliance, valuation, fees/expenses.
3. While having an off-the-shelf version of a Day One deck prepared in anticipation of any future examination is recommended, what is actually presented to EXAMS should be tailored to address their specific issues or concerns.

**F. Criteria for choosing interviewees**

1. EXAMS will generally provide guidance on the interviewees it would like to interview, or at least the relevant departments or subject matter.
  - a) If given the option to select individuals, consider their substantive knowledge of the relevant issue, as well as their demeanor and credibility.

**II. Current issues in private funds exams**

**A. Post-commitment period management fees**

1. The SEC has paid increased attention to the calculation of fees after the end of a fund’s commitment period, particularly where the sponsor has a conflict of interest.
  - a) Post-commitment management fee calculations are a top three issue on virtually every closed-end fund adviser exam and should remain a high priority for compliance efforts.
  - b) The SEC is focused on what exactly adviser fund document say about how management fees are calculated, how write-downs and portfolio company reorganizations are accounted for, and whether adviser practices match what the documents state.

**B. Affiliated service providers**

1. EXAMS has shown a focus on conflicts, controls, and disclosures regarding investment advisers managing private funds and their use of affiliated service providers.
2. Examiners will usually review adherence to an adviser’s fiduciary duty standard, focusing on economic incentives that an adviser may have to recommend affiliated service providers.
3. Tasks performed by affiliated service providers may include asset-level due diligence, loan servicing, property management, accounting, in-house legal, fund administration, and other similar services typically performed by outside professionals.

4. Examiners will compare practices to disclosure, including the parties involved, descriptions of their services, how they are paid, and whether the adviser engages in any benchmarking.

**C. Following disclosure (e.g., due diligence disclosures/ESG)**

1. Examiners often review adherence to an adviser's fiduciary duty standard, focusing on disclosures and statements (e.g., through marketing or even more informally) made to investors and whether they include all material facts and are consistent with policies, procedures, and practices.

2. With respect to ESG in particular, the main concern is greenwashing – i.e., communicating to investors that advisers are taking ESG actions that they are not actually implementing.

3. Whether as related to due diligence disclosures more generally or on ESG specifically, it is important to ensure that disclosures and statements are accurate and align with policies, procedures, and practices.

4. In addition, on ESG, advisers should ensure cross-firm coordination, including among IR, legal/compliance, ESG, and investment personnel.

**D. Marketing**

1. EXAMS is likely to focus on whether advisers have:

a) adopted policies and procedures addressing the new marketing rules;

b) appropriately disclosed their marketing-related information on Form ADV;

c) maintained substantiation of factual claims and other required books and records.

2. Reviews will generally also assess whether advertisements are misleading and comply with requirements for performance (including hypothetical and predecessor performance), third-party ratings, and testimonials and endorsements.

**E. Adherence to contractual requirements related to LPACs**

1. Examiners generally focus on adherence to contractual requirements regarding limited partnership advisory committees or similar structures (e.g., advisory boards), including adhering to any contractual notification and consent processes.

2. They are likely to ask whether the LPAC is authorized under the LPA to make the required approval and whether it received disclosure of all material facts and conflicts.

**F. Fees & expenses**

1. Examiners have generally focused on allocation of certain fees and expenses among the investment adviser, the funds/clients, and/or co-investors, and clear, accurate, and timely disclosure of allocation practices.

2. Recent general fee and expense and allocation focuses include:

a) Calculation of management fees;

- b) Expenses not authorized by the LPA or governing documents (for instance, with respect to fund extensions, or compliance, examination and enforcement inquiry costs);
- c) Recycling provisions;
- d) Expenses not borne by certain funds despite shared benefit, e.g., “broken deal” costs;
- e) Allocation of financing costs;
- f) Expenses allocated to co-investors;
- g) Expenses of the adviser being allocated to a fund / investment that could be considered “overhead” (for instance, use of platform companies to employ certain firm individuals);
- h) Services of adviser personnel being charged to a client / investment (“in-sourcing”);
- i) Expenses benefitting adviser (such as insurance premiums).

**G. Loans & guarantees**

1. Loans and guarantees can lead to a number of inherent conflicts that EXAMS may review, including those between the adviser and funds or portfolio companies.
2. For example, EXAMS will expect advisers to have considered and/or disclosed, as appropriate, whether the loans or guarantees are in the best interests of the clients involved, whether terms are “market”, and capital structure conflicts.

**H. Crypto-assets and emerging financial technology**

1. For crypto, examiners typically assess appropriate standards of conduct, particularly the duty of care; the routine review, update, and enhancement of compliance practices (including crypto wallet reviews, custody practices, Bank Secrecy Act compliance reviews and valuation procedures); operational resiliency practices (i.e., data integrity and business continuity plans); compliance with the custody rule; and appropriate risk-disclosure.
2. According to EXAMS’s 2024 Priorities Report, it remains focused on automated investment tools, artificial intelligence and trading algorithms or platforms, and the risks associated with the use of emerging technologies and alternative sources of data.

## Exams of Private Fund Advisers:

2024 Exam Priorities: <https://www.sec.gov/files/2024-exam-priorities.pdf>

The SEC's Division of Examinations (EXAMS) will continue to focus on the following topics:

- The portfolio management risks present when there is exposure to recent market volatility and higher interest rates. This may include private funds experiencing poor performance, significant withdrawals and valuation issues and private funds with more leverage and illiquid assets.
- Adherence to contractual requirements regarding limited partnership advisory committees or similar structures (e.g., advisory boards), including adhering to any contractual notification and consent processes.
- Accurate calculation and allocation of private fund fees and expenses (both fund-level and investment-level), including valuation of illiquid assets, calculation of post commitment period management fees, adequacy of disclosures, and potential offsetting of such fees and expenses.
- Due diligence practices for consistency with policies, procedures, and disclosures, particularly with respect to private equity and venture capital fund assessments of prospective portfolio companies.
- Conflicts, controls, and disclosures regarding private funds managed side-by-side with registered investment companies and use of affiliated service providers.
- Compliance with Advisers Act requirements regarding custody, including accurate Form ADV reporting, timely completion of private fund audits by a qualified auditor and the distribution of private fund audited financial statements.
- Policies and procedures for reporting on Form PF, including upon the occurrence of certain reporting events.

## Topics Included in Selected 2023 Exam Letters on Private Funds:

- **Fund Information:**
  - Name as shown in organizational documents (as amended)
  - Domicile (country)
  - Date the Fund began accepting investors
  - Whether the Fund is currently closed to new investors and when it closed
  - Number of investors
  - Total net assets
  - Short description of investment strategy
  - Amount, if any, of Registrant's equity interest in the Fund
  - Amount, if any, of Registrant's affiliated persons' interest in the Fund
  - Each custodian used by the Fund
  - Primary Fund counsel
  - Auditor of the Fund
  - Whether the Fund is currently above its high-water mark
  - Lock-up periods for both initial and subsequent investments

- If the Fund is part of a master/feeder fund structure, whether it is a master or feeder fund, and if it is a feeder fund, the full name of its master fund
  - The management fee charged for the most recent billing period
  - The date the most recent management fee was charged
  - The performance fee (if applicable) charged for the most recent billing period
  - The date the most recent performance fee was charged.
- **Fund Documents, Performance, and Investors.** For each Fund that is offered to U.S. investors, provide the following information or documents:
  - A copy of the Fund's organizational documents, including the management agreement, limited partnership agreement or operating agreement, whichever is applicable, and its private placement memorandum
  - A copy of the Fund's most recent audited financial statements;
  - The monthly and annual performance returns for the past four years, or since inception, whichever is shorter
  - A list of investors, including:
    - Name of investor
    - Account balances
    - Whether the investor is a related person or a proprietary account;
    - Country of Domicile
    - The name of the third party consultant used (if any)
    - Whether Registrant directly manages the account or acts as a sub-adviser
    - Date of initial investment
    - Whether the investor pays a performance fee
- **Investment Positions**
- **Investments not held by a Qualified Custodian.**



# RISK ALERT

DIVISION OF EXAMINATIONS

January 27, 2022

## Observations from Examinations of Private Fund Advisers

### I. Introduction

On June 23, 2020, the Division of Examinations (“EXAMS”) published a Risk Alert (the “2020 Private Fund Adviser Risk Alert”) providing an overview of compliance issues observed by EXAMS staff\* in examinations of registered investment advisers that manage private funds (“private fund advisers”).<sup>1</sup> In light of the significant role of private fund advisers in the financial markets, we are publishing this risk alert detailing additional observations: (A) failure to act consistently with disclosures; (B) use of misleading disclosures regarding performance and marketing; (C) due diligence failures relating to investments or service providers; and (D) use of potentially misleading “hedge clauses.”<sup>2</sup>

More than 5,000 SEC-registered investment advisers, approximately 35% of all SEC-registered advisers, manage approximately \$18 trillion in private fund assets.<sup>3</sup> In the past five years alone, we have observed substantial growth in reported private fund assets, which have increased by 70% in that period. These assets are deployed through a variety of investment strategies employed by hedge funds, private equity funds, and real estate-related funds, among others. The size and complexity of advisers vary widely from, for example, an adviser with a private fund limited to investors made up of friends and family, to an adviser with a worldwide footprint managing multiple private funds with hundreds of billions of dollars in assets. This Risk Alert is intended to assist private fund advisers in reviewing and enhancing their compliance programs, and also to provide investors with information concerning private fund adviser deficiencies.

### II. Legal Background

An investment adviser’s fiduciary duty under the Investment Advisers Act of 1940 (“Advisers

---

\* This Risk Alert represents the views of the staff of EXAMS. This Risk Alert is not a rule, regulation, or statement of the Securities and Exchange Commission (the “SEC” or the “Commission”). The Commission has neither approved nor disapproved the content of this Risk Alert. This Risk Alert, like all staff statements, has no legal force or effect: it does not alter or amend applicable law, and it creates no new or additional obligations for any person. This document was prepared by EXAMS staff and is not legal advice.

<sup>1</sup> EXAMS Risk Alert, [Observations from Examinations of Investment Advisers Managing Private Funds](#) (June 23, 2020) (the “2020 Private Fund Adviser Risk Alert”).

<sup>2</sup> The observations in this Risk Alert and the 2020 Private Fund Adviser Risk Alert were drawn from over 5 years of examinations of private fund advisers. This Risk Alert, the 2020 Private Fund Adviser Risk Alert, and [The Five Most Frequent Compliance Topics](#) (Feb. 17, 2017) (for all advisers) reflect observations of the EXAMS staff regarding private fund advisers and are intended to assist private fund adviser compliance staff.

<sup>3</sup> Form ADV data current as of November 30, 2021.

Act”) comprises a duty of care and a duty of loyalty.<sup>4</sup> This means the adviser must, at all times, serve the best interest of its client and not subordinate its client’s interest to its own. In other words, the investment adviser cannot place its own interests ahead of the interests of its client. This combination of care and loyalty obligations requires the investment adviser to act in the “best interest” of its client at all times. Although investment advisers owe their clients a fiduciary duty under the Advisers Act, that fiduciary duty must be viewed in the context of the agreed-upon scope of the relationship between the adviser and the client.<sup>5</sup>

In addition, Advisers Act Rule 206(4)-8 prohibits investment advisers to pooled investment vehicles from: (1) making any untrue statement of a material fact or omitting to state a material fact necessary to make the statements made, in the light of the circumstances under which they were made, not misleading, to any investor or prospective investor in the pooled investment vehicle; or (2) otherwise engaging in any act, practice, or course of business that is fraudulent, deceptive, or manipulative with respect to any investor or prospective investor in the pooled investment vehicle.

Advisers Act Rule 206(4)-7 (the “Compliance Rule”) requires registered investment advisers to adopt and implement written policies and procedures reasonably designed to prevent violations of the Advisers Act and the rules that the Commission has adopted under the Advisers Act by the adviser or any of its supervised persons. In developing its policies and procedures, an adviser should identify matters that create risk exposure for the adviser and its clients in light of the firm's particular operations and then design compliance policies and procedures that address those risks. The Compliance Rule also requires advisers to review, no less frequently than annually, the adequacy of the policies and procedures established and the effectiveness of their implementation.

### **III. Private Fund Adviser Deficiencies<sup>6</sup>**

#### **A. Conduct Inconsistent with Disclosures**

EXAMS staff has observed the following failures to act consistently with material disclosures to clients or investors:

- *Failure to obtain informed consent from Limited Partner Advisory Committees, Advisory Boards or Advisory Committees (collectively “LPACs”) required under fund disclosures.* EXAMS staff observed private fund advisers that did not follow practices described in their limited partnership agreements (“LPAs”), operating agreements, private placement memoranda, due-diligence questionnaires, side letters or other disclosures (“fund disclosures”) regarding the use of LPACs. For example, staff observed private fund advisers that failed to bring conflicts to their LPACs for review and consent, in

---

<sup>4</sup> See Commission Interpretation Regarding Standard of Conduct for Investment Advisers, Advisers Act Release No. 5248 (June 5, 2019) (“Fiduciary Interpretation”).

<sup>5</sup> See Fiduciary Interpretation.

<sup>6</sup> This Risk Alert does not address all deficiencies among private fund advisers. In addition to the 2020 Private Fund Adviser Risk Alert, EXAMS also published, for example, a risk alert on February 7, 2017, [The Five Most Frequent Compliance Topics Identified in OCIE Examinations of Investment Advisers](#), which identifies deficiencies across all types of investment advisers.

contravention of fund disclosures. EXAMS staff also observed private fund advisers that did not obtain consent for certain conflicted transactions from the LPAC until after the transaction had occurred or obtained approval after providing the LPAC with incomplete information in contravention of fund disclosures.

- *Failure to follow practices described in fund disclosures regarding the calculation of Post-Commitment Period fund-level management fees.* EXAMS staff observed private fund advisers that did not follow practices described in fund disclosures regarding the calculation of the fund-level management fee during a private fund's Post-Commitment Period.<sup>7</sup> EXAMS staff observed that such failures resulted in investors paying more in management fees than they were required to pay under the terms of the fund disclosures. For example, private fund advisers did not reduce the cost basis of an investment when calculating their management fee after selling, writing off, writing down or otherwise disposing of a portion of an investment. Other private fund advisers used broad, undefined terms in the LPA, such as "impaired," "permanently impaired," "written down," or "permanently written down," but did not implement policies and procedures reasonably designed to apply these terms consistently when calculating management fees, potentially resulting in inaccurate management fees being charged.
- *Failure to comply with LPA liquidation and fund extension terms.* EXAMS staff observed advisers that extended the terms of private equity funds without obtaining the required approvals or without complying with the liquidation provisions described in the funds' LPAs, which, among other things, resulted in potentially inappropriate management fees being charged to investors.
- *Failure to invest in accordance with fund disclosures regarding investment strategy.* EXAMS staff observed private fund advisers that did not comply with investment limitations in fund disclosures. For example, the staff observed private fund advisers that implemented an investment strategy that diverged materially from fund disclosures. EXAMS staff also observed advisers that caused funds to exceed leverage limitations detailed in fund disclosures.
- *Failures relating to recycling practices.* "Recycling" refers to contractual provisions that allow a fund to add realized investment proceeds back to the capital commitments of investors. EXAMS staff observed private fund advisers that did not accurately describe the "recycling" practices utilized by their funds or omitted material information from such disclosures. In some instances, this failure may have caused private fund advisers to collect excess management fees.
- *Failure to follow fund disclosures regarding adviser personnel.* EXAMS staff observed advisers that did not adhere to the LPA "key person" process after the departure of

---

<sup>7</sup> Advisers to private equity funds typically assess a management fee based on a percentage of limited partner capital commitments during the period of time the fund deploys capital ("Commitment Period"). The basis of the amount used to calculate this fee, however, is generally reduced to "invested capital," less dispositions, write downs and write offs after the Commitment Period ("Post-Commitment Period"). These arrangements vary in accordance with contractual provisions.

several adviser principals or did not provide accurate information to investors reflecting the status of key previously-employed portfolio managers.

## B. Disclosures Regarding Performance and Marketing

EXAMS staff has observed private fund advisers providing to investors or prospective investors misleading track records or other marketing statements that appear to violate Rule 206(4)-8.<sup>8</sup> In addition, Advisers Act Rule 204-2(a)(16) requires advisers to maintain all accounts, books, internal working papers, and any other records or documents that are necessary to form the basis for or demonstrate the calculation of any performance or rate of return of any or all managed accounts or securities recommendations. EXAMS staff has also observed failures by private fund advisers to maintain these required records.

- *Misleading material information about a track record.* EXAMS staff observed private fund advisers that provided inaccurate or misleading disclosures about their track record, including how benchmarks were used or how the portfolio for the track record was constructed. For example, the staff observed advisers that only marketed a favorable or cherry-picked track record of one fund or a subset of funds or did not disclose material information about the material impact of leverage on fund performance. In addition, the staff observed private fund advisers that utilized stale performance information in presentations to potential investors or track records that did not accurately reflect fees and expenses.
- *Inaccurate performance calculations.* EXAMS staff observed private fund advisers that presented inaccurate performance calculations to investors. For example, the staff observed private fund advisers that used inaccurate underlying data (*e.g.*, data from incorrect time periods, mischaracterization of return of capital distributions as dividends from portfolio companies, and/or projected rather than actual performance used in performance calculations) when creating track records, thereby leading to inaccurate and potentially misleading disclosures regarding performance.
- *Portability - failure to support adequately, or omissions of material information about, predecessor performance.* EXAMS staff observed private fund advisers that did not maintain books and records supporting predecessor performance at other advisers as required under Advisers Act Rule 204-2(a)(16). In addition, the staff observed private fund advisers that appeared to have omitted material facts about predecessor performance. For example, the staff observed private fund advisers that marketed incomplete prior track records or advertised performance that persons at the adviser were not primarily responsible for achieving at the prior adviser.
- *Misleading statements regarding awards or other claims.* EXAMS staff observed private fund advisers that made misleading statements regarding awards they received or characteristics of their firm. For example, the staff observed private fund advisers that

---

<sup>8</sup> The Commission adopted significant revisions to Advisers Act Rule 206(4)-1 that address the marketing of private funds. The rule, which advisers must comply with by November 4, 2022, provides additional specificity regarding misleading marketing materials. In addition to Rule 206(4)-1 and Rule 206(4)-8, the anti-fraud provisions of the federal securities laws, *e.g.*, Section 206 of the Advisers Act, Section 17(a) of the Securities Act of 1933, and Section 10(b) of the Securities Exchange Act of 1934, may apply to this activity.

marketed awards received, but failed to make full and fair disclosures about the awards, such as the criteria for obtaining them, the amount of any fee paid by the adviser to receive them, and any amounts paid to the grantor of the awards for the adviser's right to promote its receipt of the awards. The staff also observed advisers that incorrectly claimed their investments were "supported" or "overseen" by the SEC or the United States government.

### C. Due Diligence

As a fiduciary, an investment adviser must have a reasonable belief that the advice it provides is in the best interest of the client based on the client's objectives. A reasonable belief that investment advice is in the best interest of a client also requires that an adviser conduct a reasonable investigation into the investment that is sufficient to ensure that the adviser is not basing its advice on materially inaccurate or incomplete information.<sup>9</sup>

EXAMS staff observed potential failures to conduct a reasonable investigation into an investment, to follow the due diligence process described to clients or investors, and to adopt and implement reasonably designed due diligence policies and procedures pursuant to the Compliance Rule:

- *Lack of a reasonable investigation into underlying investments or funds.* EXAMS staff observed advisers that did not perform reasonable investigations of investments in accordance with their policies and procedures, including the compliance and internal controls of the underlying investments or private funds in which they invested. In addition, the staff observed advisers that failed to perform adequate due diligence on important service providers, such as alternative data providers and placement agents.
- *Inadequate policies and procedures regarding investment due diligence.* EXAMS staff observed private fund advisers that did not appear to maintain reasonably designed policies and procedures regarding due diligence of investments. For example, the staff observed private fund advisers that outlined a due diligence process in fund disclosures, but did not maintain policies and procedures related to due diligence that were tailored to their advisory businesses.

### D. Hedge Clauses

Whether a clause in an agreement, or a statement in disclosure documents provided to clients and investors, that purports to limit an adviser's liability (a "hedge clause") is misleading and would violate Sections 206(1) and 206(2) of the Advisers Act depends on all of the surrounding facts and circumstances.<sup>10</sup> EXAMS staff observed private fund advisers that included potentially misleading hedge clauses in documents that purported to waive or limit the Advisers Act fiduciary duty except for certain exceptions, such as a non-appealable judicial finding of gross negligence, willful misconduct, or fraud. Such clauses could be inconsistent with Sections 206 and 215(a) of the Advisers Act.

---

<sup>9</sup> See Fiduciary Interpretation.

<sup>10</sup> See Fiduciary Interpretation.

#### IV. Conclusion

Examinations of private fund advisers have resulted in a range of actions, including deficiency letters and, where appropriate, referrals to the Division of Enforcement. In response to these observations, many of the advisers modified their practices to address the issues identified by EXAMS staff. The Division encourages private fund advisers to review their practices, and written policies and procedures, including implementation of those policies and procedures, to address the issues identified in this Risk Alert.

---

*This Risk Alert is intended to highlight for firms risks and issues that EXAMS staff has identified. In addition, this Risk Alert describes risks that firms may consider to (i) assess their supervisory, compliance, and/or other risk management systems related to these risks, and (ii) make any changes, as may be appropriate, to address or strengthen such systems. Other risks besides those described in this Risk Alert may be appropriate to consider, and some issues discussed in this Risk Alert may not be relevant to a particular firm's business. The adequacy of supervisory, compliance and other risk management systems can be determined only with reference to the profile of each specific firm and other facts and circumstances.*

---

# 2024 / Investment Adviser Compliance Conference

MARCH 6-8 / WASHINGTON, DC

EFFECTIVE STRATEGIES & BEST PRACTICES

## Compliance in the Era of M&A

**Chad Estep** / Corient Private Wealth LLC

**Tori Erker** / Mercer Advisors

**Matt Ahlstrand** / SS&C Advent

**Jamie Lynn Walter** / Latham & Watkins LLP

1



2024 / Investment Adviser  
Compliance Conference

EFFECTIVE STRATEGIES  
& BEST PRACTICES

### Introduction

- Overview of Key Transaction Types
- Panelist Experience
- Lifecycle of a Transaction
  - Introductory Phase
  - LOI
  - Due Diligence
  - Integration
- Role of Outside Counsel

2



## Due Diligence Process

- Overview of Due Diligence Process
  - Pre-LOI
  - Post-LOI
- Key Documents Requested
- Role of Compliance
- Best Practices

3



## Due Diligence Process (continued)

- Important considerations and potential “deal breakers”
  - People and Culture
  - Financial Arrangements
  - Processes and Tools
  - “Assignment” and Change of Control Considerations
  - Other Investment Advisers Act and Investment Company Act Issues

4



## Integration

- Certain Key Risk Areas:
  - Marketing Materials, Endorsements, Testimonials
  - Portfolio Management Systems and Prior Deal Commitments
  - Constraints on Other Operations/Compliance Functions
    - Affiliated Entities and Conflicts of Interest
    - Soft Dollar Arrangements
    - Calculation of Fees; Expense Allocations

5



## Integration (continued)

- Certain Key Risk Areas (continued):
  - Employee Contracts / Compensation Arrangements
  - Books and Records / Legacy Firm Data
- Best Practices for Compliance Testing and Annual Reviews

6



## Closing Remarks

7



## Appendix: Select SEC Case Studies

- *Securities and Exchange Commission v. Navellier & Associates, Inc., and Louis Navellier*, Civil Action No. 17-CV-11633 (District of Massachusetts, filed August 31, 2017), <https://www.sec.gov/litigation/complaints/2017/comp23925.pdf>
- *In the Matter of Sam P. Douglass and Anthony R. Moore* (February 24, 2011), <https://www.sec.gov/litigation/admin/2011/34-63953.pdf>
- *In the Matter of Timbervest, LLC, et al.* (September 17, 2015), <https://www.sec.gov/litigation/opinions/2015/ia-4197.pdf>
- *In the Matter of Morgan Stanley Smith Barney, LLC* (January 13, 2017), <https://www.sec.gov/litigation/admin/2017/34-79794.pdf>
- *In the Matter of Wells Fargo Clearing Services* (August 25, 2023), <https://www.sec.gov/files/litigation/admin/2023/34-98221.pdf>

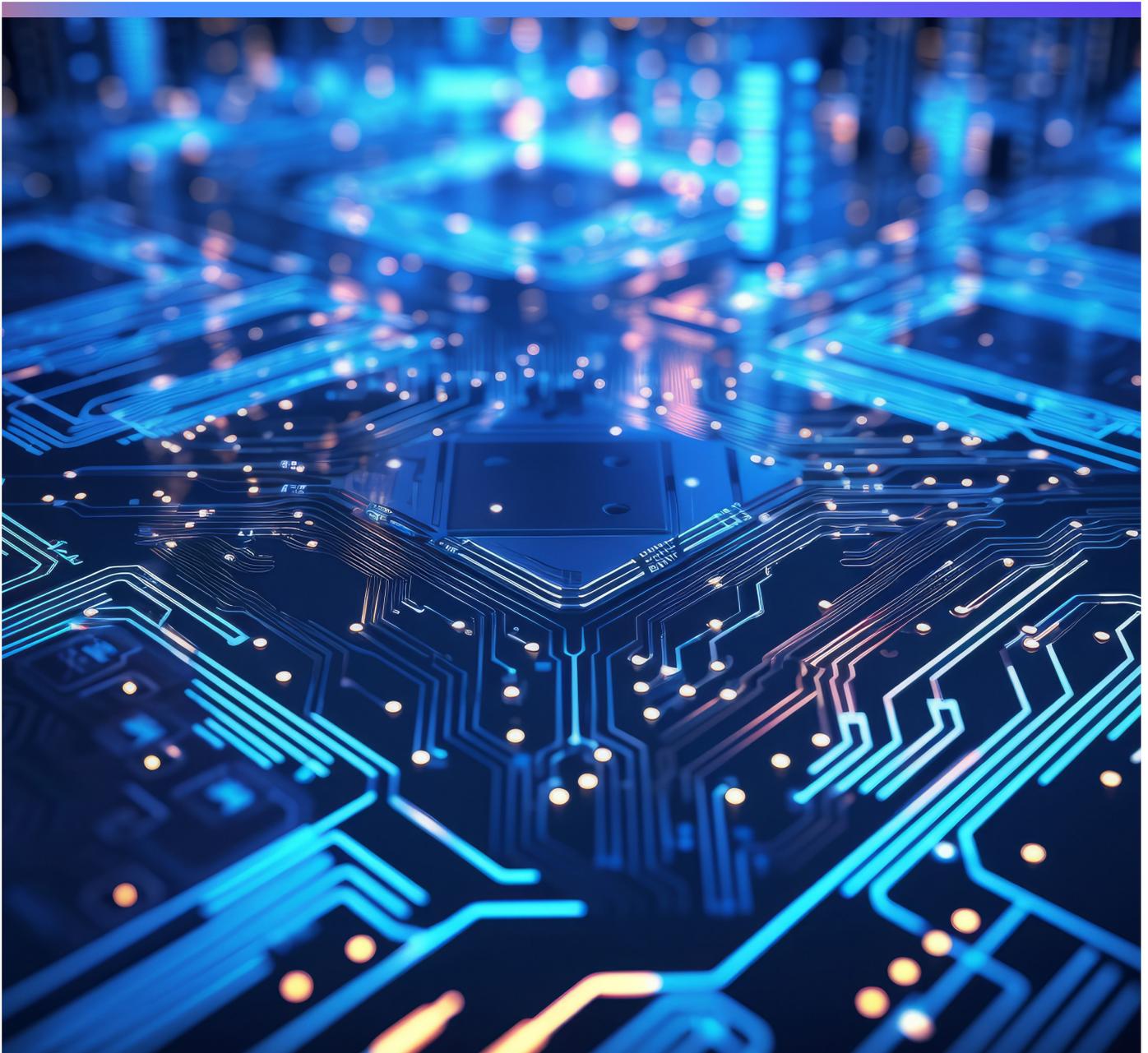
8



9

# Disruptive Technology Views

Achieving better investment outcomes with AI



## Introduction

Will it rain today in my city—or on my portfolio? Since the 1970s, artificial intelligence (AI) has assisted investors with trading strategies and meteorologists with weather forecasts. Defined as machines that mimic the cognitive functions of the human brain, AI seeks and compiles information, helps sift through data, and analyzes it to improve decision-making used in our day-to-day living. AI powers the sensors that collect data on weather, carbon emissions, traffic patterns and countless other items.

The development and deployment of AI tools continue to embed themselves into nearly all aspects of daily life. AI platforms can allow individual users to use facial recognition on their phones, get new streaming recommendations based on personal viewing patterns, ask Siri for directions while driving, and even allow cars to drive without a human at the helm. The challenge of providing such customization cost-effectively and at scale requires AI deployment to understand the interests of clients and prospects as well as the context surrounding them. Automating selections of the next “best” offer for a customer requires real-time database connections, machine-learning and orchestration.

AI can boost most investors’ scale, speed and sophistication. Wealth management profiling systems can dynamically monitor clients’ behaviors and those of their family and associates to help inform their portfolio needs using AI’s ongoing flow of information. Portfolio managers can utilize AI to monitor sentiment across analysts’ reports, earnings calls, stock-price movements, news articles and social media activities. With AI tools, a portfolio manager can identify incongruencies that may lead to large price moves or behavioral biases in trade executions, and they can also decipher in real time whether a company’s practices meet targets for pay equity or carbon footprint reduction. The quality of AI results depend on the human to submit quality queries for better usage and outcomes.

With well-designed AI algorithms, investors can produce better outcomes. However, we still need professionals to operate AI tools to both guide and gut-check their recommendations. In this issue, we provide more on the transformative power of AI in investment management, with **“Copilot, not autopilot: How generative AI augments, but doesn’t replace active management,”** written by Max Gokhman, Head of MosaiQ Investment Strategy; **“Durable passive thematic strategies—A solution unlocked by artificial intelligence,”** by Ralph Corasaniti, Strategic Accounts & Innovation Director, Retirement & Insurance; and **“The ripe opportunity for AI in the workplace,”** by Josh Anderson, Strategic Accounts & Innovation Director, Retirement & Insurance.

# Copilot, not autopilot: How generative AI augments, but doesn't replace active management



**Max Gokhman, CFA**  
Head of MosaiQ Investment  
Strategy, Franklin Templeton  
Investment Solutions

Artificial intelligence (AI) is commonly defined as machines that mimic the cognitive functions of the human brain. For some cases, like playing checkers, where the rulebook is simple, this is a relatively low bar. Indeed, this was one of the first use cases of AI by Arthur Lee Samuel in 1952.<sup>1</sup> However, the bar rises exponentially with every notch of complexity. It wasn't until 1997 that Gary Kasparov would lose a full match to Deep Blue.<sup>2</sup> It took nearly two more decades, even with all the exponential strides in computing power over that time, before AlphaGo beat Go grandmaster Lee Sedol in 2016.<sup>3</sup> Thus, while advances in AI, including the ones we'll discuss in this article, are expanding Earth's collective cognitive ability, it is premature to seek shelter from sentient robot overlords or even fear that they'll fully replace many knowledge workers, such as investment professionals.

Instead, with the advent of large language models (LLMs), which are deep learning algorithms trained on gigantic datasets, AI's output can range from concise summaries to detailed insights. What may first come to mind is OpenAI's GPT-3, of which ChatGPT is the result.<sup>4</sup> GPT-3 was trained

---

**With terabytes of training data, extensive power amplified by distributed computing, and some old-school human ingenuity, the applications of AI to many fields, including investing, will continue to rapidly advance.**

on nearly the entirety of the internet and most books.<sup>5</sup> This gave its neural network 175 billion parameters,<sup>6</sup> which it uses to opine on topics ranging from banal to sublime. With terabytes of training data, extensive power amplified by distributed computing, and some old-school human ingenuity, the applications of AI to many fields, including investing, will continue to rapidly advance. While many of these are beyond the scope of this introductory article, we present use cases of how AI can be harnessed by different investors to potentially improve their desired outcomes and workflows.

## AI capabilities: Data analysis and predictive power

Distilling investing to an extreme, we could say it is determining the fair value of assets—based on analyzing as much public information as can be gathered—and then, if prevailing market prices differ from the results, buying or selling them. The sheer amount of relevant data is vast—financial documents, earnings transcripts, regulatory filings, news articles, day-long congressional testimonies, and nowadays even Reddit conversations and tweets. This data is noisy, non-normal and increasingly unstructured (that is, inherently difficult to analyze). LLMs can both consume and, critically, understand this data at rates eclipsing any analyst team.

A basic output of this task is the ability to summarize information for human consumption—whether it's thousands of social media threads written in zoomer vernacular (no cap)<sup>7</sup> or the dense legalese of a corporate deposition (veritably).<sup>8</sup> Taking it a step further, AI can combine different data sets to extract insights not immediately apparent to even a seasoned human investor.

So, should we all retire and let the machines take over? Not so fast. When properly prompted, LLMs are quick to offer answers with the confidence of an economist spouting talking points on TV. This is because LLMs are trained, on a Pavlovian level, to offer responses humans will trust. There is a reward function in most algorithms for providing acceptable answers. But is their confidence justified? This depends on many factors, and even if fed high-quality data, deep learning algorithms are

fallible. For example, transformer models (which construe most LLMs) can easily veer off track, or hallucinate, because they work by sequentially predicting the next most probable word in a sentence. This is an autoregressive process, where words the LLM generated itself are used to predict the next ones. While at first it sounds similar to how humans think—after all the words we say next are predicated on the ones that just left our mouths—LLMs have a much harder time realizing if they are talking nonsense. Recognizing when content-sounding AI is abjectly wrong, phrasing questions for it with precision, fine-tuning its training, and feeding it the most nutritional data are all reasons for why humans remain a crucial part of the process. We offer practical examples in the world of investing below.

## Use cases for asset management, wealth management, traders and retail investors

Investors of all stripes can potentially benefit from using AI. The technology will not put retail traders on equal footing with institutional investors because they do not have access to the disproportionately expensive and often proprietary data on which to train an AI system that institutional investors have been cultivating for decades; nor would they typically know how to fine-tune deep learning algorithms to maximize their potential. Still AI can boost most investors' scale, speed and sophistication.

### Asset management use cases

Portfolio managers can train LLMs on earnings calls, stock price movements, news articles and social media chatter. They can further input information on behavioral biases (the theory that inefficiencies in the market exist due to human irrationality), their own research notes, security ratings and trade executions. After training, this data can be piped into the LLM in real-time. That, in turn, leads to several novel applications such as:

- Combining the sentiment expressed via unstructured information (tweets, subreddits, analyst reports, news, etc.) with structured data (company fundamentals, consensus forecasts, macro indicators) to identify incongruencies that may lead to large price moves.
- AI can help risk managers by providing early warnings of market shocks inferred from secondary and tertiary effects. For example, imagine a fixed income portfolio where some positions' credit spreads begin rapidly widening. A human manager would immediately understand the increased risk to those underlying positions but what about the rest of the

portfolio? An AI with billions of optimized synapses could predict which issuers could be the next domino based on a multitude of data points—from time series correlations to news articles to 10-Ks (company annual reports). A recent, though tragic, example would be the invasion of Ukraine leading to a sudden contraction in neon gas exports, a key component of automotive semiconductors affecting chipmakers, which then impacted carmakers. A well-trained neural network could find this complex linkage the moment the first mortar hit Mariupol, something few humans did.

- AI can alert portfolio managers if their desired trades exhibit behavioral biases. For instance, according to the disposition effect, some investors are reluctant to sell losing positions, yet happy to shed assets that just had big price pops. Differentiating between a prudent decision supported by valuations and one driven by emotions, like regret avoidance, is where an AI trained on previous trades and behavioral finance can take the role of an unbiased coach.
- Because LLMs can process conversational queries, the knowledge moats for doing complex investment tasks—like multiperiod optimization, strategy simulation and factor decomposition—are drying up. In a way, generative AI is democratizing some of the superpowers quantitative (or quant) investors previously hoarded. Soon a multi-asset portfolio manager could ask their AI copilot to “construct a portfolio that is most resilient to a US Federal Reserve pivot, but could still offer 4% yield, is not overweight the growth factor, and wouldn't have had annualized risk greater than 17% over the last five years” and get a model back. Provided, of course, that one could be constructed with those hurdles. While we know there are no guarantees to achieving these outcomes, we are working on building such a tool at Franklin Templeton Investment Solutions.

### Limitation example

Predicting sentiment from audio and video, as some modern natural learning processing (NLP) engines purport to, is far more complex. If 90% of communication is non-verbal, there are inherent limitations in the ability of AI to glean insights from human interaction. Varying intonations and body language may be subtle and can greatly change the meaning of what is meant in an exchange. Humans have a remarkable ability to pick up on these cues, based on thousands of years of evolution; AI is not capable of this yet.

---

**Understandably, there is both fear and excitement around the advent of AI, and as with most breakthroughs, the nuanced truth should evoke some of both.**

### Sustainable investing use cases

Environmental, social and corporate governance (ESG) analysts could train their AI system on the sustainability disclosures of public companies, quantifiable ESG metrics and press releases about a company's ESG declarations.

- The AI could then attempt deciphering whether popular beliefs about a company's ESG practices match reality, or whether companies practice what they preach on any number of sustainability metrics, such as equal pay, carbon footprint reduction and board independence.
- By analyzing data that has not yet flowed into disclosures, AI can identify which companies are making improvements in their ESG practices. Identifying such ESG improvers early may yield better investment results. For example, what if a company plagued by controversy over its treatment of minority employees started putting in diversity, equity and inclusion (DE&I) language into its newest job postings? AI can generate inferences from data points like this nearly in real-time when properly tuned and trained.

### Wealth management use cases

Financial advisors can use AI systems to maximize their clients' ability to meet the goals most important to them—a task that often involves more than just maximizing return for a given level of risk.

- Determining client investment objectives and risk tolerance is often done through straightforward questions. But how well do clients know themselves, especially under duress? Advisors often receive panicked phone calls from clients after small market drops, demanding “corrective” action, even from those who say they can tolerate large market swings. These requests are often against the clients' interests. AI trained on past interactions can look beyond surveys and better predict client behavior to suggest portfolios most likely to keep them invested through volatility and even recommend opportunities to proactively reach out, before panic sets in.

- Just as self-reported risk tolerance may not match reality, client financial goals are often not appropriately prioritized. AI can analyze client consumption patterns, needs and desires to chart a dynamic path most likely to maximize the chance of achieving their highest priority goals, while minimizing the chance of running out of money. This is an area where we have been pioneering AI use since 2020, by creating a solution that makes personalized asset allocation and consumption recommendations.

### Retail investor use cases

Most examples above require extensive proprietary data and the knowledge to train and tune models. It bears repeating that while AI is a step toward democratization of investing, it is not an equalizer. Without terabytes of quality data, real-time feeds and superlative computing power, even sophisticated retail investors will be at a disadvantage compared to institutions. Nonetheless, commercially available AI models can still benefit them.

- Even more so than institutional portfolio managers who generally have risk managers looking over their shoulder, AI may alert retail investors to behavioral biases they may be exhibiting based on the context surrounding their trading. For example, are they entering an option position where risk could far exceed the equity trades they're used to?
- AI may help create insightful charts, with topical overlays to give visual context to earnings announcements, economic regimes, sector profit margins and possible payouts for a trading strategy.
- LLMs can extract key concepts from lengthy documents—like management commentary or central banker speeches—to help retail investors grasp key concepts.

### Conclusion

Understandably, there is both fear and excitement around the advent of AI, and as with most breakthroughs, the nuanced truth should evoke some of both. While AI may create negative externalities, eradicating humankind is unlikely to become its agenda; and though it will augment our lives, it won't create utopia. For now, in the world of investing, it can fill the role of a tireless junior analyst or unbiased coach, as illustrated by the case studies above. By partnering with algorithms, investors may produce better returns, mitigate risk, reduce their irrational impulses and may come closer to achieving their financial goals.

# Durable passive thematic strategies—A solution unlocked by artificial intelligence



**Ralph Corasaniti, CIMA**  
Strategic Accounts & Innovation  
Director, Retirement & Insurance,  
Franklin Templeton

Few investment styles are as polarizing among professional investors and financial industry observers as thematic investing. Proponents evangelize the unique ability of thematic funds to facilitate participation in structural changes of generational significance, while critics aren't shy in questioning higher relative fees<sup>9</sup> and lower relative performance.<sup>10</sup> Given the intensity of the debate, one might be surprised to learn that thematic investing is far from a recent development, with many considering the 1948 launch of Chester Tripp's "Television Fund," an open-end investment trust "specializing in securities of television, electronics and radio companies,"<sup>11</sup> as the advent of modern thematic investing. Some 75 years later, the traditional definition of a thematic strategy remains a portfolio that offers exposure to an emerging trend with the potential to disrupt an industry, if not society as a whole. The results for fund sponsors in separating trend from fad have predictably been mixed, with the Television Fund's initial thesis being a fair example of success as TV ownership did in fact explode from 1% of households in the United States at the time of the fund's inception to 75% by the time *The Honeymooners* debuted seven years later in 1955.<sup>12</sup>

However, for every vindicated prediction, there are cases of misplaced optimism. The ill-fated Steadman Oceanographic Fund is perhaps the best example, as it captured the imaginations of those inspired by Jacques Cousteau's undersea exploits of the early 1960s, with the fund's intention "to profit from companies that were farming and building communities at the bottom of the sea."<sup>13</sup> Investment returns in that case unfortunately rode Cousteau's damp coattails to the bottom.

Investors for their part seem decidedly undeterred by the raging debate and the wide dispersion of returns, as thematic investment strategies have experienced incredible growth in recent years. Thematic strategies saw their share of the global equity fund market triple to 2.7% by the end of 2021, with over US\$800 billion in assets under management (AUM).<sup>14</sup> While a few well-known strategies have driven the lion's share of that AUM growth, the category's rise has also coincided with a proliferation of thematic fund options—1,952 according to Morningstar, which the research firm classifies using 200 thematic labels as varied as Cloud Computing, Automated Driving, mRNA and Baby Boomers.<sup>15</sup> On one hand, the explosive growth of investable themes has itself been an empowering and democratizing trend that offers the retail investor another way to test, express and evaluate their own investment theses. However, the fear from a fiduciary perspective is that the aggregate effect of this increased optionality may exacerbate a traditional behavioral finance challenge by introducing additional opportunities for investors to make poor decisions around timing. For years, DALBAR has published a study that uses long-term mutual fund flow data to assess and compare average investor returns to various investment categories—recently showcasing a return of 3.1% for investors vs 9.8% for US equities over the 2003–2022 timeframe.<sup>16</sup> "The explanation for why retail investors lagged the broader market to such

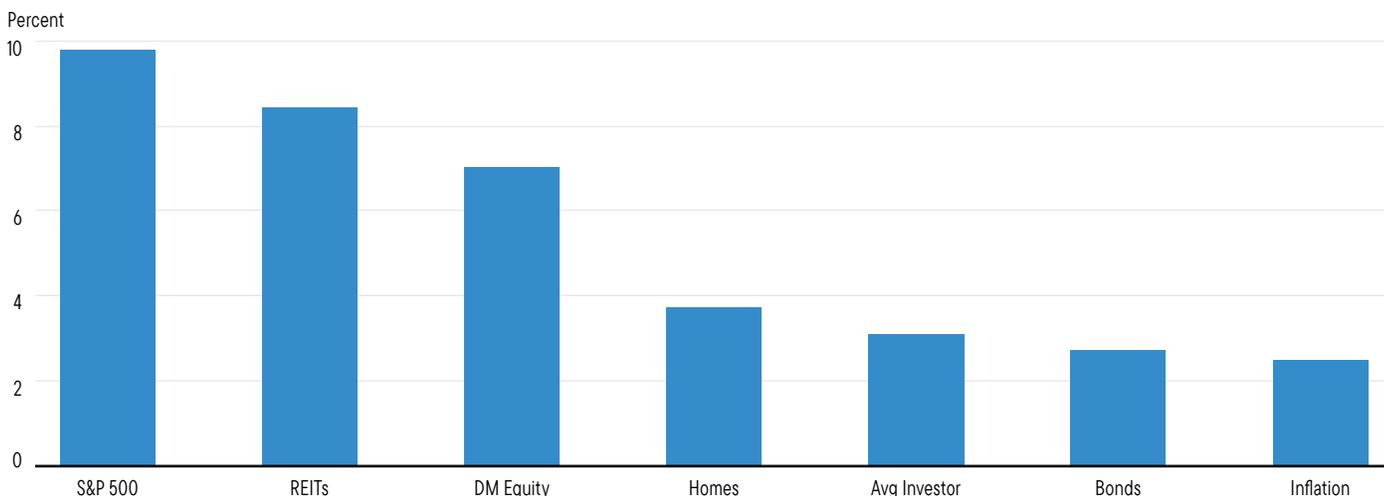
---

**“The explanation for why retail investors lagged the broader market to such a devastating degree over the course of an epic two-decade run in the stock market comes down to fear and volatility. Too often investors get sucked into the news cycle and end up selling at the worst time.”**

**Jeff Schulze**  
Head of Economic and Market Strategy  
ClearBridge Investments

## Effects of Panic Attacks on Average Investors

**Exhibit 1: 20-Year Annualized Returns by Asset Class (2003–2022)**



Source: Bloomberg. June 30, 2023. Indexes and data used—S&P 500 Index, FTSET NAREIT All Equity REITS Index, MSCI EAFE Index, US Existing Home Sales Median Price YOY %, Bloomberg Global Aggregate TR Index, US CPI Urban Consumers YOY. Indexes are unmanaged and one cannot directly invest in them. They do not include fees, expenses, or sales charges. Important data provider notices and terms available at [www.franklintempletondatasources.com](http://www.franklintempletondatasources.com). **Past performance is not an indicator or guarantee of future results.**

a devastating degree over the course of an epic two-decade run in the stock market comes down to fear and volatility. Too often investors get sucked into the news cycle and end up selling at the worst time,” Jeff Schulze, Head of Economic and Market Strategy at ClearBridge Investments, a leading global equity manager with US\$165.4 billion in AUM as of June 30, 2023.

As startling as the 6%+ annualized lag is, it’s prudent to wonder whether net returns might be even worse for investors buying into thematic funds vs the broader US mutual fund universe that DALBAR analyzed, which predominantly skews toward long-term buy-and-hold type strategies. By contrast, many of today’s thematic strategies, particularly in the passive category, are built to capture growth from impermanent trends—leaving investors that are already struggling to steel themselves against volatility the additional challenge of identifying when an investment theme has run its course. Let’s take another look at some of the thematic labels listed above.

Automated driving carries promise of societal change, but the theme has a destination at which point the technology/ infrastructure would become commonplace and no longer carry outsize growth expectations. mRNA applications including rapid vaccine development are at the bleeding edge of biotech innovation today, but how long until that approach matures or is supplanted? Finally, cloud computing

technology has unquestionably driven both structural change and investment performance in related strategies, but the technology is now in the late stages of mass adoption. Each of these examples showcase the four phases of the technology lifecycle: research and development (R&D), growth, maturation and decline, visually expressed by the traditional “S-Curve” pattern seen in the below exhibit.

## Cloud Computing Appears to Be Reaching Maturation

**Exhibit 2: Growth of US\$10,000 of Morningstar Global Cloud Computing Fund Composite**



Source: Morningstar Direct. As of July 2023. **Past performance is not an indicator or a guarantee of future results.**

Simply put, a major challenge with thematic investing today is that a large proportion of strategies focus on singular, static themes with finite windows of growth, rendering them as most appropriate for tactical exposures and not as long-term holdings.

One solution for the static problem in thematic investing already exists: actively managed thematic strategies that target multiple themes with mandates broad enough to allow for manager discretion in navigating transitions from declining to emerging growth opportunities. Certainly not a panacea, as ultimate success will vary based on manager skill, but an active approach effectively removes the structural limitation inherent in a passive portfolio constructed based on insights from a single point in time. For the larger passive thematic category, which Morningstar estimated to represent 75% in the United States as of August 2023, there may be two solutions worth pursuing: a) the industry can offer improved educational content and tools at the point of sale that clearly identify narrowly focused thematic strategies as tactical vehicles vs long-term holdings (and advise on prudent usage); and/or b) with the help of AI, passive thematic strategies can expand beyond tactical concepts by implementing durable evergreen investment theses.

Within the world of AI, recent advancements in NLP and the related ability for sophisticated LLMs to interact with verified Knowledge Graphs offer the potential for a fundamental evolution in thematic investing. This progress may also unlock a new investment style—durable passive thematic strategies. By harnessing these new innovations, an asset manager can effectively design an evergreen passive strategy that builds, monitors and calibrates portfolios comprised of companies with verified connections to desired themes. To explain, let's first examine how the AI-driven approach works, and then we'll compare that to a legacy passive approach.

ChatGPT, the generative AI solution that OpenAI developed with funding from Microsoft, has demonstrated for the AI-curious masses in 2023 that LLMs have an impressive ability to respond instantly to complex questions or prompts with seemingly well-reasoned rationales. While it's clearly a powerful tool, when it comes to accuracy, even OpenAI's CEO Sam Altman cautions that ChatGPT has the ability to "hallucinate" and "confidently state things as if they were facts that are entirely made up,"<sup>17</sup> which illuminates the reality that language models on their own do not equal knowledge models. According to Shankar Vaidyanathan, Founder and CEO of Noonum (an AI-powered service for building

### Passive Strategies Now Dominate Thematic Investing

**Exhibit 3: Passive Market Share of US Thematic Funds**



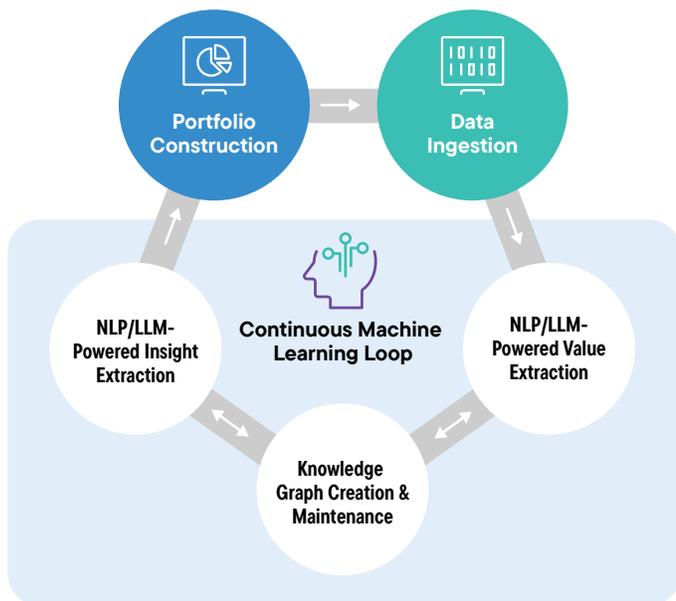
Source: Morningstar Direct. As of August 30, 2023.

customized thematic portfolios and indexes), in order for AI to effectively generate investable insights that are trustworthy, a language model must be paired with a knowledge model or graph that converts billions of ingested data points into a fact-based temporal network.

The three hallmark components of a knowledge graph are nodes (e.g., a person, company, industry, place, etc.), edges (the relationships between and among nodes), and labels that identify the nature of those relationships. For illustrative purposes, the AI-driven portfolio construction process for a thematic portfolio might break out as follows: 1) market-focused data ingestion (earnings call transcripts, Securities and Exchange Commission filings, patent applications, financial industry news, etc.); 2) NLP/LLM powered value extraction (what is implied in the text, is the sentiment positive or negative, etc.); 3) knowledge graph creation and maintenance (verifiable and auditable relationship network); 4) NLP/LLM powered insight extraction (what themes are inherent from the captured data and relationships and how are companies quantifiably connected to each theme); and 5) based on the strategy design, an allocated portfolio can then be created and continuously updated without the day-to-day involvement of a human portfolio manager.

### How Might an AI-Driven Portfolio Construction Process for a Thematic Portfolio Breakout?

**Exhibit 4: Continuous Machine-Learning Loop**



Source: Franklin Templeton Industry Advisory Services. For illustrative purposes only.

**According to Shankar Vaidyanathan, Founder and CEO of Noonum (an AI-powered service for building customized thematic portfolios and indexes), in order for AI to effectively generate investable insights that are trustworthy, a language model must be paired with a knowledge model or graph that converts billions of ingested data points into a fact-based temporal network.**

To highlight the potential magnitude of improvement here, let's compare a static passive thematic approach to a durable passive thematic approach using two FinTech themes as our focus: blockchain and mobile payments. The simple legacy passive approach would be to create separate portfolios tied to each theme, using only the insights available at a singular point in time to define the theme and desired exposure methodologies (e.g., basing weights on market-capitalization and/or relative revenue percentages tied to the theme are two common approaches).

For a sophisticated active trader that values flexibility and control, the legacy approach likely works fine as the trader can tactically determine when they want to shift their allocation out of a maturing theme and into a developing theme in order to both avoid declines and capture periods of rapid growth. However, for long-term investors that are ill-equipped or uninterested in running a tactical portfolio, or for financial products that require minimum duration investment periods, e.g., index-linked insurance solutions with typical contract terms of 7–10 years, the static approach is suboptimal or even non-viable. This claim is accentuated by the fact that these two themes in particular find themselves on opposite ends of the technology life cycle, with mobile payments arguably approaching the maturation phase, while blockchain technology is very much in the early R&D phase.

---

**While static passive thematic strategies will likely persist as a desired solution for day traders and tactical allocators, AI-powered durable passive thematic portfolios can offer investors access to robust long-term investment strategies that optimize allocations to existing and perhaps yet-to-emerge themes, in a manner that will hopefully improve both strategy returns and realized investor outcomes.**

Revisiting the AI-powered process detailed prior, a durable passive approach would offer a few advantages. First, the AI strategy could be designed to take an empirical approach to implementing the shift from a maturing theme like mobile payments to an emerging theme like blockchain. At the discretion of a portfolio manager informed by powerful AI-based insights, perhaps a blended multi-theme portfolio would be programmed to maintain a low allocation to a theme like blockchain while capital expenditures on R&D relative to revenue are proportionally greater than a theme like mobile payments, while being poised to quickly invert allocations based on momentum shifts in the underlying data. Beyond that, perhaps in generation 2.0 of these strategies, an effective knowledge graph and language model pairing might detect when a thematically related but entirely new investment category emerges that promises to supplant the current category, e.g., blockchain is replaced by some yet to be invented galactic-chain protocol that disburses transaction records across an interstellar network of nano-satellites (one day!). Then not only is AI handling the shift from a maturing S-curve to an emerging S-curve for known technologies, it's then also eventually identifying a third technology that didn't exist when the fund launched, determining its thematic relevance to the strategy, and implementing an allocation transition. By automating allocations to companies at the vanguard of innovation within a chosen sector or category, the strategy is ensuring long-term, durable relevance for the consumer—a significant improvement over the buy- (and sell) at-your-own-risk static thematic funds of today.

As investors have indicated with their dollars, the targeted exposures thematic investing strategies have offered since 1948—active or passive—are attractive in spite of their inherent limitations. Albeit gradually, the asset-management industry fortunately seems eager to better understand or even embrace emerging AI capabilities, which should ultimately usher in a new generation of solutions that address some of the enduring challenges. While static passive thematic strategies will likely persist as a desired solution for day traders and tactical allocators, AI-powered durable passive thematic portfolios can offer investors access to robust long-term investment strategies that optimize allocations to existing and perhaps yet-to-emerge themes, in a manner that will hopefully improve both strategy returns and realized investor outcomes.

# The ripe opportunity for AI in the workplace



**Josh Anderson, CFA**  
Strategic Accounts & Innovation  
Director, Retirement & Insurance,  
Franklin Templeton

---

## Two imperfect plans

The way Americans have saved for retirement has changed and evolved over time. Until the 1970s, the primary retirement vehicle corporations offered to their employees was a defined benefit (DB) plan, or pension. This type of plan provides a pre-determined benefit typically calculated via a combination of salary, years of employment and other factors. When an employee retired, they had the benefit of knowing they would have a consistent source of income. The downside for the employer was that pensions carry a large cost and sit as a balance-sheet liability, potentially impacting the company's stock price or credit rating.

Then came the Revenue Act of 1978, which created the defined contribution (DC) plan. This type of plan allows the employee to contribute a percentage of their salary, often with an employer match, with the ability to invest it on their own. The benefit to the employer is that it no longer carries pension liability, has more consistent plan funding costs, and shifts the responsibility of investment returns to the employee. The benefit to the employee is that they have more control over the accounts and how much they save.

---

**The next-generation chatbots that financial services will deploy will have the knowledge of a top financial advisor with the power of financial calculators at the speed of milliseconds.**

Since the 1980s, there has been a trend of replacing DB plans with DC plans, which has contributed to a retirement income shortfall; this is partly due to the knowledge gap in the average employees' investing and financial planning skills versus the professionals who manage DB plans. The average person lacks the skill to effectively determine the nuances of a financial plan, including how much to save, what account type to use, what *and* how much to invest in.

## Putting AI to work

Conversational AI can significantly enhance the employee/participant experience with their work benefits. Think of today's online chatbots used for customer service on websites for cable, phone and other service providers where simple conversations or tasks are taking place. The next-generation chatbots that financial services will deploy will have the knowledge of a top financial advisor with the power of financial calculators at the speed of milliseconds. In addition, the advice given via these AI chatbots will be hyper-personalized to the user engaging with it. How? With integrations, conversational AI will have connections to payroll systems, recordkeepers, wealth platforms and custodians, which will unleash not only operational tasks such as changing contributions or getting a statement emailed through the chatbots, but also provide answers to questions like: "Will I be able to retire at age 60?" The power of AI, along with these integrations, will allow the chatbots not only to provide a simple yes/no answer to that burning question on everyone's minds, but also provide personalized advice.

In addition, AI will be able to generate personalized financial reports and videos either monthly, quarterly or even ad hoc for one's entire workplace benefit picture.

When it comes to what one should do next financially, AI will provide the "next best action" tailored to an individual. How does Amazon know what you want to buy next, or Netflix know what you should binge next, or Spotify what you want to listen to next? As creepy as it sometimes is, these "can't do without" services all leverage AI to create a better user experience and huge brand loyalty. This is exactly what companies in the financial services sector are building with AI—what should you do *next*?

## The changing workplace

A more recent development than the DB-to-DC shift is the generational change in the way people work, and therefore how they receive employer benefits like health insurance and retirement plans. Over the past 10–15 years, technology has enabled millions of Americans to find alternative ways of making money through the gig economy. The “gig economy” is a term used to describe a system that connects workers with temporary jobs, typically on demand, and is credited with disrupting multiple large industries. One notable example is Uber, which competes with taxis and allows users to call a ride on demand via a mobile app. In 2014, a New York City taxi medallion had a peak value of US\$1.32 million, but in 2022 that value had dropped to an average of US\$137,000.<sup>18</sup> Over this same period, Uber has increased its revenue from less than US\$500 million to over US\$31 billion in 2022.<sup>19</sup> There are many other gig economy services like renting a house (Airbnb), a car (Turo), a recreational vehicle (RVshare), or having someone grocery shop for you (Instacart) or deliver your takeout (DoorDash). The gig economy has also proliferated into skilled labor as well, with platforms like Upwork and Fiverr matching coders, designers, writers and more with customers who need specific projects done.

It is estimated that by 2027, over half the American workforce will be in the gig economy if growth trends persist.<sup>20</sup> This poses both a challenge and opportunity. As workers leave the employee/W-2 world for the gig economy/10-99 world, they will need to replace the corporate benefits they were receiving. When leaving the corporate world, access to quality advice will be a challenge. Most will lose access to the financial wellness programs their employers had offered. Typically, financial advisors target those with investable assets over US\$1 million. Roughly 98% of the US population falls beneath this threshold, and therefore will need to receive advice in an alternative way.

## AI for the big picture

There are digital services for individual retirement savers that exist, but most are fragmented and non-integrated—they look at an individual's financial picture in silos based on account type. In the real-world, people don't view themselves as only a 401k or IRA investor. They also have other planning needs like health savings, emergency savings, college planning, budgeting and debt management, to name a few. Legacy services haven't had particularly engaging user experiences that might spur an investor to take action on a recommendation.

One of the primary advantages of AI in retirement investing is its ability to offer a comprehensive overview of an individual's financial situation. AI-powered platforms can consolidate information from various sources, including bank accounts, investment portfolios, real estate holdings, and more. By analyzing this data, AI can provide investors with a clear, real-time picture of their financial health. This holistic view enables better decision-making, as investors can see how different aspects of their finances interconnect and impact their retirement goals.

One company addressing this challenge is TIFIN, a Colorado-based fintech. TIFIN has built a fully integrated workplace platform utilizing AI-assistants to provide personalized, intelligent and actionable advice. In addition to providing advice on major goals like saving for retirement, the platform

---

**One of the primary advantages of AI in retirement investing is its ability to offer a comprehensive overview of an individual's financial situation. AI-powered platforms can consolidate information from various sources, including bank accounts, investment portfolios, real estate holdings, and more.**

---

**Imagine a not-too-distant future where workers will receive an email from human resources, or gig workers will sign up via app. These individuals will then go through a discussion about their goals and current finances with an avatar of their choice. It could be someone they admire or feel more comfortable with—or even an aged version of themselves.**

can advise on smaller goals like: “How much car can I afford?” This is done within the context of the individual’s holistic picture and long-term plans, thus helping to balance both long-term and short-term goals. TIFIN is using conversational AI to increase engagement by having a more human-like experience throughout the entire process.

Where will this take us? Imagine a not-too-distant future where workers will receive an email from human resources, or gig workers will sign up via app. These individuals will then go through a discussion about their goals and current finances with an avatar of their choice. It could be someone they admire or feel more comfortable with—or even an aged version of themselves. The AI will be able to combine information from the previously discussed sources (i.e., payroll, recordkeeping, custody) and fill in the blanks via the discussion with the avatar. The worker will then receive a holistic and personalized plan to achieve their goals across all of their accounts, including insurance. With one step, they can take action—account paperwork is automatically filled and opened.

To the worker, this entire experience happens within a human-like discussion with conversational AI. Accounts are monitored over time and suggestions periodically provided to help optimize goal achievement. They can get answers in the context of their entire personalized picture to questions such as: “How much house can I afford in Tampa?” AI will help increase access to high-quality personalized advice and over time, should lead to better outcomes.

---

## Endnotes

1. Source: Samuel, A.L. “Some Studies in Machine Learning Using the Game of Checkers,” IBM Journal of Research and Development, July 1959.
2. Source: IBM, Icons of Progress, “Deep Blue,” Featured September 13, 2011.
3. Source: Borowiec, S. “AlphaGo seals 4-1 victory over Go grandmaster Lee Sedol,” The Guardian, March 15, 2016.
4. Companies referenced are for illustrative purposes only. Discussions should not be regarded as any type of trading recommendation, or as a signal about any past, current or future trading activity in any fund or strategy, by Franklin Templeton and its affiliates.
5. Source: Brown, T., B. Mann, N. Ryder, et al., “Language Models are Few-Shot Learners,” Cornell University arXiv, 2020.
6. A trainable parameter within a neural network is the weight given to each connection between neurons that is adjusted during training to optimize the model’s accuracy in making predictions on data it hasn’t seen yet. The more parameters, the more complex the neural pathways, and thus the overall model.
7. “No cap” is a slang phrase... It means “no lie” or “I’m not lying” and is often used to emphasize the truthfulness or sincerity of a statement. OpenAI’s ChatGPT.
8. “Veritably” is an adverb that means in a manner that is unquestionably true, accurately, or genuinely. It is used to emphasize the truth or accuracy of a statement... OpenAI’s ChatGPT.
9. Source: Lee, Isabelle and Bloomberg. “The \$115 billion thematic ETF boom is still going strong despite a brutal year: ‘We are narrative creatures.’” Fortune. December 10, 2022.
10. Source: “Thematic funds triple share of global investments in a decade.” Financial Times. April 10, 2022.
11. Source: “TimesMachine: August 24, 1948.” NY Times. Accessed October 2023.
12. Source: “Television in the United States.” Wikipedia. Accessed October 2023.
13. Source: Jaffe, Chuck. “Lessons learned in funds that died.” The Seattle Times. December 30, 2007.
14. Source: “Thematic Fund Handbook: Answering the key questions asked by investors considering an allocation to thematic investments.” Morningstar. September 13, 2022.
15. Source: “Morningstar Global Thematic Funds Landscape 2022.” Morningstar. March 2022.
16. Source: “US Economy: Anatomy of a Recession.” ClearBridge Investments. October 2023. **Past performance is not an indicator or a guarantee of future results.**
17. Source: Reed, Betsy. “‘We are a little bit scared’: OpenAI CEO warns of risks of artificial intelligence.” The Guardian. March 17, 2023.
18. Source: “NYC Yellow Taxicabs—The Road Ahead!” Black Car News. July 1, 2022.
19. Sources: “Global net revenue of Uber from 2013 to 2022.” Statista. August 29, 2023; Uber 2022 Annual Report.
20. Source: “Number of freelancers in the United States from 2017 to 2028.” Statista. November 3, 2023.

## WHAT ARE THE RISKS?

**All investments involve risks, including possible loss of principal.**

**Blockchain and cryptocurrency investments** are subject to various risks, including inability to develop digital asset applications or to capitalize on those applications, theft, loss, or destruction of cryptographic keys, the possibility that digital asset technologies may never be fully implemented, cybersecurity risk, conflicting intellectual property claims, and inconsistent and changing regulations. Speculative trading in bitcoins and other forms of cryptocurrencies, many of which have exhibited extreme price volatility, carries significant risk; an investor can lose the entire amount of their investment. Blockchain technology is a new and relatively untested technology and may never be implemented to a scale that provides identifiable benefits. If a cryptocurrency is deemed a security, it may be deemed to violate federal securities laws. There may be a limited or no secondary market for cryptocurrencies.

**Digital assets** are subject to risks relating to immature and rapidly developing technology, security vulnerabilities of this technology, (such as theft, loss, or destruction of cryptographic keys), conflicting intellectual property claims, credit risk of digital asset exchanges, regulatory uncertainty, high volatility in their value/price, unclear acceptance by users and global marketplaces, and manipulation or fraud. Portfolio managers, service providers to the portfolios and other market participants increasingly depend on complex information technology and communications systems to conduct business functions. These systems are subject to a number of different threats or risks that could adversely affect the portfolio and their investors, despite the efforts of the portfolio managers and service providers to adopt technologies, processes and practices intended to mitigate these risks and protect the security of their computer systems, software, networks and other technology assets, as well as the confidentiality, integrity and availability of information belonging to the portfolios and their investors.

Any companies and/or case studies referenced herein are used solely for illustrative purposes; any investment may or may not be currently held by any portfolio advised by Franklin Templeton. The information provided is not a recommendation or individual investment advice for any particular security, strategy, or investment product and is not an indication of the trading intent of any Franklin Templeton managed portfolio.



## IMPORTANT LEGAL INFORMATION

This material is intended to be of general interest only and should not be construed as individual investment advice or a recommendation or solicitation to buy, sell or hold any security or to adopt any investment strategy. It does not constitute legal or tax advice. This material may not be reproduced, distributed or published without prior written permission from Franklin Templeton.

The views expressed are those of the investment manager and the comments, opinions and analyses are rendered as of the publication date and may change without notice. The underlying assumptions and these views are subject to change based on market and other conditions and may differ from other portfolio managers or of the firm as a whole. The information provided in this material is not intended as a complete analysis of every material fact regarding any country, region or market. There is no assurance that any prediction, projection or forecast on the economy, stock market, bond market or the economic trends of the markets will be realized. The value of investments and the income from them can go down as well as up and you may not get back the full amount that you invested. Past performance is not necessarily indicative nor a guarantee of future performance. **All investments involve risks, including possible loss of principal.**

Any research and analysis contained in this material has been procured by Franklin Templeton for its own purposes and may be acted upon in that connection and, as such, is provided to you incidentally. Data from third-party sources may have been used in the preparation of this material and Franklin Templeton ("FT") has not independently verified, validated or audited such data. Although information has been obtained from sources that Franklin Templeton believes to be reliable, no guarantee can be given as to its accuracy and such information may be incomplete or condensed and may be subject to change at any time without notice. The mention of any individual securities should neither constitute nor be construed as a recommendation to purchase, hold or sell any securities, and the information provided regarding such individual securities (if any) is not a sufficient basis upon which to make an investment decision. FT accepts no liability whatsoever for any loss arising from use of this information and reliance upon the comments, opinions and analyses in the material is at the sole discretion of the user.

Products, services and information may not be available in all jurisdictions and are offered outside the U.S. by other FT affiliates and/or their distributors as local laws and regulation permits. Please consult your own financial professional or Franklin Templeton institutional contact for further information on availability of products and services in your jurisdiction.

**Issued in the U.S.** by Franklin Distributors, LLC, One Franklin Parkway, San Mateo, California 94403-1906, (800) DIAL BEN/342-5236, franklintempleton.com – Franklin Distributors, LLC, member FINRA/SIPC, is the principal distributor of Franklin Templeton U.S. registered products, which are not FDIC insured; may lose value; and are not bank guaranteed and are available only in jurisdictions where an offer or solicitation of such products is permitted under applicable laws and regulation.

**Canada:** Issued by Franklin Templeton Investments Corp., 200 King Street West, Suite 1500 Toronto, ON, M5H3T4, Fax: (416) 364-1163, (800) 387-0830, www.franklintempleton.ca.

**Offshore Americas:** In the U.S., this publication is made available only to financial intermediaries by Franklin Distributors, LLC, member FINRA/SIPC, 100 Fountain Parkway, St. Petersburg, Florida 33716. Tel: (800) 239-3894 (USA Toll-Free), (877) 389-0076 (Canada Toll-Free), and Fax: (727) 299-8736. Investments are not FDIC insured; may lose value; and are not bank guaranteed. Distribution outside the U.S. may be made by Franklin Templeton International Services, S.à r.l. (FTIS) or other sub-distributors, intermediaries, dealers or professional investors that have been engaged by FTIS to distribute shares of Franklin Templeton funds in certain jurisdictions. This is not an offer to sell or a solicitation of an offer to purchase securities in any jurisdiction where it would be illegal to do so.

**Issued in Europe by:** Franklin Templeton International Services S.à r.l. – Supervised by the *Commission de Surveillance du Secteur Financier* – 8A, rue Albert Borschette, L-1246 Luxembourg. Tel: +352-46 66 67-1, Fax: +352-46 66 76. **Poland:** Issued by Templeton Asset Management (Poland) TFI S.A.; Rondo ONZ 1; 00-124 Warsaw. **South Africa:** Issued by Franklin Templeton Investments SA (PTY) Ltd, which is an authorised Financial Services Provider. Tel: +27 (21) 831 7400, Fax: +27 (21) 831 7422. **Switzerland:** Issued by Franklin Templeton Switzerland Ltd, Stockerstrasse 38, CH-8002 Zurich. **United Arab Emirates:** Issued by Franklin Templeton Investments (ME) Limited, authorized and regulated by the Dubai Financial Services Authority. **Dubai office:** Franklin Templeton, The Gate, East Wing, Level 2, Dubai International Financial Centre, P.O. Box 506613, Dubai, U.A.E. Tel: +9714-4284100, Fax: +9714-4284140. **UK:** Issued by Franklin Templeton Investment Management Limited (FTIML), registered office: Cannon Place, 78 Cannon Street, London EC4N 6HL. Tel: +44 (0)20 7073 8500. Authorized and regulated in the United Kingdom by the Financial Conduct Authority.

**Australia:** Issued by Franklin Templeton Australia Limited (ABN 76 004 835 849) (Australian Financial Services License Holder No. 240827), Level 47, 120 Collins Street, Melbourne, Victoria 3000. **Hong Kong:** Issued by Franklin Templeton Investments (Asia) Limited, 17/F, Chater House, 8 Connaught Road Central, Hong Kong. **Japan:** Issued by Franklin Templeton Japan Co., Ltd., Shin-Marunouchi Building, 1-5-1 Marunouchi Chiyoda-ku, Tokyo 100-6536, registered in Japan as a Financial Instruments Business Operator [Registered No. The Director of Kanto Local Finance Bureau (Financial Instruments Business Operator), No. 417]. **Korea:** Issued by Franklin Templeton Investment Trust Management Co., Ltd., 3rd fl., CCMM Building, 12 Youido-Dong, Youngdungpo-Gu, Seoul, Korea 150-968. **Malaysia:** Issued by Franklin Templeton Asset Management (Malaysia) Sdn. Bhd. & Franklin Templeton GSC Asset Management Sdn. Bhd. This document has not been reviewed by Securities Commission Malaysia. **Singapore:** Issued by Templeton Asset Management Ltd. Registration No. (UEN) 199205211E, 7 Temasek Boulevard, #38-03 Suntec Tower One, 038987, Singapore.

Please visit [www.franklinresources.com](http://www.franklinresources.com) to be directed to your local Franklin Templeton website.

The views and opinions expressed are not necessarily those of the broker/dealer, or any affiliates. Nothing discussed or suggested should be construed as permission to supersede or circumvent any broker/dealer policies, procedures, rules, and guidelines.



# 2024 / Investment Adviser Compliance Conference

MARCH 6-8 / WASHINGTON, DC

EFFECTIVE STRATEGIES & BEST PRACTICES

## Outsourcing and Vendor Due Diligence

Smaller and Medium Firms

Joe LaFemina / SS&C Advent

Gretchen Lee / Clifford Swan Investment Counsel

Jyothi San Juan / Segall Bryant & Hamill

Karen A. Aspinall / Practus LLP (MODERATOR)

1



2024 / Investment Adviser  
Compliance Conference

EFFECTIVE STRATEGIES  
& BEST PRACTICES

## Fiduciary Obligations of Investment Advisers

### Fiduciary Standard

- ❖ Duty of Care – act in client’s best interests
- ❖ Duty of Loyalty – prevent, mitigate and disclose conflicts

These standards apply to “supervised persons” but also apply to the oversight of third parties that perform certain functions for the adviser

2



## Why Outsource?

- ❖ Technical expertise
- ❖ Less expensive than building out functionality
- ❖ Lack of appropriate personnel
- ❖ Efficiency

3



## Overview of Proposed Rule 206(4)-11

### Create a Framework for Service Provider Oversight:

- ❖ Conduct *reasonable* due diligence before engaging a Service Provider to perform a Covered Function
- ❖ Periodically monitor the performance and reassess the retention of the Service Provider to reasonably determine it is appropriate to continue to outsource to the Service Provider
- ❖ Recordkeeping Amendments – Proposed Rule 204-2
- ❖ Form ADV amendments

4



## Overview of Proposed Rule 206(4)-11

### What is a Covered Function?

- ❖ those necessary for the adviser to provide its investment advisory services in compliance with the Federal securities laws; and
- ❖ those that, 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.

5



## Overview of Proposed Rule 206(4)-11

### Who is a Service Provider?

A Service Provider is an entity that performs a Covered Function and is not otherwise a supervised person of an investment adviser

- ✓ The Proposal does not provide an exclusion for affiliates

6



## Overview of Proposed Rule 206(4)-11

### Examples of Service Providers and Covered Functions

- ❖ Sub-Adviser / provides investment advice
- ❖ Pricing service / provides critical data
- ❖ Model provider / provides algorithms used to run a strategy
- ❖ Compliance functions / outsourced CCO, routine filings agent
- ❖ Ministerial/clerical activities are not a Covered Function

7



## Overview of Proposed Rule 206(4)-11

### Pre-Engagement Due Diligence

- ❖ Scope of Services
- ❖ Mitigation of Risks
- ❖ Determination of capacity/competency/resources
- ❖ Assess Service Provider's material subcontracting arrangements, if any, and how to mitigate/manage risks
- ❖ Reasonable assurance of recordkeeping
- ❖ Reasonable assurance Service Provider will provide an orderly process for termination

8

**IAA** 2024 Investment Adviser Compliance Conference **EFFECTIVE STRATEGIES & BEST PRACTICES**

## Overview of Proposed Rule 206(4)-11

### Post Engagement Due Diligence

- ❖ Must conduct reasonable ongoing due diligence
- ❖ Periodic monitoring of performance - timing and frequency depends on facts and circumstances
- ❖ Determine Service Provider remains appropriate to continue to outsource the Covered Function

9

**IAA** 2024 Investment Adviser Compliance Conference **EFFECTIVE STRATEGIES & BEST PRACTICES**

## Overview of Proposed Rule 206(4)-11

### Methods to Conduct Due Diligence

- ❖ Tailored to scope and function (has there been any change in the services)
- ❖ Conduct risk assessment and mitigate risks
- ❖ Review standard reports or DDQs (SOC1, SOC2 reports)
- ❖ Onsite meetings
- ❖ Technology demonstrations, changes in applications, testing

10



## Overview of Proposed Rule 204-2

### Proposed Recordkeeping Amendments

- ❖ Record of Service Providers and Covered Functions
- ❖ Records of initial due diligence assessment and ongoing monitoring
- ❖ Written agreements with a Service Provider
- ✓ Maintain in easily accessible place during relationship and 5 years after.
- ✓ Due diligence and monitoring applies to outsourced recordkeepers (e.g., cloud storage)

11



## Overview of Proposed Rule 204-2

### Proposed Recordkeeping Amendments

- ❖ Obtain reasonable assurance that the Service Provider will:
  - Implement processes for maintaining records that meet the adviser's obligations under Proposed Rule 204-2
  - Allow the adviser and the SEC staff to access the adviser's electronic records easily through computers or systems
  - Ensure continued availability of records after termination of the Service Provider

12



**IAA** 2024 Investment Adviser Compliance Conference **EFFECTIVE STRATEGIES & BEST PRACTICES**

## ADV Amendments

### Proposed Amendments to Form ADV

- ❖ New Item 7.C to Part 1A
  - Name and other information about the arrangement
  - Classify nature of Covered Functions – check boxes
  - Doesn't apply to recordkeepers – duplicative of Item 1.L

13



**2024** Investment Adviser Compliance Conference  
MARCH 6-8 / WASHINGTON, DC  
**EFFECTIVE STRATEGIES & BEST PRACTICES**

# QUESTIONS?

14



15

**Outsourcing and Vendor Due Diligence  
(Smaller and Medium Firms)**

**Karen Aspinall, Practus, LLP  
Partner, Practice Area Chair - Financial Services**

**Investment Adviser Association Compliance Conference**

**March 8, 2024**

On October 26, 2022, the U.S. Securities and Exchange Commission (“SEC”) proposed rule 206(4)-11 (the “Proposed Rule”) under the Investment Advisers Act of 1940, as amended (the “Advisers Act”) regarding outsourcing by investment advisers.<sup>1</sup> While the Proposed Rule is still pending, it continues to be listed as one of the rules that is in the final rule stage on the SEC’s Fall 2023 Agency Rule List.<sup>2</sup> The Proposed Rule provides a more prescriptive approach to outsourcing, and articulates specific requirements that must be met to satisfy an investment adviser’s fiduciary duties when outsourcing. The Proposal also includes new recordkeeping requirements and amendments to Form ADV Part 1A, which will require certain census-type information about an investment adviser’s service providers.

The SEC issued the Proposal to seek to address the increased use of outsourcing by investment advisers and the risks that accompany outsourcing of certain types of functions. The SEC expressed concern that outsourcing, in many cases, relates to functions that are critical to the investment adviser’s business. The SEC notes that outsourcing of certain types of functions, without proper oversight by the investment adviser, creates or otherwise increases the risk that clients could be significantly harmed, particularly if the services are not performed or performed in a negligent manner. Therefore, the SEC issued the Proposal, which seeks to provide an oversight framework for investment adviser outsourcing, which the SEC believes will further an adviser’s compliance with its fiduciary responsibilities.

**Why are investment advisers increasingly turning to outsourcing?**

There are many reasons why an investment adviser may turn to outsourcing, particularly for smaller and medium-sized firms. Outsourcing can reduce risk, costs or other burdens on an investment adviser to perform certain functions. Outsourcing can also be used to access

---

<sup>1</sup> Outsourcing by Investment Advisers, 87 Fed. Reg. 68816 (Nov. 16, 2022), available at <https://www.sec.gov/files/rules/proposed/2022/ia-6176.pdf> (the “Proposal”).

<sup>2</sup> Office of Management and Budget, Office of Information and Regulatory Affairs, Agency Rule List – Fall 2023, available at: [https://www.reginfo.gov/public/do/eAgendaMain?operation=OPERATION\\_GET\\_AGENCY\\_RULE\\_LIST&currentPub=true&agencyCode=&showStage=active&agencyCd=3235&csrf\\_token=486A7B8189805E1B9B94CC2326F47332ECFDB6F679CA67A030DB218B3A5203ADA8D6590412C365766E0A82575A97FE5FACB7](https://www.reginfo.gov/public/do/eAgendaMain?operation=OPERATION_GET_AGENCY_RULE_LIST&currentPub=true&agencyCode=&showStage=active&agencyCd=3235&csrf_token=486A7B8189805E1B9B94CC2326F47332ECFDB6F679CA67A030DB218B3A5203ADA8D6590412C365766E0A82575A97FE5FACB7)

specialized expertise to perform complex functions, thereby avoiding the need to invest in significant infrastructure and personnel. For example, an investment adviser may outsource middle and back-office functions to a third-party service provider whose entire business is dedicated to providing these functions. Such a service provider will have the infrastructure, systems, capabilities and expertise necessary to perform these functions and can oftentimes provide turnkey solutions to an investment adviser. Moreover, service providers generally can provide the outsourced services with more rigor, process and oversight than an investment adviser may reasonably be able to do on its own. Outsourced service providers oftentimes can offer their services at scale, which is much more economical for the investment adviser than building out the needed capabilities itself. Outsourcing can therefore result in investment advisory clients paying lower fees while obtaining better quality services.

***Isn't an investment adviser already required to oversee its service providers?***

Investment advisers are required to adopt and implement written policies and procedures that are reasonably designed to prevent violation by the adviser or its supervised persons of the Advisers Act.<sup>3</sup> There isn't a current rule that dictates the manner and methods by which an investment adviser supervises an outsourced service provider. While the Proposed Rule does not require an investment adviser to specifically adopt policies and procedures related to outsourcing, if adopted as proposed, investment advisers would be required to adopt such policies and procedures, where applicable, to prevent a violation of the Advisers Act.

***What does the Proposed Rule require?***

The Proposed Rule would require investment advisers to:

- conduct due diligence prior to engaging a service provider to perform certain services or functions; and
- periodically monitor the performance and reassess the retention of the service provider in accordance with certain due diligence requirements to reasonably determine that it is appropriate to continue to outsource those services or functions to that service provider.

The Proposal would also:

- amend Part 1A of Form ADV to collect census-type information about each of an investment adviser's service providers; and
- amend the Advisers Act books and records rule (Rule 204-2), including a new provision requiring investment advisers that rely on a third-party to make and/or keep books and records requiring the adviser to (i) document the due diligence conducted,

---

<sup>3</sup> See Rule 206(4)-7 under the Advisers Act.

(ii) maintain a copy of any agreements entered into with a service provider regarding covered services, and (iii) maintain records documenting the periodic monitoring of each third-party service provider (collectively, the “Proposed Recordkeeping Amendments”).<sup>4</sup>

### **Who is a Service Provider?**

Under the Proposed Rule, a Service Provider is an entity that performs a Covered Function (defined below) and is not a “supervised person”<sup>5</sup> as defined in the Advisers Act.<sup>6</sup>

### **What is a Covered Function?**

Under the Proposed Rule, there isn’t a finite list of Covered Functions as each potential service provider and the services it will perform would need to be evaluated on a case-by-case basis. Additionally, a service or function may be a covered function for one investment adviser but may not be a covered function for another investment adviser depending on how the service is used.

Under the Proposed Rule, a Covered Function is defined as:

- a function or service that is necessary for the investment adviser to provide its investment advisory services in compliance with the Federal securities laws, and
- that, 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.
- A Covered Function does not include clerical, ministerial, utility, or general office functions or services.<sup>7</sup>

### Proposed Non-Exhaustive List of Covered Functions:

- functions or services that are related to an adviser’s investment decision-making process and portfolio management
- providing investment guidelines (including maintaining restricted trading lists)
- creating and providing models related to investment advice

---

<sup>4</sup> See Proposed Rule 204-2.

<sup>5</sup> See Section 2(a)(25) of the Advisers Act. A supervised person is defined as 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.

<sup>6</sup> Proposed Rule 206(4)-11(b).

<sup>7</sup> *Id.*

- creating and providing custom indexes
- providing investment risk software or services
- providing portfolio management or trading services or software
- providing portfolio accounting services
- providing investment advisory services to an adviser or the adviser's clients
- services to identify which portfolios to include or exclude in a trade
- determining how to allocate a position among portfolios and submitting final orders to a broker
- outsourced compliance functions, such as regulatory filings or any other services to assist an investment adviser with complying with regulatory requirements
- a sub-adviser who manages client investments
- affiliated entities (even those that are otherwise regulated entities (either under the Advisers Act or any other Federal securities law) and those entities that are in a control relationship with the investment adviser.<sup>8</sup>

Proposed Non-Exhaustive List of Activities that Would not be Covered Functions:

- clerical, ministerial, utility, or general office functions or services<sup>9</sup>
- an investment adviser's lease of commercial office space or equipment
- use of public utility companies, utility or facility maintenance services,
- licensing of general software providers of widely commercially available operating systems, word processing systems, spreadsheets or other similar off the shelf software.

These functions are proposed to be excluded because they are not necessary for an investment adviser to provide investment advisory services in compliance with the Federal Securities laws.

Many investment advisers obtain technological solutions that are integral to an adviser's investment decision making processes, portfolio management or other functions that are necessary for the adviser to provide its investment advisory services (e.g., artificial intelligence or software as a service). Importantly, in 2018, the SEC settled an enforcement action against an investment adviser that used models and volatility guidelines from a third-

---

<sup>8</sup> The Proposal notes that risk still exists if an investment adviser outsources to an unaffiliated entity or an affiliated entity. Proposal at 26.

<sup>9</sup> Proposed Rule 206(4)-11(b).

party sub-adviser without first ensuring that the models worked as intended.<sup>10</sup> The Proposal specifically notes that when engaging a third-party technology provider, an investment adviser may not (which also means an adviser may) need to conduct a detailed analysis and review of the underlying computer code but the investment adviser should have a reasonable understanding of how the technology is intended to operate and determine that the technology operates as intended. Depending on the type of technology, there may be other relevant considerations based on the applicable facts and circumstances. Given the move to greater automation and the substantial use of third-party technology solutions, enhancing an investment adviser's due diligence practices may warrant significant consideration.

### ***What is a “Material Negative Impact”?***

The second prong of a Covered Function includes those that, if not performed or performed negligently, would be reasonably likely to cause a *material negative impact* on the investment adviser's clients or on the investment adviser's ability to provide investment advisory services. (*emphasis added*) Under the Proposal, a material negative impact would depend on the particular facts and circumstances, but would include a material financial loss to a client or a material disruption in the investment adviser's operations resulting in the inability to effect investment decisions or to do so accurately.<sup>11</sup> The Proposal suggests that an investment adviser should consider a variety of factors when determining what would be reasonably likely to have a material negative impact on a client, such as the day-to-day operational reliance on the service provider, the existence of a robust internal backup process at the investment adviser, and whether the service provider is making or maintaining critical records.<sup>12</sup>

### ***What are the proposed initial due diligence requirements?***

Under the Proposal, before engaging a Service Provider, an investment adviser would be required to reasonably identify and determine that it would be appropriate to outsource a Covered Function and it would be appropriate to select the Service Provider by:

- Identifying the nature and scope of the Covered Function(s) the Service Provider is proposed to perform;
- Identifying and determining how the investment adviser will mitigate and manage, the potential risks to clients or to the investment adviser's ability to perform its

---

<sup>10</sup> See *In the Matter of Aegon USA Investment Management, LLC, et al*, Investment Advisers Act Rel. No. 4996 (Aug. 27, 2018). In this action, four affiliated adviser entities agreed to pay nearly \$53.3 million in disgorgement, \$8 million in interest, and a \$36.3 million penalty.

<sup>11</sup> Proposal at 24

<sup>12</sup> *Id.*

advisory services resulting from the engagement of that Service Provider to perform the Covered Function;

- Determining that the Service Provider has the competence, capacity, and resources necessary to perform the Covered Function in a timely and effective manner;
- Determining whether the Service Provider has any subcontracting arrangements that would be material to the Service Provider’s performance of the Covered Function, and identifying and determining how the investment adviser will mitigate and manage potential risks to clients or to the investment adviser’s ability to perform its advisory services in light of any such subcontracting arrangement;
- Obtaining reasonable assurance from the Service Provider that it is able to, and will, coordinate with the investment adviser for purposes of the investment adviser’s compliance with Federal securities laws, as applicable to the Covered Function; and
- Obtaining reasonable assurance from the Service Provider that it is able to, and will provide a process for orderly termination of its performance of the Covered Function.<sup>13</sup>

Under the Proposal, investment advisers would have to engage in this due diligence prior to onboarding a new Service Provider or adding services to an existing Service Provider engagement. Due diligence must be reasonably tailored to the function or services that are proposed to be outsourced to the Service Provider. The Proposal states that whether an investment adviser’s due diligence is reasonable would depend on the facts and circumstances of the services and the service provider.<sup>14</sup>

(Collectively, these are referred to herein as the “Proposed Initial Due Diligence Requirements”)

***What are the proposed ongoing due diligence requirements?***

Under the Proposed Rule, an investment adviser must periodically monitor the Service Provider’s performance of any Covered Function and reassess the retention of the Service Provider in accordance with the Proposed Initial Due Diligence requirements.<sup>15</sup> Due diligence activities would be undertaken in a manner and frequency so that the investment adviser can reasonably determine that it is appropriate to continue to outsource the Covered Function and that it remains appropriate to continue to outsource the Covered Function to the Service Provider.<sup>16</sup>

---

<sup>13</sup> Proposed Rule 206(4)-11(a)(1)(i)-(v).

<sup>14</sup> Proposal at 43.

<sup>15</sup> See Proposed Rule 206(4)-11(a)(2).

<sup>16</sup> *Id.*

The Proposal also includes examples of methods of monitoring, including, automated reviews of Service Provider data feeds, periodic meetings with the Service Provider to review service metrics, or contractual obligations to test and approve new systems prior to implementation.<sup>17</sup>

***What initial due diligence records would an investment adviser have to retain under the Proposal?***

The Proposal would amend Rule 204-2 under the Advisers Act (the “Proposed Recordkeeping Amendments”)<sup>18</sup> to require specific records to be maintained in support of the selection and ongoing retention of a Service Provider. In particular, the Proposed Recordkeeping Amendments would require an investment adviser to maintain the following records:

- A list or other record of Covered Functions that the investment adviser has outsourced to a Service Provider, including the name of each Service Provider, a record of the factors, corresponding to each listed function, that led the investment adviser to list it as a Covered Function on Form ADV (see “What are the Proposed Amendments to Form ADV” below);
- Records documenting the due diligence assessment conducted pursuant to Proposed Rule 206(4)-11, including any policies and procedures or other documentation as to how the investment adviser will comply with applicable due diligence requirements related to conflicts of interests;
- A copy of any written agreement, including any amendments, appendices, exhibits, and attachments, entered into with a Service Provider regarding Covered Functions.

The Proposed Recordkeeping Amendments require such books and records to be maintained in an easily accessible place throughout the time period during which the investment adviser has outsourced a Covered Function to a Service Provider and for a period of five years thereafter.<sup>19</sup>

***What records would an investment adviser have to retain relating to Service Provider monitoring?***

The Proposed Recordkeeping Amendments would require an investment adviser to make and retain records documenting the periodic monitoring of a Service Provider of a Covered Function.<sup>20</sup> The Proposal suggests some examples of information that investment advisers should consider, where applicable:

---

<sup>17</sup> Proposal at 68.

<sup>18</sup> Proposed Rule 204-2(a)(24).

<sup>19</sup> See Proposed Rule 204-2(e)(4).

<sup>20</sup> See Proposed Rule 204-2(a)(24)(iv).

- performance reports received from the Service Provider;
- the time, location and summary of findings of any financial, operational or third-party assessments of the Service Provider;
- identification of any new or increased Service Provider risks and a summary of how the investment adviser will mitigate and manage those risks;
- any amendments to written agreements with a Service Provider;
- the adviser's written policies and procedures applicable to monitoring;
- a record of any changes to the nature and scope of the Covered Function the Service Provider is to perform; and
- and a record of any inadequate or failed performance by a Service Provider of a Covered Function and responses from the adviser.<sup>21</sup>

These records would be required to be maintained in an easily accessible place while the investment adviser outsources the Covered Fund and for a period of five years after the investment adviser ceases outsourcing the Covered Function.<sup>22</sup> The SEC noted that these records would help it assess an investment adviser's compliance with the Proposed Rule.

***Do the Proposal apply to outsourced recordkeeping?***

Many advisers outsource certain recordkeeping functions. This includes when an investment adviser retains a Service Provider to maintain and store certain required records created by the Service Provider. Accordingly, an investment adviser may not maintain all of the records that it is required to store based on its business activities. Notwithstanding whether a required record is created by the investment adviser or a Service Provider, the adviser is responsible for complying with the Advisers Act recordkeeping requirements and those required by other Federal securities laws.

Proposed Rule 204-2(l) therefore would require every investment adviser that relies on a third-party to make or keep any required adviser books and records, to develop a comprehensive oversight framework consisting of due diligence and monitoring requirements (similar to oversight of other Service Providers). This oversight framework is designed to protect against loss, alteration, or destruction of an adviser's records and help to ensure that those records are available to the adviser and the SEC staff upon request. The Proposal notes that this specifically includes cloud service providers whereby the investment adviser should have a reasonable understanding of the cloud service and the risks of the service and be able to conclude that it can mitigate and manage those risks. The

---

<sup>21</sup> See Proposal at 69-70.

<sup>22</sup> See Proposed Rule 204-2(e)(4).

Proposal suggests that an investment adviser could review the following, during its diligence of a cloud service provider:

- Comparative cloud-based recordkeeping services, including their respective parameters, benefits, and risks;
- The cloud service provider's capability and experience with making and/or keeping records required under the recordkeeping rule;
- The cloud service's compliance and operational policies and procedures for the protection of data, and its policies and procedures addressing the maintenance and oversight of the data;
- The cloud service's prevention and detection of, and response to, cybersecurity threats; and
- The experience or lack thereof of other similarly situated advisers that have previously engaged the cloud service and any risks identified in those experiences or lack thereof.<sup>23</sup>

Once a third-party recordkeeper is retained, an adviser would be required to monitor the third-party's performance of the recordkeeping function and reassess the retention of the third-party similar to the requirements for other Service Providers. Methods for monitoring and the frequency can vary based on the recordkeeping services provided (e.g., cloud vs. physical storage).

Additionally, an investment adviser would be required to obtain reasonable assurances from the Service Provider that:

- it will adopt and implement internal processes and/or systems for making and/or keeping records on behalf of the investment adviser that meet all of the requirements of the recordkeeping rule;
- when making and/or keeping records on behalf of the adviser, the Service Provider will, in practice, actually make and/or keep records in a manner that will meet all of the requirements of the recordkeeping rule as applicable to the investment adviser;
- the Service Provider will allow the investment adviser and SEC staff to access the records easily through computers or systems during the required retention period of the recordkeeping rule; and
- arrangements will be made to ensure the continued availability of records that will meet all of the requirements of the recordkeeping rule as applicable to the

---

<sup>23</sup> Proposal at 83-84.

investment adviser in the event that the Service Provider ceases operations or the relationship with the investment adviser is terminated.<sup>24</sup>

### ***What are the Proposed Amendments to Form ADV?***

The Proposal includes amendments to Form ADV Part 1A, which would require advisers to:

- identify service providers that perform Covered Functions;
- provide the location of the office principally responsible for the Covered Functions;
- provide the date the Service Provider was first engaged to provide Covered Functions; and
- state whether they are a related person<sup>25</sup> of the investment adviser.

The Proposal would also require an investment adviser to categorize and report those Covered Functions or services provided by each Service Provider from predetermined categories of Covered Functions, which are proposed to include:

- |   |   |
|---|---|
| ▪ Adviser / Sub-Adviser                         | ▪ Pricing   |
| ▪ Client Services                               | ▪ Reconciliation  |
| ▪ Cybersecurity                                 | ▪ Regulatory Compliance                                 |
| ▪ Investment Guideline / Restriction Compliance | ▪ Portfolio Management (excluding Adviser / Subadviser) |
| ▪ Investment Risk                               | ▪ Trade Communication and Allocation                    |
| ▪ Trading Desk                                  | ▪ Valuation   |
| ▪ Portfolio Accounting                          | ▪ Other   |

If a Covered Function does not fit in a pre-defined category, the investment adviser may use the “Other” category. This information would be publicly available.

### **Compliance Consideration and Recommendations**

While the Proposal has not been finalized, compliance officers should, as a best practice, review their existing diligence practices. Below are some examples of questions you may wish to consider when conducting such a review. Additionally, any evaluation of your

---

<sup>24</sup> See Proposed Rule 204-2(l)(2)(i)-(iv).

<sup>25</sup> A related person is defined in the Glossary of Terms to Form ADV as any advisory affiliate and any person that is under common control with the adviser.

diligence practices should be based on the nature of the investment adviser's business, the specific relationship and risks associated with the applicable Service Provider and the functions or services performed.

- Does your firm have a due diligence process? Are there any guidelines regarding when due diligence is necessary and who is responsible for it? What does the diligence process entail? Are these practices appropriate to evaluate the service provider and the services to be provided?
- Are the correct people/teams at the investment adviser evaluating each Service Provider? Is due diligence scaled based on the services to be provided and risks presented to investment adviser and its clients? How are Service Provider risks evaluated and mitigated?
- What information is obtained and reviewed when a new vendor is onboarded (in addition to the sales materials, slide decks, contracts and service levels, if any)? Are there standards of information that must always be obtained from the service provider and reviewed, e.g., as applicable, financial information, management teams, compliance and regulatory background, business continuity plan, information security program, technological interfacing, third-party evaluations, such as a SOC1/SOC2, etc.
  - All diligence materials must be reviewed. It is important to go through the materials in detail to look for any red flags or concerns about the service provider and its offering.
- What kind of ongoing monitoring is performed on service providers? Do you obtain and review updated diligence materials, do onsite visits, or use other methods to re-evaluate the proposed services? Has the scope of services evolved? Does the vendor have any material updates to its business, management, personnel, regulatory history or manner in which it is providing its services? These analyses must be tailored to the facts and circumstances based on the nature of the relationship and services provided.
  - Review your documentation around your diligence processes. For example, if an on-site diligence visit occurs, be sure and document that along with any information learned and reviewed. Do you keep thorough records of diligence activities?
  - If you become aware of an issue with a service provider (e.g., a critical outage that affects the service provider's ability to provide its services or a regulatory enforcement action) it is very important to follow-up promptly on these matters to understand (i) the nature of the issue, (ii) the steps being taken to promptly correct the issue, (iii) any impact on the services that were provided

to the investment adviser or its clients, (iv) what the vendor is doing to correct the matter, and (v) what will be done to ensure that the issue (or any similar issues) does not recur. Service providers do not always proactively reach out on these matters, so it is important to be vigilant in understanding the implications of issues when they arise.

- Do you need to review your existing, or develop standard, contract clauses that you require when entering into outsourcing agreements? For example, you may seek to have a contractual right to conduct onsite due diligence visits, or you may want the service provider to be obligated to provide required records it is maintaining within a certain period of time. You may also want to consider requiring a service provider to proactively inform the investment adviser of certain events (e.g., loss of any applicable registration that is required to perform the services, claims on insurance, regulatory matters, key man departures, material errors, data security or BCP events etc.). These are just examples. Contractual provisions should be considered in light of the nature of the arrangement between the adviser and the service provider.
- Recordkeeping
  - How is recordkeeping currently addressed with an adviser's service providers? Do the service providers have an obligation to maintain required records for the adviser? If so, does the service provider have appropriate recordkeeping policies and procedures for any records it maintains on the adviser's behalf?
  - Have you ensured that your service providers have appropriate backup systems for adviser records to ensure that they are not lost, altered or deleted?
  - Have you conducted any testing on whether the service provide can produce any adviser required records in a timely fashion and in a manner that is acceptable for your needs?
  - Have you listed all service providers that maintain required records in Form ADV Part 1A, Item 1.L?

**FIRM QUESTIONNAIRE**

Company Name

Company Address

Company Website

Year Founded

Primary Relationship Manager

Primary Compliance Contact Person

**ORGANIZATIONAL STRUCTURE & OWNERSHIP**

Please provide a brief description of your organizational structure.

Please describe the ownership structure of your firm.

Please provide a high-level organizational chart identifying reporting lines and titles.

Has your firm's ownership structure significantly changed in the past year?

Have there been any changes within the past year in control of your Firm?

Is any change of control of your Firm currently underway or expected to occur in the next year?

Please identify any firms you have merged with or acquired in the past five years.

**SERVICES PROVIDED**

Please provide an overview of the products and services provided by your Firm.

Please describe the controls your Firm has in place to monitor for potential conflicts of interest based on the variety of products and services you provide.

If applicable, please provide a brief description of the portfolio valuation methods utilized.

Please list any client complaints received over the past three (3) years, including a brief description of each complaint and the corrective step(s) taken, if any.

**EMPLOYEES**

Please provide biographies for all principals/owners of your firm.

Please provide a list of key compliance personnel with a brief biography and description of each person's position within the firm's organizational structure.

Does your firm conduct criminal background checks on personnel prior to hiring?

**AUDIT & REGULATORY OVERSIGHT**

Are the Firm's financial statements audited by an independent audit firm?

Please provide the name of the independent audit firm.

Please provide a copy of the most recent report.

Has the Firm had any external audit or evaluation of its internal controls performed by an independent third-party audit firm (e.g., SAS 70 / SSAE 16)?

Please provide a copy of the most recent opinion.

Is your Firm subject to regulatory oversight?

Please provide the following details for each regulated/registered entity: registrant name, regulatory body, effective date of registration, registration ID#, type of registration.

Has your Firm or any of its affiliates been subject to examination by any regulatory or government body (e.g., the SEC, FINRA, CFTC, UK FCA, etc.) in the past two years?

Please provide the following details for each examination: regulator(s) involved, the date(s), and a summary of the outcome.

Has the Firm had any violations of the Bank Secrecy Act or USA PATRIOT Act concerning the failure of the Firm to: detect money laundering, report suspicious activity, reasonably with OFAC Regulations?

Please describe these violations.

#### **LITIGATION**

Has the Firm, its affiliates, or any of their respective officers, principals or employees, over the last five (5) years, been involved in any securities litigation, bankruptcy or other legal subpoena from any regulating body)?

Please provide a detailed explanation.

Are you aware of any threatened litigation against your Firm?

Please describe.

#### **CODE OF ETHICS & PERSONAL TRADING**

Does your Firm maintain a Code of Ethics and/or a personal trading policy?

Please provide the most recent copy.

Does your Firm obtain periodic certifications from Firm personnel with respect to your Code of Ethics (e.g., annual certifications)?

Please describe the process and controls in place with respect to these certifications.

Does your Firm monitor the personal trading activity of employees who have access to confidential client information?

Please describe the trade monitoring process.

Are employees required to pre-clear personal securities transactions?

Please describe your process for reviewing personal trade requests.

During the past two (2) years, have there been any breaches of your Firm's Code of Ethics?

Please provide a brief description of the breaches and their resolution.

Does your Firm maintain a compliance training program/continuing education for its employees?

How often do employees complete this training?

#### **POLICIES AND PROCEDURES**

Does your Firm have written compliance policies?

Please provide a copy of the most recent policies.

Please describe your Firm's compliance program and how compliance policies and procedures are developed and maintained.

When was the last date that your Firm tested its compliance policies and procedures?

Describe how your firm determines the materiality of compliance violations as well as the process for identifying and reporting violations of compliance policies and procedures into

#### **MNPI & REGULATION S-P**

Please describe how MNPI is handled within your Firm.

Are employees, temporary workers and subcontractors with access to client data bound by confidentiality agreements (whether separately or incorporated into other Firm documents)?

Please describe the internal controls that exist to ensure adherence to your Firm's policies concerning confidential treatment of client information.

Describe your Firm's security measures with respect to systems access.

Please provide your Firm's current privacy policy.

During the past twelve months, have there been any violations of any policies related to the handling, disclosure or use of MNPI? If yes, please describe.

During the past twelve months, have there been any violations of the Graham-Leach-Bliley Act / Regulation S-P (or violations of policies related to those statutes or regulations) concerning sharing of non-public, personal information? If yes, please describe.

#### **EMAIL SECURITY**

Do you pre-screen e-mails for potentially malicious attachments and links?

Do you provide a quarantine service to your users?

Do you have the capability to automatically detonate and evaluate attachments in a sandbox to determine if malicious prior to delivery to the end-user?

Do you strictly enforce Sender Policy Framework (SPF) on incoming e-mails?

How often is phishing training conducted to all staff (e.g. monthly, quarterly, annually)?

Can your users access e-mail through a web app on a non-corporate device?

If Yes: do you enforce Multi-Factor Authentication (MFA)?

Do you use Office 365 in your organization?

If Yes: Do you use the o365 Advanced Threat Protection add-on?

#### **INTERNAL SECURITY**

Do you use an endpoint protection (EPP) product across your enterprise?

Do you use an endpoint detection and response (EDR) product across your enterprise?

Do you use MFA to protect privileged user accounts?

Is a hardened baseline configuration materially rolled out across servers, laptops, desktops and managed mobile devices?

What % of the enterprise is covered by your scheduled vulnerability scans?

In what time frame do you install critical and high severity patches across your enterprise?

If you have any end of life or end of support software, is it segregated from the rest of the network?

Have you configured host-based and network firewalls to disallow inbound connections by default?

Do you use a protective DNS service (e.g. Quad9, OpenDNS or the public sector PDNS)?

Do you use an endpoint application isolation and containment technology?

Do your users have local admin rights on their laptop / desktop?

Can users run MS Office Macro enabled documents on their system by default?

Do you provide your users with a password manager software?

Do you manage privileged accounts using tooling? E.g. CyberArk

Do you have a security operations center established, either in-house or outsourced?

#### **BACK-UP AND RECOVERY POLICIES**

Are your backups encrypted?

Are your backups kept separate from your network ('offline'), or in a cloud service designed for this purpose?

Do you use a Cloud syncing service (e.g. Dropbox, OneDrive, SharePoint, Google Drive) for backups?

Have you tested the successful restoration and recovery of key server configurations and data from backups in the last 6 months?

Are you able to test the integrity of back-ups prior to restoration to be confident it is free from malware?

#### **RECORDKEEPING**

Please describe the procedures in place that ensure your Firm is meeting its recordkeeping obligations.

**OTHER RANSOMWARE**

Please describe any additional steps your organization takes to detect and prevent ransomware attacks (e.g. segmentation of your network, additional software tools, external sec

# 2024 / Investment Adviser Compliance Conference

MARCH 6-8 / WASHINGTON, DC

EFFECTIVE STRATEGIES & BEST PRACTICES

## Outsourcing Vendor Due Diligence for Larger Firms

**Nevis Bregasi** / MFS Investment Management

**Drew Bowden** / TCW

**Stephen Johnson** / Charles Schwab & Co. Inc.

**Michael Koffler** / Eversheds Sutherland (US) LLP (MODERATOR)

1

IAA 2024 / Investment Adviser  
Compliance Conference

EFFECTIVE STRATEGIES  
& BEST PRACTICES

## Overview

### Challenges with the Proposal

- Overview
- Comments
  - Lack of coherent explanation for need for new regime
  - SEC bias against outsourcing vs. reality
  - Scope of Covered Function definition – too wide/vague
  - Additional liability + an anti-fraud rule + Monday morning quarterbacking
  - In practice, a strict liability standard

2



## Overview

### Challenges with the Proposal

- Comments
  - Books and records provisions – unworkable contract requirements
  - Merit based reviews by staff - not just process focused
  - Costs (will cause small advisers to go out of business)
  - Increased friction in outsourcing functions
  - Economic changes to market for outsourcing
  - Rigidity of the rule – forcing a Hobbesian choice
  - Shifts liability for vendors' failures onto advisers

3



## Audience Question

Where are you on the “Rage-o-meter”?



- ④ Worst SEC rule proposal ever ... an outrage.
- ③ Impractical. Expensive. Overbroad. A cure in search of a problem ... but we will endure under protest.
- ② Another day. Another challenging rule. Keeps me employed.
- ① A yawn. No biggie. We already do all this.

4



**2024** Investment Adviser  
Compliance Conference

**EFFECTIVE STRATEGIES  
& BEST PRACTICES**



## Audience Question

Biggest pain point/concern

- Unworkable contract requirements
- Conflicts with business objective to outsource more
- Costs to implement (initial and ongoing diligence; recordkeeping)
- Increase in risks associated with outsourcing

5



**2024** Investment Adviser  
Compliance Conference

**EFFECTIVE STRATEGIES  
& BEST PRACTICES**



## Audience Question

If you could change one thing, it would be:

- Convert to a principles and risk-based approach.
- Clarify and narrow definition of a “covered function.”
- Exclude certain categories of “service providers,” including affiliates, registered entities, providers to registered funds, and custodians.

6



## Due Diligence Considerations

### Things to think about

- Selection criteria – the end of a risk-based approach?
- Need to make governance changes? Elevate to enterprise risk management?
- What is treated as outsourcing (e.g., purchasing a platform/insourcing)?
- Existing contract language – is it enough?
- Expertise and composition of due diligence teams

7



## Due Diligence Considerations

### Things to think about

- Initial monitoring
- Ongoing monitoring
- Pulling the plug on vendors/making changes
- Documentation
- Treatment of affiliates

8



## What else will change

### Considerations

- Costs and number of vendors utilized
- Disclosure
- Liability – advisers are caught between clients and vendors
  - Implications for indemnification, reps and warranties and other contractual provisions
  - Certifications, information requests

9



## Liability “Catch 22”

- Is an adviser liable to clients if it outsources a covered function and performs sufficient diligence/oversight?
  - An adviser remains liable for its obligations, including under the Advisers Act, Federal securities laws and any contract entered into with clients, even if it outsources functions. In addition, an adviser cannot waive its fiduciary duty.
  - In order to comply with its legal obligations when outsourcing a function, the adviser should confirm the service provider is able to perform the applicable function timely and effectively to the same standards applicable to the adviser.

10



## Liability “Catch 22”

- Is an adviser liable to a client if the adviser outsources a covered function and performs a sufficient level of diligence and oversight?
  - If an adviser allocates client portfolios to a sub-adviser, the adviser is still responsible for ensuring the services rendered are consistent with the adviser’s representation of the services to clients.
  - When an adviser outsources a covered function, should the rule include an express provision that prohibits an adviser from disclaiming liability when it is not performing a covered function itself

11



## A Preview of Enforcement?

- CCM Case (IA-5943), 1/11/22
  - “CCM and its IARs will be liable only for their own acts of gross negligence or willful misconduct. CCM and its IARs will not be liable for any act or omission, or the failure or inability to perform any obligation, of any broker, dealer, investment adviser, sub-custodian or other agent, including affiliates, whom CCM selected with reasonable care.”
  - “CCM’s revised advisory agreement purports to relieve CCM from liability for conduct as to which the client has a non-waivable cause of action against CCM . . . The hedge clause is inconsistent with an adviser’s fiduciary duty . . . Moreover, the statement that “CCM and its IARs will be liable only for their own acts of gross negligence or willful misconduct” is an inaccurate statement of the liability standards . . . Accordingly, both the original and the revised hedge clause violate Section 206(2) . . .”

12



## 80% of \$1B+ AUM Firms Outsource Technology Systems/Data Management

Outsourcing of Technology Systems-Planned to Outsource in 2023	All Firms	Over \$1B
Full outsourcing: Computer hardware infrastructure is hosted offsite and maintained by a third-party provider, and portfolio accounting day-to-day data management processes are managed by a third-party provider	23%	19%
Operational and data management outsourcing: Portfolio accounting day-to-day management processes are managed by a third-party provider	28%	30%
Infrastructure outsourcing: Computer hardware infrastructure is hosted offsite and maintained by a third-party provider	28%	33%
No outsourcing: Computer hardware infrastructure and portfolio accounting day-to-day data management processes are maintained entirely in-house	21%	18%
<b>Total</b>	<b>100%</b>	<b>100%</b>

Results for all firms with \$25 million or more in AUM and firms with \$1 billion or more in AUM. Past performance is not an indicator of future results. 2023 RIA Benchmarking Study from Charles Schwab, fielded January to March 2023. Study contains self-reported data from 1,300 firms. Participant firms represent various sizes and business models categorized into peer groups by AUM.

13



## Most firms Don't Plan to Outsource Key areas of Investment Management

In-House, No Outsourcing Planned	All Firms	Under \$250M	Over \$1B	Diff Under \$250M and Over \$1B
Investment research – Traditional	71%	72%	75%	3%
Investment research – Alternatives	69%	74%	63%	-10%
Market commentary for clients	70%	65%	79%	14%
Model portfolios	82%	78%	87%	9%
Tax-loss harvesting	84%	82%	81%	-1%
Portfolio monitoring	88%	85%	90%	5%
Trading and rebalancing	87%	83%	91%	7%
Chief Investment Officer role/responsibilities	90%	87%	94%	7%

Results for all firms with \$25 million or more in AUM, firms with under \$250 million in AUM, and firms with \$1 billion or more in AUM. Past performance is not an indicator of future results. 2023 RIA Benchmarking Study from Charles Schwab, fielded January to March 2023. Study contains self-reported data from 1,300 firms. Participant firms represent various sizes and business models categorized into peer groups by AUM.

14



**2024** Investment Adviser  
Compliance Conference

**EFFECTIVE STRATEGIES  
& BEST PRACTICES**

## Most firms are handling Investment Management Functions In-House

Firms Outsourcing Approach for Investment Management Areas	Full Outsourcing	Partial Outsourcing	In-House, but Considering Outsourcing	In-House, No Outsourcing Planned
Investment research-Traditional	5%	21%	4%	71%
Investment research-Alternatives	7%	18%	6%	69%
Market commentary for clients	5%	18%	6%	70%
Model portfolios	3%	10%	5%	82%
Tax-loss harvesting	2%	9%	5%	84%
Portfolio monitoring	2%	6%	4%	88%
Trading and rebalancing	2%	6%	5%	87%
CIO role/responsibilities	2%	5%	3%	90%

Results for all firms with \$25 million or more in AUM. Values may not sum to 100% due to rounding. Past performance is not an indicator of future results. 2023 RIA Benchmarking Study from Charles Schwab, fielded January to March 2023. Study contains self-reported data from 1,300 firms. Participant firms represent various sizes and business models categorized into peer groups by AUM.

15

# 2024 Investment Adviser Compliance Conference

MARCH 6-8 / WASHINGTON, DC

**EFFECTIVE STRATEGIES  
& BEST PRACTICES**



16

**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<sup>1</sup> 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")<sup>2</sup> 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'

---

<sup>1</sup> The Investment Advisers Act of 1940, as amended.

<sup>2</sup> 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.<sup>3</sup> 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.

---

<sup>3</sup> 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<sup>4</sup>**

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.<sup>5</sup> 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.<sup>6</sup>

#### **A. Policies and Procedures**

---

<sup>4</sup> See Compliance Programs of Investment Companies and Investment Advisers, 68 Fed. Reg. 74714 (Dec. 24, 2003) (“Adopting Release”).

<sup>5</sup> 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.

<sup>6</sup> 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.<sup>7</sup>
- Policies and procedures should employ, among other methods of detection, compliance tests that analyze information over time in order to identify unusual patterns.<sup>8</sup>
- Prevention should be a key objective of a firm’s compliance policies and procedures.<sup>9</sup>

## B. Annual Review

- Each adviser must review its policies and procedures annually to determine their adequacy and the effectiveness of their implementation.<sup>10</sup>
- 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.<sup>11</sup>
- Advisers should consider the need for interim review in response to significant compliance events, changes in business arrangements, and regulatory developments.<sup>12</sup>

**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<sup>13</sup> requires an adviser registered with the Commission to periodically determine whether it offers or maintains “covered accounts.”<sup>14</sup> As a part of this determination, the adviser must conduct a risk assessment and take into consideration: (1) methods it provides to open

---

<sup>7</sup> Id.

<sup>8</sup> Id. at n. 15.

<sup>9</sup> Id. at n. 16.

<sup>10</sup> Id. at 74720.

<sup>11</sup> Id.

<sup>12</sup> Id.

<sup>13</sup> 17 C.F.R. 248.201et seq.

<sup>14</sup>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)<sup>15</sup>

- 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)<sup>16</sup>

- 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

---

<sup>15</sup> 2024 Examination Priorities Report located at <https://www.sec.gov/files/2024-exam-priorities.pdf>.

<sup>16</sup> [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)<sup>17</sup>**

- 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

---

<sup>17</sup> <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)<sup>18</sup>**

- 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

---

<sup>18</sup> <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)<sup>19</sup>**

- 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)<sup>20</sup>**

---

<sup>19</sup> <https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20Network%20Storage.pdf>.

<sup>20</sup> <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)<sup>21</sup>

- **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)<sup>22</sup>

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

<sup>22</sup> <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)<sup>23</sup>

- **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)

---

<sup>23</sup> 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)<sup>24</sup>**

- 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

---

<sup>24</sup> <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)<sup>25</sup>**

- 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.

---

<sup>25</sup> <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<sup>26</sup>**

- 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<sup>27</sup>**

- 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<sup>28</sup>**

---

<sup>26</sup> FINRA Regulatory Notice 21-29 located at <https://www.finra.org/sites/default/files/2021-08/Regulatory-Notice-21-29.pdf>.

<sup>27</sup> Id.

<sup>28</sup> 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



## **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

# 2024 / Investment Adviser Compliance Conference

MARCH 6-8 / WASHINGTON, DC

EFFECTIVE STRATEGIES & BEST PRACTICES

## Safeguarding/Custody

David Bartels / Dechert LLP

Samuel Thomas / SEC Division of Investment Management

Zephram Yowell / PIMCO

Laura Grossman / Investment Adviser Association (MODERATOR)

1



2024 / Investment Adviser  
Compliance Conference

EFFECTIVE STRATEGIES  
& BEST PRACTICES

## Current Challenges

Enforcement cases

Examinations

2



## **Proposed Safeguarding Rule**

### Expanded Scope of the Rule

- Expansion to “assets” from “funds and securities”
- Discretionary trading authority triggers the rule

3



## **Proposed Safeguarding Rule (continued)**

### Qualified Custodian Requirements

- Possession and Control Requirement
- QC contract requirements and reasonable assurances

4

**IAA** 2024 Investment Adviser Compliance Conference **EFFECTIVE STRATEGIES & BEST PRACTICES**



## **Proposed Safeguarding Rule (continued)**

### Exceptions to QC Requirements

- Privately Offered Securities/Physical Assets
- Discretionary Trading authority over DVP assets

5

**IAA** 2024 Investment Adviser Compliance Conference **EFFECTIVE STRATEGIES & BEST PRACTICES**



## **Proposed Safeguarding Rule (continued)**

### Miscellaneous

- Recordkeeping
- ADV updates

6



## Proposed Safeguarding Rule

Industry perspectives

- Institutional
- Retail
- Multiple business lines
- Smaller advisers

7



## Takeaways

Rulemaking status

Issues to be determined

Potential impacts

8



ONPOINT / A legal update from Dechert's Financial Services Group

# Safeguarding Client Assets: SEC Proposes Overhaul of Adviser Custody Rule

Authored by David P. Bartels, Brenden P. Carroll, Mark D. Perlow, Paul  
S. Stevens Jr., Phillip Garber, Michael Murphy, and Ashley N. Rodriguez

March 2023

Dechert  
LLP



# Safeguarding Client Assets: SEC Proposes Overhaul of Adviser Custody Rule

March 2023 / Authored by David P. Bartels, Brenden P. Carroll, Mark D. Perlow, Paul S. Stevens Jr., Phillip Garber, Michael Murphy, and Ashley N. Rodriguez

The U.S. Securities and Exchange Commission, by a vote of four-to-one, proposed a major overhaul of the investment adviser custody rule on February 15, 2023. The proposal would amend and redesignate Rule 206(4)-2 under the Investment Advisers Act of 1940 (Custody Rule), as new Rule 223-1 under Section 223 of the Advisers Act (Proposed Rule).<sup>1</sup>

The Proposed Rule seeks to restructure dramatically the way that qualified custodians provide custody services, as well as the nature and scope of advisers' responsibilities with respect to custody (reflected in the rebranding of the rule as "Safeguarding"). It would attempt to regulate custodians indirectly through a set of required undertakings to advisers and would require burdensome and intrusive new verification audits for private transactions. In these and many other ways, if adopted the Proposed Rule would have a significant impact on advisers, advisory clients, investors and the market for custody services. For example, the Proposed Rule would:

- Disrupt existing custodial practices and arrangements by requiring advisers to enter into written agreements directly with custodians and, under certain circumstances, independent public accountants. Advisers would also need to obtain written assurances from custodians on certain matters (e.g., that the custodian will indemnify the client for losses in the event of the custodian's own negligence, recklessness, or willful misconduct); many existing custody agreements are not consistent with these required assurances, and it is open to doubt whether custodians will provide these assurances to all advisers, or perhaps only to their largest clients.
- Expand the universe of advisers that are deemed to have "custody" by expanding the definition of custody to include discretionary investment authority. This expanded definition is likely to impact collateralized loan obligation (CLO) managers (among others) and significantly increase the number of advisers that are deemed to have custody.
- Expand the type of assets that are subject to the rule to include digital/crypto assets and physical assets, including real estate. The SEC is here trying to reorganize the back-office operations of the digital asset industry to conform with those of traditional asset classes.
- Impose new conditions for serving as a "qualified custodian," including potentially unrealistic conditions for foreign financial institutions.

The Proposed Rule would also increase reporting and recordkeeping requirements (similar to more recent SEC proposals). The Proposed Rule could be costly for the industry and its participants, and it could stifle competition and innovation by driving smaller advisers and custodians away from non-traditional assets or out of business. In justifying the Proposed Rule, the SEC stated that "the evolution of financial products and services...has led to

---

<sup>1</sup> [Safeguarding Advisory Client Assets](#), Release No. IA-6240 (Feb. 15, 2023) (Release). The three Democratic Commissioners, Chairman Gary Gensler, Commissioner Caroline A. Crenshaw and Commissioner Jaime Lizárraga, and one Republican Commissioner, Commissioner Mark T. Uyeda, voted to propose the Proposed Rule, whereas one Republican Commissioner, Commissioner Hester M. Peirce, dissented. At times, this *Dechert OnPoint* tracks the Release without the use of quotation marks. Terms not defined in this *Dechert OnPoint* have the meaning assigned to them in the Release.

new entrants and new services in the custodial marketplace, including newly launched state-chartered trust companies....” The SEC also asserted that the SEC staff has “observed a general reduction in the level of protections offered by custodians.”

This *OnPoint* summarizes the Proposed Rule and discusses some of the wider implications. Advisers, custodians and investors should consider submitting comment letters to the SEC to address aspects of the proposal by May 8, 2023.

## Overview of Proposed Rule

If adopted, among other matters, the Proposed Rule would:

- *Expand the Scope of Assets Covered Under the Rule:* expand the scope of assets covered by the rule to include all client “funds, securities, or other positions held in a client’s account” for which an adviser has custody. Notably, the rule would apply to crypto assets and physical assets of which an adviser has custody.
- *Expand the Scope of Activity Constituting Custody:* expand the definition of custody to include any discretionary authority to trade for a client’s account.
- *Create New Requirements for Arrangements with Custodians:* require advisers with custody of client assets to enter into written agreements with, and obtain “reasonable assurances” from, each qualified custodian on certain matters.
- *Impose New Conditions on the Use of Foreign Financial Institutions:* impose new requirements on foreign financial institutions (FFIs) to meet the definition of “qualified custodian,” including a requirement that FFIs be subject to anti-money laundering requirements similar to those imposed on U.S. institutions.
- *Impose New Requirements on Privately Offered Securities and Physical Assets:* impose new requirements on privately offered securities and physical assets that cannot be held at a qualified custodian, including new verification requirements.
- *Segregation Requirements:* subject client assets to new segregation requirements, including a requirement that client assets be segregated from the assets of the adviser and its related persons.
- *Audit Provision:* expand the audit provision exception to cover any entity that is subject to an annual audit, codify or expand timelines for distribution of audited financials for funds of funds (and funds of funds), codify existing staff positions on the use of non-U.S. auditing standards for preparation of non-U.S. entity financials, and require a written agreement with the independent public accountant that would require the accountant to notify the SEC under certain circumstances.
- *Recordkeeping Amendments:* amend Rule 204-2 under the Advisers Act (Recordkeeping Rule) to impose new recordkeeping requirements related to the Proposed Rule.
- *Form ADV Amendments:* amend Form ADV to align reporting obligations with the Proposed Rule and increase the custody-related data available to the SEC.

Each of these changes in the Proposed Rule is discussed in more detail below.

## Proposed Rule

### Expanded Scope of Assets Covered Under the Proposed Rule

The current Custody Rule applies to any adviser registered or required to be registered with the SEC that has custody of a client's "funds or securities." The Proposed Rule would apply to any adviser with custody of a client's "assets," which it defines as "funds, securities, or other positions held in a client's account." The SEC pointed to Section 223<sup>2</sup> of the Advisers Act as legal authority for this expansion. Section 223 was enacted in 2010 and provides that investment advisers "shall take such steps to safeguard client assets" as the SEC may prescribe by rule.<sup>3</sup>

The Proposed Rule does not define "other positions," but the Release states the term "other positions" encompasses all investments, even if such investments are neither funds nor securities. The Release states that "other positions" includes holdings "that may not necessarily be recorded on a balance sheet as an asset for accounting purposes, including, for example, short positions and written options." The Release also states that investments that are accounted "in the liabilities column of a balance sheet or represented as a financial obligation of the client[,] including negative cash," would be within the scope of the Proposed Rule.

The Release specifies or indicates that the following investment positions would be included in the scope of the Proposed Rule: all digital/crypto assets, including those that are not funds or securities;<sup>4</sup> assets traded on foreign exchanges; physical assets, including real estate, precious metals, physical commodities (including corn, oil, wheat and other grains, lumber and gold bullion and other precious metals), valuable papers, rare coins, jewelry, antiques and artwork; short positions; written options; futures; financial liabilities or obligations; financial contracts held for investment purposes; collateral posted in connection with swap contracts; physical evidence of non-physical assets that can be used to transfer beneficial ownership, such as physical coupon bonds, physical security certificates, stock certificates and other physical security certificates, private keys, and bearer or registered instruments; physical evidence of physical assets that can be used to transfer physical ownership, such as warehouse receipts for commodities and deeds or other similar indicia of ownership of real estate; and "asset types that develop in the future regardless of their status as funds or securities."

### Expanded Scope of Activity Covered Under the Proposed Rule

The Proposed Rule would add to the Custody Rule's definition of custody any "discretionary authority" over client assets. The Proposed Rule defines "discretionary authority" as "authority to decide which assets to purchase and sell for [a] client." The Proposed Rule would also change the definition of custody from any arrangement under which the adviser is authorized or permitted to "withdraw client funds or securities" to any arrangement under which the adviser is authorized or permitted to "withdraw or transfer beneficial ownership of client assets" upon the adviser's instruction. If adopted, these changes would significantly increase the universe of advisers subject to the Custody Rule. According to estimates in the Release, approximately 93 percent of advisers would be deemed to have custody if the Proposed Rule is adopted, up from approximately 57 percent currently.

---

<sup>2</sup> Although the rule has been designated under Section 223 of the Adviser Act, the SEC indicated that it would still be able to pursue enforcement actions against advisers for failing to safeguard assets under Section 206(4), the statutory authority for the Custody Rule and one of the Advisers Act's antifraud provisions.

<sup>3</sup> Congress adopted Section 223 in response to multiple high-profile instances of misappropriation by advisers of client assets.

<sup>4</sup> The Release notes, however, that "most crypto assets are likely to be funds or crypto asset securities covered by the current [Custody Rule]."

In the 2003 and 2009 amendments to the Custody Rule, the SEC recognized that “authorized trading” was not within the definition of “custody.” In reliance on that position, many types of funds and accounts have been structured in such a manner that the adviser to those accounts is not deemed to have custody of client assets under the current Custody Rule. Under the Proposed Rule, the elimination of the authorized trading exception would result in a significant number of advisers becoming subject to the rule’s requirements for the first time.

For example, CLOs have typically been structured in a manner such that the collateral manager to that CLO would not be deemed to have custody over CLO assets under the current Custody Rule. However, collateral management agreements typically provide a collateral manager with authorities that could meet the “discretionary authority” test of the Proposed Rule. Accordingly, collateral managers may be deemed to have “custody” under the Proposed Rule and become subject to the rule’s requirements for the first time, including, for example, the surprise exam requirement. An exception from the surprise exam requirement may be available for CLOs that undergo an annual audit and satisfy the requirements of the audit exception. However, the expense of a surprise exam, or compliance with the audit exception, is not typically contemplated in CLO governing documents.

The Proposed Rule would retain the current exception for registered investment companies; however, certain aspects of the Proposed Rule may have indirect effects on trading and settlement of investments by registered investment companies, for example, if market practices that arise from the indirect requirements placed upon qualified custodians by an adopted rule become industry standards.

## **Qualified Custodian Requirements**

The Proposed Rule would generally preserve the types of financial institutions deemed to meet the definition of “qualified custodian” under the Custody Rule. However, the Proposed Rule would impose additional requirements on banks and savings associations to protect investors in the event of bank insolvency or failure and would also impose additional requirements on FFIs.

### ***New Segregation Requirements for Bank Custodians***

The Proposed Rule would amend the definition of a “qualified custodian” to require a bank or savings association to hold client assets in an account that is designed to protect such assets from the bank or savings association’s creditors in the event of insolvency or failure. The SEC suggested in the Release that an account would be so designed if the client assets were clearly segregated from the bank’s assets and easily identifiable as the client’s assets. In addition, the SEC noted in the Release that the account terms should clarify that the relationship between the client and the qualified custodian protects the client assets, in the event of an insolvency or failure, from the bank or saving association’s creditors. The SEC views this requirement as being aligned with similar protections required for broker-dealers, futures commission merchants and FFIs serving as qualified custodians.

### ***New Requirements for Foreign Financial Institutions***

The Proposed Rule would impose seven new requirements on FFIs to meet the definition of “qualified custodian.” The SEC noted that the new requirements would align the protections required of an FFI with those of a domestic qualified custodian and cited recent events in crypto markets as the impetus for requiring enhanced custodial safeguards of client assets held outside the United States. For an FFI to be a qualified custodian under the Proposed Rule, it would need to be:

- Incorporated or organized under the laws of a foreign country, and the adviser and the SEC would need to be able to enforce judgments against the FFI. The Release states that a FFI could satisfy this requirement by appointing an agent for service of process, or by having offices, in the United States.

- Regulated by a foreign government or foreign financial regulatory authority as a banking institution, trust company or other financial institution that customarily holds financial assets for its customers.
- Required by law to comply with anti-money laundering provisions similar to those of the Bank Secrecy Act and regulations thereunder. The Release states that an FFI could satisfy this condition if the institution is required to comply with the laws or regulations of a member jurisdiction of the Financial Action Task Force (FATF) and the institution is not otherwise identified on a sanctions list maintained by the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) or Financial Crimes Enforcement Network (FinCEN).
- Holding financial assets for its customers in accounts designed to protect such assets from the FFI's creditors in the event of insolvency or failure.
- Having the requisite financial strength to provide due care for client assets. The Release states that a determination as to the financial strength of a FFI could be based on indicators of financial health that are comparable to the standards that apply to U.S. banks and other regulated financial institutions, noting that governments and banking regulators typically require foreign banking institutions to satisfy regulatory capital requirements.
- Required by law to adopt practices, procedures and internal controls designed to ensure the exercise of due care with respect to the safekeeping of client assets. The Release states that this requirement should ensure that the FFI's practices, procedures and internal controls are not materially different from those of U.S. qualified custodians, including with respect to the safekeeping of certificated and uncertificated assets, security and data protections and recordkeeping.
- Not operated for the purpose of avoiding the requirements of the Proposed Rule.

The Release recognizes that many FFIs may be unable to meet these requirements. These changes could make it difficult for advisers to offer investment strategies focused on emerging markets.

### **New Written Agreement with, and “Reasonable Assurances” from, each Qualified Custodian**

The Proposed Rule would require a new written agreement between the adviser and each qualified custodian that holds and maintains client assets. Each qualified custodian would also need to agree to certain minimum provisions in the agreement with the adviser, and the adviser would need to reasonably believe that such provisions have been implemented in order for the adviser to be in compliance with the Proposed Rule.

In addition to a written agreement requirement, the Proposed Rule would require the adviser to obtain certain reasonable assurances in writing from each qualified custodian, and the adviser would need to maintain an ongoing reasonable belief that the custodian is complying with the required assurances.

This element of the Proposed Rule would be a significant change from existing commercial norms, where qualified custodians enter into custody agreements with each client and advisers are typically not a party to such agreements.

### ***Qualified Custodian Must Have Possession or Control of Client Assets***

Where the current Custody Rule states simply that a qualified custodian must maintain client funds and securities, the Proposed Rule provides that a qualified custodian must maintain “possession or control” of client assets pursuant to a written agreement between the adviser and each qualified custodian. The Proposed Rule

sets forth a three-prong test to determine if “possession or control” is established. A qualified custodian would have possession or control of client assets if:

- The qualified custodian is required to participate in any change in beneficial ownership of client assets;
- The qualified custodian’s participation would effectuate the transaction required for the change in beneficial ownership; and
- The qualified custodian’s participation is a condition precedent to the change in beneficial ownership.

The Release indicates that the definition of “possession or control” is designed to be consistent with the custody requirements imposed by a custodian’s primary regulator. The Proposed Rule provides an exception from this requirement for privately offered securities and physical assets that are unable to be maintained with a qualified custodian in a manner by which a qualified custodian can maintain possession or control (see below).

The Release states that the qualified custodian’s required participation in changes in beneficial ownership of client assets will serve several important safeguarding functions, including by providing assurance to clients that the party hired for safekeeping services is involved in any change in beneficial ownership and by ensuring the integrity of account statements provided by qualified custodians.

The SEC acknowledged in the Release that demonstrating possession or control of crypto assets may be more challenging for qualified custodians than for traditional assets such as stocks and bonds. Given the nature of crypto assets, which can be transferred by anyone who possesses the corresponding private keys, a custodian may effectively be required to prove a negative to demonstrate exclusive possession or control (e.g., that no other party has a copy of the respective private keys). The SEC asserted, however, that demonstrating that a qualified custodian maintains “possession or control” also can be accomplished where the custodian’s involvement is required in order to effect any change of beneficial ownership of the crypto assets. This can be demonstrated, for example, where a custodian holds private keys in a multi-signature or multi-party computational solution. In these solutions, the custodian will hold one of a number of shards required in order to recompose a crypto asset’s private keys. Depending on the implementation, however, some solutions may not comply with the Proposed Rule (such as where two of three keys are required to effect a transaction and the custodian holds only one). The SEC further acknowledged that due to the prevailing methods used by crypto trading platforms that directly settle on such platforms, investors are often required to pre-fund trades by transferring their crypto assets or funds to the trading platforms prior to settlement. As a result, this practice would generally result in violations of the Proposed Rule for advisers that have custody of assets traded on crypto trading platforms that do not qualify as qualified custodians. The Release does acknowledge that certain SEC-registered crypto asset securities are traded on alternative trading systems that do not require pre-funding of trades, but it also notes that these systems do not allow trading of crypto assets that are not securities.

The Release overall is noncommittal as to the extent to which an adviser could satisfy its obligations under the Proposed Rule with respect to crypto assets using existing crypto trading platforms, a point which was emphasized by Commissioners Peirce and Uyeda. Commissioner Peirce noted, in particular, that the approach to crypto under the Proposed Rule would likely shrink “the ranks of qualified crypto custodians” and “could leave investors in crypto assets *more* vulnerable to theft or fraud.”<sup>5</sup> Commission Uyeda noted that the Release

---

<sup>5</sup> Commissioner Hester M. Peirce, [Statement on Safeguarding Advisory Client Assets Proposal](#) (Feb. 15, 2023).

“indicates that it is unlikely that crypto assets can be maintained at qualified custodians or traded on crypto trading platforms in compliance with the proposed rule.”<sup>6</sup>

### ***Minimum Provisions of Agreements Between Adviser and each Qualified Custodian***

Under the Proposed Rule, the written agreements between the adviser and each qualified custodian would need to contain the following provisions, and the adviser would need to have a reasonable belief that these provisions have been implemented:

- *Provision of Records:* require the qualified custodian to promptly, upon request, provide records relating to client assets to the SEC or an independent public accountant for purposes of complying with the Proposed Rule.
- *Account Statements:* require the qualified custodian to send account statements at least quarterly to the client and the adviser that identify the amount of client assets in the custodial account as well as the transactions that took place in the account during the period covered by the report.<sup>7</sup> The written agreement must further prohibit a qualified custodian from identifying assets on account statements over which the qualified custodian does not have possession or control, unless requested by the client. The requirement that the qualified custodian send account statements to the adviser as well as the client is a change from the Custody Rule, which requires only that the investment adviser have a reasonable belief that the qualified custodian sends a quarterly statement to the client.
- *Internal Control Report:* require the qualified custodian to provide the investment adviser with a written internal control report at least annually. Such internal control report must include an independent public accountant’s opinion as to whether controls designed to ensure the safeguarding of client assets are in place, are suitably designed and are operating effectively. The Release indicates that a SOC 1, Type 2 report, or its equivalent, would satisfy this requirement.
- *Adviser’s Level of Authority:* specify the adviser’s agreed-upon level of authority to effect transactions in the client’s custodial account. The Proposed Rule also requires that the agreement must permit the adviser and the client to reduce that level of authority.

Consistent with the Custody Rule, the Proposed Rule would permit an adviser or its related person to serve as qualified custodian, provided the adviser or its related persons who act as a qualified custodian satisfy certain additional requirements.

### ***Written Assurances from each Qualified Custodian***

Under the Proposed Rule, an adviser would have to both obtain written “reasonable assurances” from a qualified custodian, and maintain an ongoing reasonable belief, that the qualified custodian will:

- *Due Care:* exercise due care in accordance with reasonable commercial standards and implement appropriate measures to safeguard client assets from theft, misuse, misappropriation or other similar types of loss. The SEC acknowledged that appropriate measures will vary with the type of asset to be safeguarded.

---

<sup>6</sup> Commissioner Mark T. Uyeda, [Statement on Proposed Rule Regarding the Safeguarding of Advisory Client Assets](#) (Feb. 15, 2023).

<sup>7</sup> This provision would not be required for custodial arrangements in which the client is an entity whose investors will receive audited financial statements under the audit provision of the Proposed Rule.

- *Indemnification*: indemnify the client, and have adequate insurance arrangements in place to protect the client, against the risk of loss due to the qualified custodian's own negligence, recklessness or willful misconduct.
- *Sub-custodian or Other Similar Arrangements*: not be excused from any of its obligations to the client due to the existence of any sub-custodial, securities depository or other similar arrangements with regard to the client's assets. The Release states that such assurances would reduce the qualified custodian's ability to avoid responsibility for any losses suffered by the client caused by the custodian's decision to outsource part of its custodial functions.
- *Segregation of Client Assets*: clearly identify the client's assets and segregate them from the qualified custodian's proprietary assets and liabilities.<sup>8</sup>
- *No Liens Unless Authorized in Writing*: not subject client assets to any right, charge, security interest, lien or claim in favor of the qualified custodian or its related persons or creditors, except to the extent authorized by the client in writing. This requirement would not prohibit typical lending arrangements whereby a qualified custodian extends funds or leverage to a client collateralized by the assets in the client's account. It would, however, require the adviser to obtain reasonable assurances that the client has authorized in writing any interests in the client's assets in favor of the qualified custodian that might arise from such arrangements.

These new requirements would represent a significant departure from existing market practices, and would essentially dictate contractual terms with entities that are not directly regulated by the SEC. The Release acknowledges that custody arrangements vary widely and that many do not conform to the minimum requirements of the Proposed Rule. Custodians would have to agree to these new arrangements and related terms, which would likely impose substantial additional burdens and costs on custodians. It is not clear whether any or all custodians would agree to these new arrangements and related terms or, if they did, whether they would seek to pass along any of the related costs.

### **New Requirements for Privately Offered Securities and Physical Assets that Cannot be Maintained with a Qualified Custodian**

Under the Proposed Rule, an adviser would be exempt from complying with the qualified custodian requirements with respect to privately offered securities and physical assets, under stricter and more burdensome conditions than under the current Custody Rule.

The Release acknowledges that there are impediments to most privately offered securities and certain physical assets being maintained with a qualified custodian and that the marketplace for custody services for such assets is thin. The Proposed Rule, like the current Custody Rule, would provide an exception from the qualified custodian requirements for such assets, in recognition of these realities. However, the Proposed Rule would impose new requirements for privately offered securities and physical assets that cannot be maintained at a qualified custodian.

Under the Proposed Rule, an adviser with custody of privately offered securities or physical assets would not be required to comply with the qualified custodian requirements of the Proposed Rule if:

---

<sup>8</sup> The requirement to obtain assurances that the qualified custodian will segregate client assets would supplant the Custody Rule's requirement to maintain client funds and securities with a qualified custodian (1) in a separate account for each client under the client's name; or (2) in accounts that contain only client funds and securities under an adviser's name as agent or trustee for the clients.

- The adviser reasonably determines and documents in writing that ownership cannot be recorded and maintained in a manner by which a qualified custodian can maintain possession or control of such assets. The Release indicates that this determination would be a fact-specific inquiry but would generally turn on the custodial solutions available in the market and whether any qualified custodians are capable of, and willing to, custody the privately offered securities.
- The adviser reasonably safeguards the assets from loss, theft, misuse, misappropriation or the adviser's financial reverses, including the adviser's insolvency.
- The adviser enters into a written agreement with an independent public accountant, pursuant to which the accountant verifies any purchase, sale or transfer of beneficial ownership of such assets promptly upon receiving notice from the adviser of such transaction and notifies the SEC within one business day upon finding any material discrepancies during the course of performing its procedures.
- The adviser notifies the independent public accountant of any transactions requiring the accountant's verification within one business day.
- The existence and ownership of each of the client's privately offered securities or physical assets that are not maintained with a qualified custodian are verified during the annual surprise examination or as part of a financial statement audit. The Release explains that this requirement would ensure that a loss of a client's privately offered securities or physical assets does not go undetected for an extended period of time.

The SEC justified these new requirements by, among other rationales, pointing to the rapid increase in the size of the privately offered securities market since the exception was created, discounting facts cited in prior amendments to the Custody Rule that make privately offered securities less susceptible to misappropriation risk and pointing to perceived inadequacies of existing verification processes during surprise exams and financial statement audits.

We anticipate that industry participants will comment specifically on the costs and feasibility of these proposed requirements.

### ***Definitions of Privately Offered Security and Physical Asset***

The Proposed Rule would generally leave intact the definition of "privately offered securities." However, it would impose a requirement that privately offered securities are only capable of being recorded on the non-public books of the issuer or its transfer agent in the name of the client as it appears in the records the adviser must keep under the Recordkeeping Rule. The Release acknowledges that crypto asset ownership involving public blockchains is generally evidenced through public keys or wallet addresses. As a result, crypto assets issued on such blockchains would not be able to satisfy the conditions for the privately offered securities exception under the Proposed Rule. This is problematic for advisers with possession of client crypto assets for which no custodian provides custody services and appears to leave no avenue for compliance with the Proposed Rule.

The Proposed Rule does not provide a definition for the term "physical assets," and the Release states that what constitutes a physical asset is a facts-and-circumstances analysis.

### **Segregation of Client Assets**

In addition to the requirement that advisers obtain reasonable assurance that client assets are segregated from the qualified custodian's assets, the Proposed Rule would separately require that client assets over which the adviser has custody must:

- Be titled or registered in the client's name or otherwise held for the benefit of that client.
- Not be commingled with the adviser's assets or its related persons' assets.
- Not be subject to any interest of any kind in favor of the adviser, its related persons or its creditors, except to the extent authorized by the client in writing.

The Release indicates that the purpose of these requirements is principally to ensure segregation of client assets from the adviser's and its related persons' assets.

## **Amendments to the Surprise Examination Requirement**

### ***Reasonable Belief Requirement***

The Proposed Rule would maintain the requirement that the adviser and an independent public accountant enter into a written agreement pursuant to which the accountant would conduct a surprise examination. However, the Proposed Rule would impose a requirement that the adviser also reasonably believe that the accountant will perform its examination in accordance with the agreement. According to the SEC, this requirement was intended to address circumstances where advisers failed to ensure that these surprise examinations actually occurred. The Release notes that "advisers generally should enter into a written agreement with the accountant based upon a reasonable belief that the accountant is capable of, and intends to, comply with the agreement and the obligations the accountant is responsible for under the surprise examination requirement." The Release notes, for example, that advisers generally should ensure that the accountant can access the SEC's filing system to make the Form ADV-E filing.

### ***Expanded Availability of the Audit Provision***

The current Custody Rule's audit exception is available for any "pooled investment vehicle." The Proposed Rule would expand the scope of the audit exception to apply to any "entity." The Release indicates that this would codify and expand upon certain prior SEC staff no-action positions, and states that pension plans, retirement plans, college savings plans and other entities would be covered by this provision under the Proposed Rule.

### ***Extended Deadlines for Distribution of Audited Financials and U.S. Generally Accepted Accounting Principles Requirements***

The Proposed Rule would codify existing no-action relief for funds of funds to distribute audited financials to their investors within 180 days of the fund's fiscal year end, and funds of funds of funds to distribute audited financials to investors within 260 days of the fund's fiscal year end. The Release notes that if an adviser were unable to distribute audited financials within these timeframes due to reasonably unforeseen circumstances, that the failure to distribute the financials would not provide a basis for enforcement provided that the adviser had a reasonable belief that the financials would be distributed by the deadline.

The Proposed Rule would also codify the SEC staff's current approach of permitting non-U.S. vehicles to utilize the audit provision provided that the financial statements are prepared in accordance with U.S. Generally Accepted Accounting Principles (U.S. GAAP) or, provided that any material differences are reconciled to U.S. GAAP, substantially similar requirements.

### ***New Audit Provision Contract and Notice Requirements for Independent Public Accountants***

To rely on the audit provision under the Proposed Rule, the adviser or the entity client would be required to enter into a written agreement with the independent public accountant conducting the audit. Under the terms of the agreement, the independent public accountant would be required to notify the SEC within one business day if the accountant issues a modified opinion (*i.e.*, is qualified, adverse or a disclaimer of opinion) or the auditor is dismissed, and within four business days if the auditor resigns, is dismissed or terminated from an engagement or removes itself from consideration to continue as the entity's auditor.

### ***Exception for Advisers with Limited Delivery-Versus-Payment Authority***

The SEC proposed to include an exception from the surprise examination requirement for advisers that have custody of client assets solely due to having discretionary authority to trade such assets. This exception, however, would apply only when the client assets are maintained with a qualified custodian and the adviser's discretionary authority is limited to instructing the qualified custodian to trade the client assets on a delivery versus payment (DVP) basis. Notwithstanding the availability of this exception, the Release recognizes that qualified custodians have been generally unwilling in the past to accept adviser requests to limit the adviser's authority to DVP instructions.

### ***Exception for Standing Letters of Authorization***

Consistent with existing SEC staff relief, the Proposed Rule would also include an exception from the surprise examination requirement for advisers that have custody of client assets solely due to having a standing letter of authorization (SLOA). Under the Proposed Rule, a SLOA would be any arrangement among the adviser, the client and the qualified custodian that authorizes the adviser to direct the qualified custodian to disburse client assets to a third-party according to a specified schedule.

### **Amendments to the Recordkeeping Rule**

The SEC proposed various amendments to the Recordkeeping Rule. The amendments are intended to ensure a complete custodial record is maintained. Under the Proposed Rule, advisers would be required to maintain:

- *Client Communications*: copies of all written notices required to be sent to clients under the Proposed Rule and any client responses. Copies of custodial account opening notifications and any notices of changes to the qualified custodian's name, address and account number would need to be maintained under this requirement.
- *Client Accounts*: records pertaining to client account information; custodian identification, including copies of each agreement with a qualified custodian and documents forming the basis for the reasonable assurances obtained by the adviser; the reasons why an adviser has custody over assets in a client account, including whether the adviser has discretionary authority or the ability to deduct fees from the client's account; account statements received or sent by the adviser; transaction and holdings information; and SLOAs.
- *Account Activity*: copies of any account statement delivered by the qualified custodian to the client and to the adviser as well as any account statement the adviser delivers to the client. An adviser would also need to maintain records of all transaction activity in a client's account, which would include all debits and credits into the account. This would expand the Recordkeeping Rule's current requirement to maintain records related to a client account's trading activity.
- *Independent Public Accountant Engagements*: all audited financial statements prepared under the Proposed Rule; internal control reports received by the adviser; and copies of written agreements between the adviser and accountant.

- *Standing Letters of Authorization*: any copies of, and records pertaining to, a SLOA issued by a client.

## Form ADV Amendments

The final element of the SEC's proposal involves changes to Form ADV Part 1A. Among other amendments, a new subsection would be added in which an adviser would indicate its reliance on certain exceptions to the Proposed Rule. The Form ADV amendments would further require an adviser to indicate if it has custody of client assets directly, indirectly through a related person or due solely to its ability to deduct fees from the client's account or because it has discretionary authority.

If adopted, the Form ADV amendments would require an adviser to report the amount of client assets over which it has custody and break down that amount into different categories that give rise to custody. The categories would include custody due to: (1) having the ability to deduct fees; (2) discretionary trading authority; (3) serving as general partner, managing member or trustee for private fund clients; (4) serving as general partner, management member or trustee for non-private fund clients; (5) having check writing authority or a general power of attorney over client-assets; (6) acting pursuant to a SLOA; (7) having physical possession of client assets; (8) serving as a qualified custodian; (9) a related person having custody; and (10) any other reason.

Additionally, the Form ADV amendments would require an adviser with custody of client assets to provide identifying information about the qualified custodian at which those assets are maintained as well as identifying information about accountants that complete surprise examinations, financial statement audits or verification of client assets as required under the Proposed Rule.

## Key Dates and Timing

If adopted, the Proposed Rule and related amendments to the Recordkeeping Rule and Form ADV would have a transition period of one year from the effective date of the Proposed Rule. For advisers with less than \$1 billion in assets under management, the SEC proposes an extended transition period of eighteen months.

## Conclusion

The Proposed Rule would represent a substantial update to the current Custody Rule. The Proposed Rule would impose significant new requirements on advisers and would make an adviser's compliance largely contingent on financial institutions, which the SEC does not regulate directly, agreeing to specified commercial standards. If adopted, significant amendments may be required to existing commercial arrangements among investors, clients, advisers, custodians and independent accounting firms. New or updated commercial arrangements with such service providers would likely come at much higher cost. Advisers would have administrative burdens associated with updating these commercial arrangements and would bear new administrative expenses related to ongoing compliance obligations. For certain clients or client assets, it is also possible that a market comprised of qualified custodians that fully comply with the Proposed Rule may never develop or may be so thin that the risks and costs to clients become significant. Furthermore, the market might develop in ways that disadvantage or disenfranchise certain types of advisers that custodians may not want to serve on commercially reasonable terms. In light of these challenges, coming into compliance would be particularly difficult within the SEC's proposed one-year transition period for large advisers and eighteen months for small advisers.

Stakeholders may wish to provide their views to the SEC during the public comment period for the Proposed Rule, which ends May 8, 2023.

This update was authored by:



**David P. Bartels**  
Partner  
Washington, D.C.  
+1 202 261 3375  
[david.bartels@dechert.com](mailto:david.bartels@dechert.com)



**Brenden P. Carroll**  
Partner  
Washington, D.C.  
+1 202 261 3458  
[brenden.carroll@dechert.com](mailto:brenden.carroll@dechert.com)



**Mark D. Perlow**  
Partner  
San Francisco  
+1 415 262 4530  
[mark.perlow@dechert.com](mailto:mark.perlow@dechert.com)



**Paul S. Stevens Jr.**  
Partner  
Washington, D.C.  
+1 202 261 3353  
[paul.stevens@dechert.com](mailto:paul.stevens@dechert.com)



**Phillip Garber**  
Associate  
San Francisco  
+1 415 262 4554  
[phillip.garber@dechert.com](mailto:phillip.garber@dechert.com)



**Michael Murphy**  
Associate  
Boston  
+1 617 728 7155  
[michael.murphy@dechert.com](mailto:michael.murphy@dechert.com)



**Ashley N. Rodriguez**  
Associate  
Washington, D.C.  
+1 202 261 3446  
[ashley.rodriquez@dechert.com](mailto:ashley.rodriquez@dechert.com)

© 2022 Dechert LLP. All rights reserved. This publication should not be considered as legal opinions on specific facts or as a substitute for legal counsel. It is provided by Dechert LLP as a general informational service and may be considered attorney advertising in some jurisdictions. Prior results do not guarantee a similar outcome. We can be reached at the following postal addresses: in the US: 1095 Avenue of the Americas, New York, NY 10036-6797 (+1 212 698 3500); in Hong Kong: 27/F Henley Building, 5 Queen's Road Central, Hong Kong (+852 3518 4700); and in the UK: 160 Queen Victoria Street, London EC4V 4QQ (+44 20 7184 7000). Dechert internationally is a combination of separate limited liability partnerships and other entities registered in different jurisdictions. Dechert has more than 900 qualified lawyers and 700 staff members in its offices in Belgium, China, France, Germany, Georgia, Hong Kong, Ireland, Kazakhstan, Luxembourg, Russia, Singapore, the United Arab Emirates, the UK and the US. Further details of these partnerships and entities can be found at [dechert.com](http://dechert.com) on our Legal Notices page.

---

# SEC Charges Four Investment Advisers with Violations of the Custody Rule

## ADMINISTRATIVE PROCEEDING

File No. 3-21760

**September 28, 2023** – The Securities and Exchange Commission today announced settled charges against four investment advisers owned by Osaic, Inc., formerly known as Advisor Group, Inc. (the “Advisers”): FSC Securities Corporation, Osaic Wealth, Inc. (formerly known as Royal Alliance Associates), SagePoint Financial, Inc., and Woodbury Financial Services. The Advisers failed to obtain verification by an independent public accountant of client funds and securities of which they had custody by virtue of a provision in agreements among the Advisers, their clients, and a clearing firm.

According to the SEC’s orders, from June 2017 to December 2022, each Adviser used a form agreement to govern certain aspects of the relationship among the Adviser, its clients, and a particular clearing agent the Adviser used. As set forth in the orders, these agreements each included a margin account agreement that contained language, required by this clearing agent, that permitted the clearing agent to accept, without inquiry or investigation, any instructions given by the Adviser concerning these clients’ accounts. The orders find that, as a consequence of the Advisers having this authority with respect to the client funds and securities in these accounts, the Advisers had custody of these assets. The orders further find that, because the Advisers failed to obtain verification by actual examination of the client funds and securities in these accounts by an independent public accountant, the Advisers violated Section 206(4) of the Advisers Act and Rule 206(4)-2 thereunder, commonly referred to as the “custody rule.”

Each of the Advisers consented to the entry of an SEC order finding that the firm willfully violated the custody rule. Without admitting or denying the findings, each of the Advisers agreed to a cease-and-desist order, a censure, and a \$100,000 civil penalty to settle the charges.

The SEC’s investigation was conducted by Craig Welter and was supervised by Lee A. Greenwood, Andrew Dean, and Corey Schuster, all of the Division of Enforcement’s Asset Management Unit. The examination that led to Enforcement’s investigation was conducted by Arjuman Sultana, Michael Qualter, Lev Miller, Margaret Pottanat, Hareesh Mehta, and Merry Hoffman of the Division of Examinations.

## Related Materials

- [Order - FSC Securities Corporation](#)
- [Order - Osaic Wealth, Inc.](#)
- [Order - SagePoint Financial, Inc.](#)
- [Order - Woodbury Financial Services, Inc.](#)

*Modified: Sept. 28, 2023*

**UNITED STATES OF AMERICA**  
**Before the**  
**SECURITIES AND EXCHANGE COMMISSION**

**INVESTMENT ADVISERS ACT OF 1940**  
**Release No. 6441 / September 28, 2023**

**ADMINISTRATIVE PROCEEDING**  
**File No. 3-21757**

**In the Matter of**

**FSC SECURITIES  
CORPORATION,**

**Respondent.**

**ORDER INSTITUTING ADMINISTRATIVE  
AND CEASE-AND-DESIST PROCEEDINGS,  
PURSUANT TO SECTIONS 203(e) AND  
203(k) OF THE INVESTMENT ADVISERS  
ACT OF 1940, MAKING FINDINGS, AND  
IMPOSING REMEDIAL SANCTIONS AND  
A CEASE-AND-DESIST ORDER**

**I.**

The Securities and Exchange Commission (“Commission”) deems it appropriate and in the public interest that public administrative and cease-and-desist proceedings be, and hereby are, instituted pursuant to Sections 203(e) and 203(k) of the Investment Advisers Act of 1940 (“Advisers Act”) against FSC Securities Corporation (“FSC” or “Respondent”).

**II.**

In anticipation of the institution of these proceedings, Respondent has submitted an Offer of Settlement (the “Offer”) which the Commission has determined to accept. Solely for the purpose of these proceedings and any other proceedings brought by or on behalf of the Commission, or to which the Commission is a party, and without admitting or denying the findings herein, except as to the Commission’s jurisdiction over Respondent and the subject matter of these proceedings, which are admitted, Respondent consents to the entry of this Order Instituting Administrative and Cease-and-Desist Proceedings, Pursuant to Sections 203(e) and 203(k) of the Investment Advisers Act of 1940, Making Findings, and Imposing Remedial Sanctions and a Cease-and-Desist Order (“Order”), as set forth below.

### III.

On the basis of this Order and Respondent's Offer, the Commission finds<sup>1</sup> that

#### **Summary**

1. This matter arises out of the failure of FSC, a registered investment adviser, to obtain verification by an independent public accountant of client funds and securities of which it had custody. From June 2017 to December 2022 (the "Relevant Period"), FSC used a form agreement to govern certain aspects of the relationship among FSC, its clients, and a particular clearing agent FSC used (the "Clearing Agent"). Each of these agreements ("Customer Agreements") included a margin account agreement that contained language, required by the Clearing Agent, that permitted the Clearing Agent to accept, without inquiry or investigation, any instructions given by FSC concerning these clients' accounts (the "Affected Accounts"). As a consequence of FSC having this authority with respect to the client funds and securities in the Affected Accounts, FSC had custody of these assets. Accordingly, because FSC failed to obtain verification by actual examination of the client funds and securities in the Affected Accounts by an independent public accountant, FSC violated Section 206(4) of the Advisers Act and Rule 206(4)-2 thereunder, commonly referred to as the "custody rule."

#### **Respondent**

2. FSC, a Delaware corporation with its principal place of business in Atlanta, Georgia, is a dually registered investment adviser and broker-dealer. FSC has been registered with the Commission as an investment adviser since 1992 and as a broker-dealer since 1977. As of December 31, 2022, FSC managed approximately \$11.8 billion in regulatory assets under management. FSC is a subsidiary of Osaic, Inc. (f/k/a Advisor Group, Inc.), a wholly-owned subsidiary of Osaic Holdings, Inc.

#### **Facts**

3. The custody rule requires that registered investment advisers who have custody of client funds or securities implement an enumerated set of requirements to prevent the loss, misuse, or misappropriation of those assets.

4. During the Relevant Period, the Clearing Agent served as clearing agent for more than 49,000<sup>2</sup> FSC advisory clients' funds and securities under management. Certain aspects of the relationship among these Affected Accounts clients, FSC, and the Clearing Agent were governed by the Customer Agreements.

---

<sup>1</sup> The findings herein are made pursuant to Respondent's Offer of Settlement and are not binding on any other person or entity in this or any other proceeding.

<sup>2</sup> As of December 31, 2022.

5. FSC included as part of its Customer Agreements a section that served as a margin account agreement, the language for which was required by the Clearing Agent. This section of the Customer Agreements stated, in relevant part:

Until receipt from the Customer of written notice to the contrary, [the Clearing Agent] may accept from FSC, without inquiry or investigation, (i) orders for the purchase or sale of securities and other property on margin or otherwise, and (ii) any other instructions concerning said accounts.

6. All of the Customer Agreements included a margin account agreement with the above language during the Relevant Period. As of December 31, 2022, 458 FSC advisory clients maintained margin accounts.

7. An investment adviser has custody of client assets if it holds, directly or indirectly, client funds or securities, or if it has the ability to obtain possession of those assets. *See* Rule 206(4)-2(d)(2). Custody includes “[a]ny arrangement . . . under which [an investment adviser is] authorized or permitted to withdraw client funds or securities maintained with a custodian upon [its] instruction to the custodian.” *See* Rule 206(4)-2(d)(2).

8. An investment adviser who has custody of client assets must, among other things: (i) maintain clients’ assets with a qualified custodian; (ii) notify the client in writing of accounts opened by the adviser at a qualified custodian on the client’s behalf; (iii) have a reasonable basis for believing that the qualified custodian sends account statements at least quarterly to clients, except if the client is a limited partnership or limited liability company for which the adviser or a related person is a general partner, the account statements must be sent to each limited partner or member; and (iv) obtain verification of client funds and securities by actual examination each calendar year by an independent public accountant at a time chosen by the accountant without prior notice or announcement to the adviser. *See* Rule 206(4)-2(a).

9. By virtue of FSC’s authority under the Customer Agreements described above to give “any other instructions” concerning the Affected Accounts “without inquiry or investigation” by the Clearing Agent, which could include instructions by FSC regarding the withdrawal of client funds or securities, FSC had custody of the assets in the Affected Accounts under Rule 206(4)-2.

10. With respect to the Affected Accounts, Respondent failed to obtain verification of client funds and securities by annual actual examinations by an independent public accountant for the calendar years 2017 through 2022.

11. In August 2020, in connection with an ongoing examination of FSC, the staff of the Commission’s Division of Examinations expressed in writing “concerns” regarding the language contained in the Customer Agreements described above and stated that FSC “appeared to have violated the Custody Rule.” In November 2020, FSC responded that it believed it was in compliance with the custody rule. On May 18, 2023, FSC removed the language described above from its Customer Agreements. In August 2023, FSC engaged an independent public

accountant to verify by actual examination the client funds and securities for accounts subject to the Customer Agreements during the calendar year 2023.

### **Violations**

12. Section 206(4) of the Advisers Act prohibits an investment adviser from engaging in acts, practices or courses of business that are fraudulent, deceptive, or manipulative, as defined by the Commission in rules and regulations promulgated under the statute. Proof of scienter is not required to establish a violation of Section 206(4) of the Advisers Act and the rules thereunder. *See SEC v. Steadman*, 967 F.2d 636, 647 (D.C. Cir. 1992).

13. Among other things, Rule 206(4)-2 requires registered investment advisers that have custody of client funds or securities to have independent public accountants conduct a verification of those client funds and securities by actual examination at least once each calendar year. By failing to have such a surprise examination of these client funds and securities for which it had custody, FSC willfully<sup>3</sup> violated Section 206(4) of the Advisers Act and Rule 206(4)-2 thereunder.

### **IV.**

In view of the foregoing, the Commission deems it appropriate, in the public interest, and for the protection of investors to impose the sanctions agreed to in Respondent FSC's Offer.

Accordingly, pursuant to Sections 203(e) and 203(k) of the Advisers Act, it is hereby ORDERED that:

A. Respondent FSC cease and desist from committing or causing any violations and any future violations of Section 206(4) of the Advisers Act and Rule 206(4)-2 promulgated thereunder.

B. Respondent FSC is censured.

C. FSC shall, within 10 days of the entry of this Order, pay a civil money penalty in the amount of \$100,000 to the Securities and Exchange Commission for transfer to the general fund of the United States Treasury, subject to Section 21F(g)(3) of the Securities Exchange Act of 1934. If timely payment is not made, additional interest shall accrue pursuant to 31 U.S.C. § 3717.

Payment must be made in one of the following ways:

- (1) Respondent may transmit payment electronically to the Commission, which will provide detailed ACH transfer/Fedwire instructions upon request;

---

<sup>3</sup> "Willfully," for purposes of imposing relief under Section 203(e) of the Advisers Act, "means no more than that the person charged with the duty knows what he is doing." *Wonsover v. SEC*, 205 F.3d 408, 414 (D.C. Cir. 2000) (quoting *Hughes v. SEC*, 174 F.2d 969, 977 (D.C. Cir. 1949)). There is no requirement that the actor "also be aware that he is violating one of the Rules or Acts." *Tager v. SEC*, 344 F.2d 5, 8 (2d Cir. 1965).

- (2) Respondent may make direct payment from a bank account via Pay.gov through the SEC website at <http://www.sec.gov/about/offices/ofm.htm>; or
- (3) Respondent may pay by certified check, bank cashier's check, or United States postal money order, made payable to the Securities and Exchange Commission and hand-delivered or mailed to:

Enterprise Services Center  
Accounts Receivable Branch  
HQ Bldg., Room 181, AMZ 341  
6500 South MacArthur Boulevard  
Oklahoma City, OK 73169

Payments by check or money order must be accompanied by a cover letter identifying FSC as a Respondent in these proceedings, and the file number of these proceedings; a copy of the cover letter and check or money order must be sent to Lee A. Greenwood, Assistant Regional Director, Asset Management Unit, Division of Enforcement, Securities and Exchange Commission, New York Regional Office, 100 Pearl Street, Suite 20-100, New York, NY 10004.

D. Amounts ordered to be paid as civil money penalties pursuant to this Order shall be treated as penalties paid to the government for all purposes, including all tax purposes. To preserve the deterrent effect of the civil penalty, Respondent agrees that in any Related Investor Action, it shall not argue that it is entitled to, nor shall it benefit by, offset or reduction of any award of compensatory damages by the amount of any part of Respondent's payment of a civil penalty in this action ("Penalty Offset"). If the court in any Related Investor Action grants such a Penalty Offset, Respondent agrees that it shall, within 30 days after entry of a final order granting the Penalty Offset, notify the Commission's counsel in this action and pay the amount of the Penalty Offset to the Securities and Exchange Commission. Such a payment shall not be deemed an additional civil penalty and shall not be deemed to change the amount of the civil penalty imposed in this proceeding. For purposes of this paragraph, a "Related Investor Action" means a private damages action brought against Respondent by or on behalf of one or more investors based on substantially the same facts as alleged in the Order instituted by the Commission in this proceeding.

By the Commission.

Vanessa A. Countryman  
Secretary

**UNITED STATES OF AMERICA**  
**Before the**  
**SECURITIES AND EXCHANGE COMMISSION**

**INVESTMENT ADVISERS ACT OF 1940**  
**Release No. 6442 / September 28, 2023**

**ADMINISTRATIVE PROCEEDING**  
**File No. 3-21758**

**In the Matter of**

**OSAIC WEALTH, INC.,**

**Respondent.**

**ORDER INSTITUTING ADMINISTRATIVE  
AND CEASE-AND-DESIST PROCEEDINGS,  
PURSUANT TO SECTIONS 203(e) AND  
203(k) OF THE INVESTMENT ADVISERS  
ACT OF 1940, MAKING FINDINGS, AND  
IMPOSING REMEDIAL SANCTIONS AND  
A CEASE-AND-DESIST ORDER**

**I.**

The Securities and Exchange Commission (“Commission”) deems it appropriate and in the public interest that public administrative and cease-and-desist proceedings be, and hereby are, instituted pursuant to Sections 203(e) and 203(k) of the Investment Advisers Act of 1940 (“Advisers Act”) against Osaic Wealth, Inc. (“Osaic Wealth” or “Respondent”).

**II.**

In anticipation of the institution of these proceedings, Respondent has submitted an Offer of Settlement (the “Offer”) which the Commission has determined to accept. Solely for the purpose of these proceedings and any other proceedings brought by or on behalf of the Commission, or to which the Commission is a party, and without admitting or denying the findings herein, except as to the Commission’s jurisdiction over Respondent and the subject matter of these proceedings, which are admitted, Respondent consents to the entry of this Order Instituting Administrative and Cease-and-Desist Proceedings, Pursuant to Sections 203(e) and 203(k) of the Investment Advisers Act of 1940, Making Findings, and Imposing Remedial Sanctions and a Cease-and-Desist Order (“Order”), as set forth below.

### III.

On the basis of this Order and Respondent's Offer, the Commission finds<sup>1</sup> that

#### Summary

1. This matter arises out of the failure of Osaic Wealth, a registered investment adviser, to obtain verification by an independent public accountant of client funds and securities of which it had custody. From June 2017 to December 2022 (the "Relevant Period"), Osaic Wealth used a form agreement to govern certain aspects of the relationship among Osaic Wealth, its clients, and a particular clearing agent Osaic Wealth used (the "Clearing Agent"). Each of these agreements ("Customer Agreements") included a margin account agreement that contained language, required by the Clearing Agent, that permitted the Clearing Agent to accept, without inquiry or investigation, any instructions given by Osaic Wealth concerning these clients' accounts (the "Affected Accounts"). As a consequence of Osaic Wealth having this authority with respect to the client funds and securities in the Affected Accounts, Osaic Wealth had custody of these assets. Accordingly, because Osaic Wealth failed to obtain verification by actual examination of the client funds and securities in the Affected Accounts by an independent public accountant, Osaic Wealth violated Section 206(4) of the Advisers Act and Rule 206(4)-2 thereunder, commonly referred to as the "custody rule."

#### Respondent

2. **Osaic Wealth**, a Delaware corporation with its principal place of business in Jersey City, NJ, is a dually registered investment adviser and broker-dealer. Osaic Wealth has been registered with the Commission as an investment adviser since 1997 and as a broker-dealer since 1988. Prior to June 21, 2023, Osaic Wealth was named Royal Alliance Associates, Inc. As of December 31, 2022, Osaic Wealth managed approximately \$29.5 billion in regulatory assets under management. Osaic Wealth is a subsidiary of Osaic, Inc. (f/k/a Advisor Group, Inc.), a wholly-owned subsidiary of Osaic Holdings, Inc.

#### Facts

3. The custody rule requires that registered investment advisers who have custody of client funds or securities implement an enumerated set of requirements to prevent the loss, misuse, or misappropriation of those assets.

4. During the Relevant Period, the Clearing Agent served as clearing agent for more than 83,000<sup>2</sup> Osaic Wealth advisory clients' funds and securities under management. Certain aspects of the relationship among these Affected Accounts clients, Osaic Wealth, and the Clearing Agent were governed by the Customer Agreements.

---

<sup>1</sup> The findings herein are made pursuant to Respondent's Offer of Settlement and are not binding on any other person or entity in this or any other proceeding.

<sup>2</sup> As of December 31, 2022.

5. Osaic Wealth included as part of its Customer Agreements a section that served as a margin account agreement, the language for which was required by the Clearing Agent. This section of the Customer Agreements stated, in relevant part:

Until receipt from the Customer of written notice to the contrary, [the Clearing Agent] may accept from [Osaic Wealth], without inquiry or investigation, (i) orders for the purchase or sale of securities and other property on margin or otherwise, and (ii) any other instructions concerning said accounts.

6. All of the Customer Agreements included a margin account agreement with the above language during the Relevant Period. As of December 31, 2022, 313 Osaic Wealth advisory clients maintained margin accounts.

7. An investment adviser has custody of client assets if it holds, directly or indirectly, client funds or securities, or if it has the ability to obtain possession of those assets. *See* Rule 206(4)-2(d)(2). Custody includes “[a]ny arrangement . . . under which [an investment advisor is] authorized or permitted to withdraw client funds or securities maintained with a custodian upon [its] instruction to the custodian.” *See* Rule 206(4)-2(d)(2).

8. An investment adviser who has custody of client assets must, among other things: (i) maintain clients’ assets with a qualified custodian; (ii) notify the client in writing of accounts opened by the adviser at a qualified custodian on the client’s behalf; (iii) have a reasonable basis for believing that the qualified custodian sends account statements at least quarterly to clients, except if the client is a limited partnership or limited liability company for which the adviser or a related person is a general partner, the account statements must be sent to each limited partner or member; and (iv) obtain verification of client funds and securities by actual examination each calendar year by an independent public accountant at a time chosen by the accountant without prior notice or announcement to the adviser. *See* Rule 206(4)-2(a).

9. By virtue of Osaic Wealth’s authority under the Customer Agreements described above to give “any other instructions” concerning the Affected Accounts “without inquiry or investigation” by the Clearing Agent, which could include instructions by Osaic Wealth regarding the withdrawal of client funds or securities, Osaic Wealth had custody of the assets in the Affected Accounts under Rule 206(4)-2.

10. With respect to the Affected Accounts, Respondent failed to obtain verification of client funds and securities by annual actual examinations by an independent public accountant for the calendar years 2017 through 2022.

11. In August 2020, in connection with an ongoing examination of Osaic Wealth, the staff of the Commission’s Division of Examinations expressed in writing “concerns” regarding the language contained in the Customer Agreements described above and stated that Osaic Wealth “appeared to have violated the Custody Rule.” In November 2020, Osaic Wealth responded that it believed it was in compliance with the custody rule. On May 18, 2023, Osaic Wealth removed the language described above from its Customer Agreements. In August 2023, Osaic Wealth engaged an independent public accountant to verify by actual examination the

client funds and securities for accounts subject to the Customer Agreements during the calendar year 2023.

### **Violations**

12. Section 206(4) of the Advisers Act prohibits an investment adviser from engaging in acts, practices or courses of business that are fraudulent, deceptive, or manipulative, as defined by the Commission in rules and regulations promulgated under the statute. Proof of scienter is not required to establish a violation of Section 206(4) of the Advisers Act and the rules thereunder. *See SEC v. Steadman*, 967 F.2d 636, 647 (D.C. Cir. 1992).

13. Among other things, Rule 206(4)-2 requires registered investment advisers that have custody of client funds or securities to have independent public accountants conduct a verification of those client funds and securities by actual examination at least once each calendar year. By failing to have such a surprise examination of these client funds and securities for which it had custody, Osaic Wealth willfully<sup>3</sup> violated Section 206(4) of the Advisers Act and Rule 206(4)-2 thereunder.

### **IV.**

In view of the foregoing, the Commission deems it appropriate, in the public interest, and for the protection of investors to impose the sanctions agreed to in Respondent Osaic Wealth's Offer.

Accordingly, pursuant to Sections 203(e) and 203(k) of the Advisers Act, it is hereby ORDERED that:

A. Respondent Osaic Wealth cease and desist from committing or causing any violations and any future violations of Section 206(4) of the Advisers Act and Rule 206(4)-2 promulgated thereunder.

B. Respondent Osaic Wealth is censured.

C. Osaic Wealth shall, within 10 days of the entry of this Order, pay a civil money penalty in the amount of \$100,000 to the Securities and Exchange Commission for transfer to the general fund of the United States Treasury, subject to Section 21F(g)(3) of the Securities Exchange Act of 1934. If timely payment is not made, additional interest shall accrue pursuant to 31 U.S.C. § 3717.

---

<sup>3</sup> "Willfully," for purposes of imposing relief under Section 203(e) of the Advisers Act, "means no more than that the person charged with the duty knows what he is doing." *Wonsover v. SEC*, 205 F.3d 408, 414 (D.C. Cir. 2000) (quoting *Hughes v. SEC*, 174 F.2d 969, 977 (D.C. Cir. 1949)). There is no requirement that the actor "also be aware that he is violating one of the Rules or Acts." *Tager v. SEC*, 344 F.2d 5, 8 (2d Cir. 1965).

Payment must be made in one of the following ways:

- (1) Respondent may transmit payment electronically to the Commission, which will provide detailed ACH transfer/Fedwire instructions upon request;
- (2) Respondent may make direct payment from a bank account via Pay.gov through the SEC website at <http://www.sec.gov/about/offices/ofm.htm>; or
- (3) Respondent may pay by certified check, bank cashier's check, or United States postal money order, made payable to the Securities and Exchange Commission and hand-delivered or mailed to:

Enterprise Services Center  
Accounts Receivable Branch  
HQ Bldg., Room 181, AMZ 341  
6500 South MacArthur Boulevard  
Oklahoma City, OK 73169

Payments by check or money order must be accompanied by a cover letter identifying Osaic Wealth as a Respondent in these proceedings, and the file number of these proceedings; a copy of the cover letter and check or money order must be sent to Lee A. Greenwood, Assistant Regional Director, Asset Management Unit, Division of Enforcement, Securities and Exchange Commission, New York Regional Office, 100 Pearl Street, Suite 20-100, New York, NY 10004.

D. Amounts ordered to be paid as civil money penalties pursuant to this Order shall be treated as penalties paid to the government for all purposes, including all tax purposes. To preserve the deterrent effect of the civil penalty, Respondent agrees that in any Related Investor Action, it shall not argue that it is entitled to, nor shall it benefit by, offset or reduction of any award of compensatory damages by the amount of any part of Respondent's payment of a civil penalty in this action ("Penalty Offset"). If the court in any Related Investor Action grants such a Penalty Offset, Respondent agrees that it shall, within 30 days after entry of a final order granting the Penalty Offset, notify the Commission's counsel in this action and pay the amount of the Penalty Offset to the Securities and Exchange Commission. Such a payment shall not be deemed an additional civil penalty and shall not be deemed to change the amount of the civil penalty imposed in this proceeding. For purposes of this paragraph, a "Related Investor Action" means a private damages action brought against Respondent by or on behalf of one or more investors based on substantially the same facts as alleged in the Order instituted by the Commission in this proceeding.

By the Commission.

Vanessa A. Countryman  
Secretary

**UNITED STATES OF AMERICA**  
**Before the**  
**SECURITIES AND EXCHANGE COMMISSION**

**INVESTMENT ADVISERS ACT OF 1940**  
**Release No. 6443 / September 28, 2023**

**ADMINISTRATIVE PROCEEDING**  
**File No. 3-21759**

**In the Matter of**

**SAGEPOINT FINANCIAL,**  
**INC.,**

**Respondent.**

**ORDER INSTITUTING ADMINISTRATIVE  
AND CEASE-AND-DESIST PROCEEDINGS,  
PURSUANT TO SECTIONS 203(e) AND  
203(k) OF THE INVESTMENT ADVISERS  
ACT OF 1940, MAKING FINDINGS, AND  
IMPOSING REMEDIAL SANCTIONS AND  
A CEASE-AND-DESIST ORDER**

**I.**

The Securities and Exchange Commission (“Commission”) deems it appropriate and in the public interest that public administrative and cease-and-desist proceedings be, and hereby are, instituted pursuant to Sections 203(e) and 203(k) of the Investment Advisers Act of 1940 (“Advisers Act”) against SagePoint Financial, Inc. (“SagePoint” or “Respondent”).

**II.**

In anticipation of the institution of these proceedings, Respondent has submitted an Offer of Settlement (the “Offer”) which the Commission has determined to accept. Solely for the purpose of these proceedings and any other proceedings brought by or on behalf of the Commission, or to which the Commission is a party, and without admitting or denying the findings herein, except as to the Commission’s jurisdiction over Respondent and the subject matter of these proceedings, which are admitted, Respondent consents to the entry of this Order Instituting Administrative and Cease-and-Desist Proceedings, Pursuant to Sections 203(e) and 203(k) of the Investment Advisers Act of 1940, Making Findings, and Imposing Remedial Sanctions and a Cease-and-Desist Order (“Order”), as set forth below.

### III.

On the basis of this Order and Respondent's Offer, the Commission finds<sup>1</sup> that

#### Summary

1. This matter arises out of the failure of SagePoint, a registered investment adviser, to obtain verification by an independent public accountant of client funds and securities of which it had custody. From June 2017 to December 2022 (the "Relevant Period"), SagePoint used a form agreement to govern certain aspects of the relationship among SagePoint, its clients, and a particular clearing agent SagePoint used (the "Clearing Agent"). Each of these agreements ("Customer Agreements") included a margin account agreement that contained language, required by the Clearing Agent, that permitted the Clearing Agent to accept, without inquiry or investigation, any instructions given by SagePoint concerning these clients' accounts (the "Affected Accounts"). As a consequence of SagePoint having this authority with respect to the client funds and securities in the Affected Accounts, SagePoint had custody of these assets. Accordingly, because SagePoint failed to obtain verification by actual examination of the client funds and securities in the Affected Accounts by an independent public accountant, SagePoint violated Section 206(4) of the Advisers Act and Rule 206(4)-2 thereunder, commonly referred to as the "custody rule."

#### Respondent

2. **SagePoint**, a Delaware corporation with its principal place of business in Phoenix, Arizona, is a dually registered investment adviser and broker-dealer. SagePoint has been registered with the Commission as both an investment adviser and a broker-dealer since 2005. As of December 31, 2022, SagePoint managed approximately \$16.5 billion in regulatory assets under management. SagePoint is a subsidiary of Osaic, Inc. (f/k/a Advisor Group, Inc.), a wholly-owned subsidiary of Osaic Holdings, Inc.

#### Facts

3. The custody rule requires that registered investment advisers who have custody of client funds or securities implement an enumerated set of requirements to prevent the loss, misuse, or misappropriation of those assets.

4. During the Relevant Period, the Clearing Agent served as clearing agent for more than 62,000<sup>2</sup> SagePoint advisory clients' funds and securities under management. Certain aspects of the relationship among these Affected Accounts clients, SagePoint, and the Clearing Agent were governed by the Customer Agreements.

---

<sup>1</sup> The findings herein are made pursuant to Respondent's Offer of Settlement and are not binding on any other person or entity in this or any other proceeding.

<sup>2</sup> As of December 31, 2022.

5. SagePoint included as part of its Customer Agreements a section that served as a margin account agreement, the language for which was required by the Clearing Agent. This section of the Customer Agreements stated, in relevant part:

Until receipt from the Customer of written notice to the contrary, [the Clearing Agent] may accept from SagePoint Financial, without inquiry or investigation, (i) orders for the purchase or sale of securities and other property on margin or otherwise, and (ii) any other instructions concerning said accounts.

6. All of the Customer Agreements included a margin account agreement with the above language during the Relevant Period. As of December 31, 2022, 579 SagePoint advisory clients maintained margin accounts.

7. An investment adviser has custody of client assets if it holds, directly or indirectly, client funds or securities, or if it has the ability to obtain possession of those assets. *See* Rule 206(4)-2(d)(2). Custody includes “[a]ny arrangement . . . under which [an investment advisor is] authorized or permitted to withdraw client funds or securities maintained with a custodian upon [its] instruction to the custodian.” *See* Rule 206(4)-2(d)(2).

8. An investment adviser who has custody of client assets must, among other things: (i) maintain clients’ assets with a qualified custodian; (ii) notify the client in writing of accounts opened by the adviser at a qualified custodian on the client’s behalf; (iii) have a reasonable basis for believing that the qualified custodian sends account statements at least quarterly to clients, except if the client is a limited partnership or limited liability company for which the adviser or a related person is a general partner, the account statements must be sent to each limited partner or member; and (iv) obtain verification of client funds and securities by actual examination each calendar year by an independent public accountant at a time chosen by the accountant without prior notice or announcement to the adviser. *See* Rule 206(4)-2(a).

9. By virtue of SagePoint’s authority under the Customer Agreements described above to give “any other instructions” concerning the Affected Accounts “without inquiry or investigation” by the Clearing Agent, which could include instructions by SagePoint regarding the withdrawal of client funds or securities, SagePoint had custody of the assets in the Affected Accounts under Rule 206(4)-2.

10. With respect to the Affected Accounts, Respondent failed to obtain verification of client funds and securities by annual actual examinations by an independent public accountant for the calendar years 2017 through 2022.

11. In August 2020, in connection with an ongoing examination of SagePoint, the staff of the Commission’s Division of Examinations expressed in writing “concerns” regarding the language contained in the Customer Agreements described above and stated that SagePoint “appeared to have violated the Custody Rule.” In November 2020, SagePoint responded that it believed it was in compliance with the custody rule. On May 18, 2023, SagePoint removed the language described above from its Customer Agreements. In August 2023, SagePoint engaged

an independent public accountant to verify by actual examination the client funds and securities for accounts subject to the Customer Agreements during the calendar year 2023.

### **Violations**

12. Section 206(4) of the Advisers Act prohibits an investment adviser from engaging in acts, practices or courses of business that are fraudulent, deceptive, or manipulative, as defined by the Commission in rules and regulations promulgated under the statute. Proof of scienter is not required to establish a violation of Section 206(4) of the Advisers Act and the rules thereunder. *See SEC v. Steadman*, 967 F.2d 636, 647 (D.C. Cir. 1992).

13. Among other things, Rule 206(4)-2 requires registered investment advisers that have custody of client funds or securities to have independent public accountants conduct a verification of those client funds and securities by actual examination at least once each calendar year. By failing to have such a surprise examination of these client funds and securities for which it had custody, SagePoint willfully<sup>3</sup> violated Section 206(4) of the Advisers Act and Rule 206(4)-2 thereunder.

### **IV.**

In view of the foregoing, the Commission deems it appropriate, in the public interest, and for the protection of investors to impose the sanctions agreed to in Respondent SagePoint's Offer.

Accordingly, pursuant to Sections 203(e) and 203(k) of the Advisers Act, it is hereby ORDERED that:

A. Respondent SagePoint cease and desist from committing or causing any violations and any future violations of Section 206(4) of the Advisers Act and Rule 206(4)-2 promulgated thereunder.

B. Respondent SagePoint is censured.

C. SagePoint shall, within 10 days of the entry of this Order, pay a civil money penalty in the amount of \$100,000 to the Securities and Exchange Commission for transfer to the general fund of the United States Treasury, subject to Section 21F(g)(3) of the Securities Exchange Act of 1934. If timely payment is not made, additional interest shall accrue pursuant to 31 U.S.C. § 3717.

---

<sup>3</sup> "Willfully," for purposes of imposing relief under Section 203(e) of the Advisers Act, "means no more than that the person charged with the duty knows what he is doing." *Wonsover v. SEC*, 205 F.3d 408, 414 (D.C. Cir. 2000) (quoting *Hughes v. SEC*, 174 F.2d 969, 977 (D.C. Cir. 1949)). There is no requirement that the actor "also be aware that he is violating one of the Rules or Acts." *Tager v. SEC*, 344 F.2d 5, 8 (2d Cir. 1965).

Payment must be made in one of the following ways:

- (1) Respondent may transmit payment electronically to the Commission, which will provide detailed ACH transfer/Fedwire instructions upon request;
- (2) Respondent may make direct payment from a bank account via Pay.gov through the SEC website at <http://www.sec.gov/about/offices/ofm.htm>; or
- (3) Respondent may pay by certified check, bank cashier's check, or United States postal money order, made payable to the Securities and Exchange Commission and hand-delivered or mailed to:

Enterprise Services Center  
Accounts Receivable Branch  
HQ Bldg., Room 181, AMZ 341  
6500 South MacArthur Boulevard  
Oklahoma City, OK 73169

Payments by check or money order must be accompanied by a cover letter identifying SagePoint as a Respondent in these proceedings, and the file number of these proceedings; a copy of the cover letter and check or money order must be sent to Lee A. Greenwood, Assistant Regional Director, Asset Management Unit, Division of Enforcement, Securities and Exchange Commission, New York Regional Office, 100 Pearl Street, Suite 20-100, New York, NY 10004.

D. Amounts ordered to be paid as civil money penalties pursuant to this Order shall be treated as penalties paid to the government for all purposes, including all tax purposes. To preserve the deterrent effect of the civil penalty, Respondent agrees that in any Related Investor Action, it shall not argue that it is entitled to, nor shall it benefit by, offset or reduction of any award of compensatory damages by the amount of any part of Respondent's payment of a civil penalty in this action ("Penalty Offset"). If the court in any Related Investor Action grants such a Penalty Offset, Respondent agrees that it shall, within 30 days after entry of a final order granting the Penalty Offset, notify the Commission's counsel in this action and pay the amount of the Penalty Offset to the Securities and Exchange Commission. Such a payment shall not be deemed an additional civil penalty and shall not be deemed to change the amount of the civil penalty imposed in this proceeding. For purposes of this paragraph, a "Related Investor Action" means a private damages action brought against Respondent by or on behalf of one or more investors based on substantially the same facts as alleged in the Order instituted by the Commission in this proceeding.

By the Commission.

Vanessa A. Countryman  
Secretary

**UNITED STATES OF AMERICA**  
**Before the**  
**SECURITIES AND EXCHANGE COMMISSION**

**INVESTMENT ADVISERS ACT OF 1940**  
**Release No. 6444 / September 28, 2023**

**ADMINISTRATIVE PROCEEDING**  
**File No. 3-21760**

**In the Matter of**

**WOODBURY FINANCIAL  
SERVICES INC.,**

**Respondent.**

**ORDER INSTITUTING ADMINISTRATIVE  
AND CEASE-AND-DESIST PROCEEDINGS,  
PURSUANT TO SECTIONS 203(e) AND  
203(k) OF THE INVESTMENT ADVISERS  
ACT OF 1940, MAKING FINDINGS, AND  
IMPOSING REMEDIAL SANCTIONS AND  
A CEASE-AND-DESIST ORDER**

**I.**

The Securities and Exchange Commission (“Commission”) deems it appropriate and in the public interest that public administrative and cease-and-desist proceedings be, and hereby are, instituted pursuant to Sections 203(e) and 203(k) of the Investment Advisers Act of 1940 (“Advisers Act”) against Woodbury Financial Services, Inc. (“Woodbury” or “Respondent”).

**II.**

In anticipation of the institution of these proceedings, Respondent has submitted an Offer of Settlement (the “Offer”) which the Commission has determined to accept. Solely for the purpose of these proceedings and any other proceedings brought by or on behalf of the Commission, or to which the Commission is a party, and without admitting or denying the findings herein, except as to the Commission’s jurisdiction over Respondent and the subject matter of these proceedings, which are admitted, Respondent consents to the entry of this Order Instituting Administrative and Cease-and-Desist Proceedings, Pursuant to Sections 203(e) and 203(k) of the Investment Advisers Act of 1940, Making Findings, and Imposing Remedial Sanctions and a Cease-and-Desist Order (“Order”), as set forth below.

### III.

On the basis of this Order and Respondent's Offer, the Commission finds<sup>1</sup> that

#### Summary

1. This matter arises out of the failure of Woodbury, a registered investment adviser, to obtain verification by an independent public accountant of client funds and securities of which it had custody. From June 2017 to December 2022 (the "Relevant Period"), Woodbury used a form agreement to govern certain aspects of the relationship among Woodbury, its clients, and a particular clearing agent Woodbury used (the "Clearing Agent"). Each of these agreements ("Customer Agreements") included a margin account agreement that contained language, required by the Clearing Agent, that permitted the Clearing Agent to accept, without inquiry or investigation, any instructions given by Woodbury concerning these clients' accounts (the "Affected Accounts"). As a consequence of Woodbury having this authority with respect to the client funds and securities in the Affected Accounts, Woodbury had custody of these assets. Accordingly, because Woodbury failed to obtain verification by actual examination of the client funds and securities in the Affected Accounts by an independent public accountant, Woodbury violated Section 206(4) of the Advisers Act and Rule 206(4)-2 thereunder, commonly referred to as the "custody rule."

#### Respondent

2. **Woodbury**, a Minnesota corporation with its principal place of business in Oakdale, Minnesota, is a dually registered investment adviser and broker-dealer. Woodbury has been registered with the Commission as an investment adviser since 1997 and as a broker-dealer since 1968. As of December 31, 2022, Woodbury managed approximately \$19.3 billion in regulatory assets under management. Woodbury is a subsidiary of Osaic, Inc. (f/k/a Advisor Group, Inc.), a wholly-owned subsidiary of Osaic Holdings, Inc.

#### Facts

3. The custody rule requires that registered investment advisers who have custody of client funds or securities implement an enumerated set of requirements to prevent the loss, misuse, or misappropriation of those assets.

4. During the Relevant Period, the Clearing Agent served as clearing agent for more than 101,000<sup>2</sup> Woodbury advisory clients' funds and securities under management. Certain aspects of the relationship among these Affected Accounts clients, Woodbury, and the Clearing Agent were governed by the Customer Agreements.

---

<sup>1</sup> The findings herein are made pursuant to Respondent's Offer of Settlement and are not binding on any other person or entity in this or any other proceeding.

<sup>2</sup> As of December 31, 2022.

5. Woodbury included as part of its Customer Agreements a section that served as a margin account agreement, the language for which was required by the Clearing Agent. This section of the Customer Agreements stated, in relevant part:

Until receipt from the Customer of written notice to the contrary, [the Clearing Agent] may accept from Woodbury, without inquiry or investigation, (i) orders for the purchase or sale of securities and other property on margin or otherwise, and (ii) any other instructions concerning said accounts.

6. All of the Customer Agreements included a margin account agreement with the above language during the Relevant Period. As of December 31, 2022, 468 Woodbury advisory clients maintained margin accounts.

7. An investment adviser has custody of client assets if it holds, directly or indirectly, client funds or securities, or if it has the ability to obtain possession of those assets. *See* Rule 206(4)-2(d)(2). Custody includes “[a]ny arrangement . . . under which [an investment advisor is] authorized or permitted to withdraw client funds or securities maintained with a custodian upon [its] instruction to the custodian.” *See* Rule 206(4)-2(d)(2).

8. An investment adviser who has custody of client assets must, among other things: (i) maintain clients’ assets with a qualified custodian; (ii) notify the client in writing of accounts opened by the adviser at a qualified custodian on the client’s behalf; (iii) have a reasonable basis for believing that the qualified custodian sends account statements at least quarterly to clients, except if the client is a limited partnership or limited liability company for which the adviser or a related person is a general partner, the account statements must be sent to each limited partner or member; and (iv) obtain verification of client funds and securities by actual examination each calendar year by an independent public accountant at a time chosen by the accountant without prior notice or announcement to the adviser. *See* Rule 206(4)-2(a).

9. By virtue of Woodbury’s authority under the Customer Agreements described above to give “any other instructions” concerning the Affected Accounts “without inquiry or investigation” by the Clearing Agent, which could include instructions by Woodbury regarding the withdrawal of client funds or securities, Woodbury had custody of the assets in the Affected Accounts under Rule 206(4)-2.

10. With respect to the Affected Accounts, Respondent failed to obtain verification of client funds and securities by annual actual examinations by an independent public accountant for the calendar years 2017 through 2022.

11. In August 2020, in connection with an ongoing examination of Woodbury, the staff of the Commission’s Division of Examinations expressed in writing “concerns” regarding the language contained in the Customer Agreements described above and stated that Woodbury “appeared to have violated the Custody Rule.” In November 2020, Woodbury responded that it believed it was in compliance with the custody rule. On May 18, 2023, Woodbury removed the language described above from its Customer Agreements. In August 2023, Woodbury engaged

an independent public accountant to verify by actual examination the client funds and securities for accounts subject to the Customer Agreements during the calendar year 2023.

### Violations

12. Section 206(4) of the Advisers Act prohibits an investment adviser from engaging in acts, practices or courses of business that are fraudulent, deceptive, or manipulative, as defined by the Commission in rules and regulations promulgated under the statute. Proof of scienter is not required to establish a violation of Section 206(4) of the Advisers Act and the rules thereunder. *See SEC v. Steadman*, 967 F.2d 636, 647 (D.C. Cir. 1992).

13. Among other things, Rule 206(4)-2 requires registered investment advisers that have custody of client funds or securities to have independent public accountants conduct a verification of those client funds and securities by actual examination at least once each calendar year. By failing to have such a surprise examination of these client funds and securities for which it had custody, Woodbury willfully<sup>3</sup> violated Section 206(4) of the Advisers Act and Rule 206(4)-2 thereunder.

### IV.

In view of the foregoing, the Commission deems it appropriate, in the public interest, and for the protection of investors to impose the sanctions agreed to in Respondent Woodbury's Offer.

Accordingly, pursuant to Sections 203(e) and 203(k) of the Advisers Act, it is hereby ORDERED that:

A. Respondent Woodbury cease and desist from committing or causing any violations and any future violations of Section 206(4) of the Advisers Act and Rule 206(4)-2 promulgated thereunder.

B. Respondent Woodbury is censured.

C. Woodbury shall, within 10 days of the entry of this Order, pay a civil money penalty in the amount of \$100,000 to the Securities and Exchange Commission for transfer to the general fund of the United States Treasury, subject to Section 21F(g)(3) of the Securities Exchange Act of 1934. If timely payment is not made, additional interest shall accrue pursuant to 31 U.S.C. § 3717.

---

<sup>3</sup> "Willfully," for purposes of imposing relief under Section 203(e) of the Advisers Act, "means no more than that the person charged with the duty knows what he is doing." *Wonsover v. SEC*, 205 F.3d 408, 414 (D.C. Cir. 2000) (quoting *Hughes v. SEC*, 174 F.2d 969, 977 (D.C. Cir. 1949)). There is no requirement that the actor "also be aware that he is violating one of the Rules or Acts." *Tager v. SEC*, 344 F.2d 5, 8 (2d Cir. 1965).

Payment must be made in one of the following ways:

- (1) Respondent may transmit payment electronically to the Commission, which will provide detailed ACH transfer/Fedwire instructions upon request;
- (2) Respondent may make direct payment from a bank account via Pay.gov through the SEC website at <http://www.sec.gov/about/offices/ofm.htm>; or
- (3) Respondent may pay by certified check, bank cashier's check, or United States postal money order, made payable to the Securities and Exchange Commission and hand-delivered or mailed to:

Enterprise Services Center  
Accounts Receivable Branch  
HQ Bldg., Room 181, AMZ 341  
6500 South MacArthur Boulevard  
Oklahoma City, OK 73169

Payments by check or money order must be accompanied by a cover letter identifying Woodbury as a Respondent in these proceedings, and the file number of these proceedings; a copy of the cover letter and check or money order must be sent to Lee A. Greenwood, Assistant Regional Director, Asset Management Unit, Division of Enforcement, Securities and Exchange Commission, New York Regional Office, 100 Pearl Street, Suite 20-100, New York, NY 10004.

D. Amounts ordered to be paid as civil money penalties pursuant to this Order shall be treated as penalties paid to the government for all purposes, including all tax purposes. To preserve the deterrent effect of the civil penalty, Respondent agrees that in any Related Investor Action, it shall not argue that it is entitled to, nor shall it benefit by, offset or reduction of any award of compensatory damages by the amount of any part of Respondent's payment of a civil penalty in this action ("Penalty Offset"). If the court in any Related Investor Action grants such a Penalty Offset, Respondent agrees that it shall, within 30 days after entry of a final order granting the Penalty Offset, notify the Commission's counsel in this action and pay the amount of the Penalty Offset to the Securities and Exchange Commission. Such a payment shall not be deemed an additional civil penalty and shall not be deemed to change the amount of the civil penalty imposed in this proceeding. For purposes of this paragraph, a "Related Investor Action" means a private damages action brought against Respondent by or on behalf of one or more investors based on substantially the same facts as alleged in the Order instituted by the Commission in this proceeding.

By the Commission.

Vanessa A. Countryman  
Secretary



**2024** / Investment Adviser  
**Compliance Conference**  
MARCH 6-8 / WASHINGTON, DC  
**EFFECTIVE STRATEGIES & BEST PRACTICES**

# Proxy Voting

Adia Finn / GW&K Investment Management  
Ian J. McPheron / Aviva Investors  
Paul Miller / Seward & Kissel LLP  
Mari-Anne Pisarri / Pickard Djinis and Pisarri LLP (MODERATOR)

1



**IAA** 2024 / Investment Adviser  
**Compliance Conference** **EFFECTIVE STRATEGIES & BEST PRACTICES**

# Agenda

- Survey of Legal and Regulatory Requirements
- Proxy Voting and the Compliance Program
- Use of Proxy Advisers
- Hot Topics
  - New N-PX Reporting Requirements
  - ESG Considerations
  - Pass-Thru Voting
  - Votes for Sale

2

**IAA** 2024 Investment Adviser Compliance Conference **EFFECTIVE STRATEGIES & BEST PRACTICES**



## Legal and Regulatory Requirements

Investment Advisers Act of 1940

- Fiduciary Duty
  - Duty of Care
  - Duty of Loyalty
- Proxy Rule
  - Proxy Voting Policies and Procedures
  - Disclosure Requirements

3

3

**IAA** 2024 Investment Adviser Compliance Conference **EFFECTIVE STRATEGIES & BEST PRACTICES**



## Legal and Regulatory Requirements

Investment Advisers Act of 1940

- Compliance Rule
  - Policies and Procedures
  - Annual Review
- Recordkeeping Rule

4

4



## Legal and Regulatory Requirements

### Investment Company Act of 1940

- Policies and Procedures
- Registration Statement Disclosures
- Voting Record Disclosures

5

5



## Legal and Regulatory Requirements

### ERISA

- Fiduciary Duty
  - Exclusive Purpose
  - Prudence
- Investment Duties Regulation

6

6

**IAA** 2024 Investment Adviser Compliance Conference **EFFECTIVE STRATEGIES & BEST PRACTICES**

## Proxy Voting and the Compliance Program

Adopt and Implement Policies and Procedures

- Choose Voting Guidelines in Clients’ Best Interest
  - Determining best interest
  - Benchmark, specialty or custom policies?
- Operational Procedures

7

7

**IAA** 2024 Investment Adviser Compliance Conference **EFFECTIVE STRATEGIES & BEST PRACTICES**

## Proxy Voting and the Compliance Program

Annual Review

- Testing proper application of voting guidelines
- Confirming best interest
- Testing sufficiency and effectiveness of operational procedures
- Testing sufficiency of disclosures

8

8

**IAA** 2024 Investment Adviser Compliance Conference **EFFECTIVE STRATEGIES & BEST PRACTICES**



## Use of Proxy Advisers

Initial Due Diligence

- Adequacy and quality of staffing
- Sources of information
- Transparency of methodology
- Conflict of interest procedures and disclosure
- Safeguarding confidential client information
- Cybersecurity

9

9

**IAA** 2024 Investment Adviser Compliance Conference **EFFECTIVE STRATEGIES & BEST PRACTICES**



## Use of Proxy Advisers

Ongoing Monitoring

- Confirm adequacy of internal controls
- Confirm sufficiency and effectiveness of conflict- of-interest policies
- Confirm selection of voting guidelines
- Spot-test vote recommendations

10

10



## Use of Proxy Advisers

### Other Considerations

- Use of standing voting instructions
- Overriding vote recommendations
- Changing votes already cast

11

11



## Hot Topics: Form N-PX

### Reports by Registered Investment Companies

- Each matter relating to a portfolio security considered at any shareholder meeting held during the reporting period for which the fund was entitled to vote
- Substantially expanded scope of required information beginning with 2024 filing

12

12



## Hot Topics: Form N-PX

### Reports by Institutional Investment Managers

Starting this year, 13F filers must report information about the following types of votes for each security as to which the manager exercised voting power:

- Compensation of named executive officers;
- Frequency of say-on-pay votes; and
- Executive compensation in extraordinary transactions (“golden parachutes”)

13

13



## Hot Topics: Form N-PX

### Terminology

- *Voting power* means the ability to vote or direct voting, including deciding whether to vote and whether to recall loaned securities
- *Exercise voting power* means to use voting power to influence a voting decision with respect to a security

14

14



## Hot Topics: Form N-PX

### Joint Reporting

- Fund reports for investment manager(s)
- Investment manager reports for other manager(s)
- Voting, Notice and Combination Reports

15

15



## Hot Topics: Form N-PX

### Required Information

- The security and shareholder meeting
- The matter voted on (as found on the proxy card)
- Each ballot item's prescribed category
- Whether the issuer or a shareholder proposed the ballot issue (funds only)
- Number of shares voted
- Number of shares loaned and not recalled

16

16



## Hot Topics: Form N-PX

### Required Information, Cont'd.

- How the shares were voted
- Whether the votes were for or against management
- (If applicable) identity of other institutional manager(s) on whose behalf the report is filed
- (If applicable) the fund series

Other information, if it does not interfere with required items

17

17



## Hot Topics: Form N-PX

### Mechanics

- Filed through EDGAR by August 31, covering reporting period ended on June 30
- Initial 13F filer reporting due August 31, 2024, covering votes from July 1, 2023 – June 30, 2024
- Confidential Treatment Requests
- Transition Rules

18

18

**IAA** 2024 Investment Adviser Compliance Conference **EFFECTIVE STRATEGIES & BEST PRACTICES**

## Hot Topics: ESG

Federal Regulatory Treatment

- SEC
- DOL

Red State / Blue State Initiatives

- Public Funds
- Other Investors

19

19

**IAA** 2024 Investment Adviser Compliance Conference **EFFECTIVE STRATEGIES & BEST PRACTICES**

## Hot Topics: ESG

Congressional Initiatives

- Bills to amend Advisers Act and ERISA
- HFSC Republican ESG Working Group

Ex-US Approach

20

20



## Hot Topics: ESG

### Practical Tips

- Disclosure
- Client selection/confirmation of voting guidelines
- Confirmation of state mandates/restrictions
- Testing
- Documentation

21

21



## Hot Topics: Pass-through Voting

Giving ultimate investors a say in proxy votes cast by collective investment vehicles

- Index funds v. actively managed funds
- Separately managed accounts
- Right to dictate votes on a pro-rata ownership basis
- Manager surveys investor preferences but makes ultimate voting decision

22

22

**IAA** 2024 Investment Adviser Compliance Conference **EFFECTIVE STRATEGIES & BEST PRACTICES**

## Hot Topics: Pass-through Voting

**Pros**

- Democratizes proxy voting
- Reduces influence of large managers and proxy advisers
- Reduces influence of ESG
- Promotes ESG

**Cons**

- Operational burdens outweigh customer demand
- Increases influence of proxy advisers

23

23

**IAA** 2024 Investment Adviser Compliance Conference **EFFECTIVE STRATEGIES & BEST PRACTICES**

## Hot Topics: Votes for Sale!

**Decoupling ownership and voting**

- Selling one season’s voting rights
- Allows investors to monetize votes they won’t use
- Opportunity for abuse

24

24



25

## PROXY VOTING:

### The State of Play

by Mari-Anne Pisarri<sup>1</sup>

Pickard Djinis and Pisarri LLP

[mpisarri@pickdjin.com](mailto:mpisarri@pickdjin.com)

Over the past several years, institutional proxy voting has been buffeted by political winds, raising the stakes for investment advisers who provide this critical service. This outline surveys existing legal and regulatory requirements, identifies hot topics, emerging risks and trends, and provides practical compliance tips along the way.

## I. Obligations Under the Investment Advisers Act of 1940

### A. General Fiduciary Duty

A proxy vote is a portfolio asset that must be managed according to the same fiduciary standards that apply to the management of any other portfolio asset.

1. While an adviser cannot disclaim an existing fiduciary duty, the duty arises only where the adviser expressly or implicitly assumes responsibility to vote proxies for, or make voting recommendations to, clients. Even then, the contours of fiduciary duty may be shaped by agreement. For example, the client and adviser may agree that the adviser will vote only on certain matters (e.g., tender offers, contested directorships) or only where the client's shareowning exceeds a stated threshold.

- **Compliance Tip:** If you do not want proxy voting responsibility, say so explicitly in your disclosure brochure and client agreement. Silence could be construed as an implicit assumption of voting authority. (*But see below for special requirements under ERISA.*)
- **Compliance Tip:** Before contractually committing yourself to a variety of voting arrangements, make sure you have an effective way to track and test compliance with those disparate commitments.

---

<sup>1</sup> This outline is intended as a general discussion of contemporary compliance issues. It is not an exhaustive treatment of the topics discussed, nor does it provide legal advice regarding fact-specific issues an investment adviser may face. We would be pleased to answer any questions you may have about these matters.

- **Compliance Tip:** An unrestricted assumption of proxy voting authority does not mean that you are obliged to vote on every single ballot issue. If you determine that the costs outweigh the benefits in voting on a particular matter and you document that determination, you can refrain from voting.
2. The fiduciary duty of care obliges an adviser to vote proxies or make proxy vote recommendations in its clients' best interests.
    - a. This means that votes and recommendations must be consistent with clients' particular investment objectives, time horizons, and specific instructions (if any).
    - b. It also means that the adviser must monitor corporate events and take reasonable steps to avoid basing its voting decisions and recommendations on materially inaccurate or incomplete information.
  - **Compliance Tip:** Not all ballot issues require the same level of analysis to satisfy the duty of care. Consider conducting enhanced analysis for extraordinary events such as mergers and acquisitions, dissolutions, conversions or consolidations or for contentious matters, such as contested director elections, shareholder proposals or environmental, social or corporate governance (ESG) issues.
  3. The fiduciary duty of loyalty prohibits the adviser from subordinating clients' interests to its own.
    - An adviser could violate its duty of loyalty by failing to devote adequate resources to proxy voting or advising or by voting or recommending votes in a manner that directly or indirectly advances the adviser's interests, but not those of the clients.

## B. The Proxy Rule

Advisers Act Rule 206(4)-6 augments the fiduciary duties of care and loyalty with three requirements.

1. An adviser who exercises voting authority over client proxies must adopt written policies and procedures reasonably designed to ensure that the proxies are voted in clients' best interests.
  - a. While adopting a single set of proxy voting guidelines is certainly the easiest approach, that approach may not produce votes that serve each client's best interest. Short-term investors and long-term

investors may have different interests, while labor unions, faith-based organizations and the like may have perspectives on ballot issues that are not shared by other types of investors.

b. Advisers must be especially careful not to adopt voting policies that put their own interests above the interests of their clients.

- The SEC took enforcement action against an adviser who voted all its clients' proxies according to a set of specialty policies the adviser adopted to curry favor with one type of investor, without considering whether those policies served the interests of other investors.

- **Compliance Tip:** Determine whether a single set of proxy voting guidelines advances the interests of all clients. If it does not, either adopt separate guidelines for separate categories of clients or at least separate policies for discrete issues where clients' interests are most likely to diverge.
- **Compliance Tip:** If you adopt multiple sets of proxy voting guidelines, consider letting clients select the guidelines you use to vote proxies on their behalf.
- **Compliance Tip:** While you should generally be mindful of the costs of proxy voting, you are not obliged to conduct a cost-benefit analysis for each vote. In deciding whether to vote on a particular issue, keep in mind that abstaining from voting may also entail costs in the long run.
- **Compliance Tip:** Your proxy voting policies and procedures should address your sources of information and the level of analysis you use for various issues.
- **Compliance Tip:** If you engage in securities lending, your proxy voting policies and procedures should establish a process for determining whether to recall and vote loaned shares.
- **Compliance Tip:** Be careful about oversimplification. Undertaking to "always" vote with management or in favor of shareholder proposals may be incompatible with "always" voting in clients' best interests. The safer course is to leave room for circumstances that might dictate a vote in the opposite direction.

- **Compliance Tip:** Make sure your proxy voting policies and procedures address how you handle material conflicts between your interests and those of your clients.
2. The adviser must describe its proxy voting policies and procedures to clients and provide a copy of same upon request.
    - Item 17 of the Form ADV brochure (Part 2A) directs advisers to disclose whether have authority to vote client proxies. If they do, they must briefly describe their voting policies and procedures; explain how they address conflicts of interest that may arise in connection with proxy voting; explain how clients may receive a copy of the proxy voting policies and procedures; and say whether, and if so, how, a client may direct voting in particular circumstances. (See proposed amendment of Item 17 in the ESG discussion below.)
  3. Finally, the adviser must tell clients how they can obtain information about how their individual shares were voted.
    - a. This information is also required by Item 17 of the ADV brochure.
    - b. Note that new “say-on-pay” disclosure requirements are in effect for the 2024 proxy season. (See discussion of Form N-PX reporting below.)

### C. The Compliance Rule

Proxy voting also implicates Advisers Act Rule 206(4)-7. In addition to adopting and implementing policies and procedures reasonably designed to comply with the Proxy Rule, advisers must also periodically test the sufficiency of those policies and procedures and the effectiveness of their implementation. In this regard, every step of the voting process should be examined.

1. In addition to confirming voting authority and the selection of voting guidelines that are in each client’s best interest, advisers should periodically ensure that they have adequately disclosed their proxy voting practices, including, where applicable, the use of proxy advisers and standing voting instructions. (See discussion of proxy advisers below.)
  - **Compliance Tip:** Keep in mind that client interests may change over time. Make sure your voting guidelines keep pace with your clients’ investment objectives, time horizons and voting instructions (if any). Consider periodically asking clients to confirm their consent to, or selection of, voting guidelines.

2. The adviser should confirm that it has not missed votes and that its voting decisions (including any decisions not to vote) align with applicable voting guidelines, unless there has been a documented decision to deviate from those guidelines.

➤ **Compliance Tip:** It is not necessary to review every vote. Examining votes regarding particularly consequential or contentious issues and reviewing a meaningful sample of other votes should suffice.

3. The adviser should confirm its compliance with proxy voting disclosure and reporting requirements.

➤ **Compliance Tip:** In order to harmonize compliance testing with your firm's natural work flow, consider scheduling your proxy voting review at the end of proxy season or after filing your Form N-PX.

#### D. Recordkeeping

Advisers must maintain the following records relating to proxy voting:

1. Proxy voting policies and procedures;
2. All proxy statements regarding client securities;
3. A record of each vote cast on clients' behalf;
4. Any documents the adviser creates that either are material to making a voting decision or that memorialize the basis for that decision;
5. All written client requests for information on how their proxies were voted and all responses to requests for voting information;

➤ **Compliance Tip:** You may rely on the EDGAR system or service providers (such as proxy advisers) for copies of proxy statements and may rely on service providers to make and maintain records of votes cast.

6. Documentation of the annual review of the sufficiency and effectiveness of compliance procedures relating to proxy voting;

7. Where the adviser engages a proxy adviser or other third party to assist in the proxy voting process, as discussed below, the adviser should maintain:

- a. Contracts with proxy advisers and other proxy service providers;  
and

- b. Documentation of initial due diligence and ongoing monitoring of proxy advisers and other proxy service providers.

## II. Obligations Under the Investment Company Act of 1940

Registered investment companies' proxy voting obligations fall into two categories: adoption and disclosure of policies and procedures and disclosure of voting records.

### A. Policies and Procedures

1. Unless they invest exclusively in non-voting securities, investment companies must describe in their registration statements their voting policies and procedures, including the procedures used when a vote presents a conflict between the interests of the fund's shareholders, on the one hand, and those of the fund's investment adviser, principal underwriter or an affiliated person of the fund, its investment adviser or its principal underwriter, on the other. In the alternative, a fund may simply include a copy of the policies and procedures themselves. Where the fund has delegated voting responsibility to its investment adviser or another third party that uses its own policies and procedures to vote fund securities, the designated party's policies and procedures must be disclosed. [Forms N-1A, N-2, N-3 and N-CSR, 17 CFR 274.11A, 274.11a-1, 274.11b and 274.128, respectively.]

2. Although the content of the required disclosure is not prescribed, the SEC has suggested that funds should disclose both general proxy voting policies and procedures and those that relate to voting on specific types of issues. This could include:

- a. The extent to which the fund delegates its proxy voting decisions to, or relies on the voting recommendations of, a third party;
- b. Policies and procedures regarding issues that may substantially affect shareholder rights and privileges;
- c. Information about the extent to which the fund will support or give weight to the views of a portfolio company's management; and
- d. Information on voting ballot issues regarding corporate governance, changes to capital structure, management compensation, and social and corporate responsibility issues.

### B. Voting Records

1. Company Act Rule 30b1-4 requires funds to file reports each year by August 31<sup>st</sup> detailing their complete proxy voting record for the 12-month

period ending June 30<sup>th</sup> of the reporting year. The reports must be filed on Form N-PX, through the EDGAR system.

2. Form N-PX calls for a range of information for each matter relating to a portfolio security considered at any shareholder meeting held during the reporting period. A substantially expanded version of the Form takes effect on July 1, 2024. (See discussion below.)

### III. Obligations Under ERISA

The Employee Retirement Income Security Act of 1974 (ERISA) imposes additional proxy voting obligations on an adviser who manages a private-sector retirement or employee benefit plan, unless voting authority has been expressly reserved to the plan's named fiduciary or assigned elsewhere. These obligations derive from ERISA's basic fiduciary standards that align, to some extent, with the duties of care and loyalty under the Advisers Act.

#### A. Fiduciary Duty

1. An ERISA fiduciary must discharge its duties solely in the interests of the plan's participants and beneficiaries and for the exclusive purpose of providing benefits to participants and beneficiaries and defraying reasonable expenses of plan administration. [Section 404(a)(1)(A) and 403(c).]

- While the statute does not specify what types of benefits are covered by the "exclusive purpose" standard, the courts and the U.S. Department of Labor (DOL) have confirmed that the benefits must be financial.

2. A fiduciary must also discharge its duties with respect to the plan with the care, skill, prudence and diligence under the prevailing circumstances that a prudent person acting in a like capacity and familiar with such matters would use in the conduct of an enterprise of a like character with like aims. [Section 404(a)(1)(B).]

#### B. The Investment Duties Regulation

1. Over the years, the DOL issued various guidance on the exercise of fiduciary duty in the context of proxy voting. While a common thread ran through this guidance, the tone of each piece reflected the prevailing political winds. As a general matter, Republican administrations have been more skeptical of the value of proxy voting and have taken a more restrictive view of the types of factors a fiduciary may properly consider when casting ballots on behalf of a covered plan. This is especially so when it comes to consideration of ESG factors that are not exclusively financial or economic. By contrast, Democratic administrations have been more favorably inclined toward the exercise of shareholder rights and have taken a broader view of

the factors a fiduciary may consider in formulating its voting decisions and recommendations.

2. In 2020, the DOL amended ERISA's Investment Duties Regulation (Rule 404a-1) to address proxy voting and ESG investing. Among other things, this amendment obliged advisers to vote proxies solely in plans' economic interests, limited the consideration of non-pecuniary factors and imposed new recordkeeping and monitoring requirements. The amendment also created two safe harbors whose practical effect would limit proxy voting by ERISA plans.<sup>2</sup> In addition, the preamble to the 2020 amendment included statements suggesting that even ordinary exercises of shareholder rights might require special justification.

3. In 2022, the DOL unwound the most chilling aspects of the 2020 changes and adopted a more measured approach to proxy voting. As it stands today, Rule 404a-1 restates basic fiduciary principles, imposes specific requirements for meeting those principles, addresses the use of proxy voting policies and confirms the parameters of voting responsibility, scope of coverage and special treatment of pooled investment vehicles.

#### *A. Fundamental Principles*

i. The fiduciary duty to manage plan assets that are shares of stock includes the management of shareholder rights appurtenant to those shares, including the right to vote proxies. [Rule 404a-1(d)(1).]

ii. When deciding if and how to exercise shareholder rights, a fiduciary must act prudently and solely in the interests of participants and beneficiaries and for the exclusive purpose of providing benefits and defraying reasonable expenses. [Rule 404a-1(d)(2)(i).]

#### *b. Specific Requirements*

When deciding whether to exercise shareholder rights and when exercising those rights, a plan fiduciary must:

i. Act solely in accordance with the economic interest of the plan, its participants and its beneficiaries, in a manner

---

<sup>2</sup> The first safe harbor allowed a fiduciary to limit proxy voting to ballot proposals determined to be substantially related to the issuer's business or expected to have a material effect on the value of the plan's investment. The second allowed a fiduciary to refrain from voting whenever the plan's holdings in a subject company relative to the plan's total investment assets are below a certain threshold.

consistent with subsection (b)(4) of the rule [Rule 404a-1(d)(2)(ii)(A)];

- Under subsection (b)(4), the fiduciary must base its determination regarding an investment or investment course of action on factors the fiduciary reasonably determines are relevant to a risk-return analysis, using appropriate investment horizons consistent with the plan's investment objectives, and considering the plan's funding policy. The relevance of any risk-return factor depends on facts and circumstances and may include the economic effects of climate change and other ESG factors. The weight given to any particular factor depends on the fiduciary's assessment of its impact on risk and return.
- ii. Consider any costs involved [Rule 404a-1(d)(2)(ii)(B)];
  - iii. Not subordinate the interests of plan participants and beneficiaries in their retirement income or financial benefits under the plan to any other objective [Rule 404a-1(d)(2)(ii)(I)]; and
  - iv. Evaluate relevant facts that form the basis for any particular proxy vote or other exercise of shareholder rights [Rule 404a-1(d)(2)(ii)(D)].

See below for requirements regarding the use of proxy advisers and other service providers.

#### *c. Proxy Voting Policies*

In deciding whether to vote proxies on behalf of an ERISA plan, a fiduciary may act in accordance with proxy voting policies that establish specific parameters “prudently designed to serve the plan’s [economic] interests” and that are reviewed periodically. The fiduciary may act in a manner contrary to proxy voting policies if it determines that it is prudent to do so after assessing the likelihood that the matter being voted on will have a material effect on the value of the investment or the investment performance of the plan’s portfolio, and after accounting for the costs involved in voting. [Rule 404a-1(d)(3).]

#### *d. Voting Responsibility*

The plan trustee is responsible for exercising shareholder rights on behalf of the plan except to the extent that either:

- i. The trustee is subject to the direction of a named fiduciary pursuant to § 403(a)(1) of ERISA, or
  - ii. The power to manage, acquire or dispose of plan assets has been delegated to one or more investment managers. [Rule 404a-1(d)(4)(i)(A).] In this case, the manager has the exclusive authority to vote proxies or exercise other shareholder rights appurtenant to such plan assets, except to the extent that the plan, trust document or investment management agreement expressly provides that such authority has been reserved to the responsible named fiduciary or assigned elsewhere. [Rule 404a-1(d)(4)(i)(B).]
- **Compliance Tip:** Do not attempt to disclaim responsibility for voting ERISA client proxies without documenting that this responsibility has been properly delegated to someone else.

*e. Scope*

The proxy voting provisions of the Investment Duties Regulation do not apply to voting, tender and similar rights with respect to securities that are passed through to participants and beneficiaries whose accounts hold such securities, pursuant to the terms of an individual account plan. [Rule 404a-1(d)(5).]

*f. Pooled Investment Vehicles*

The manager of a pooled investment vehicle in which multiple plans invest must, “insofar as possible,” reconcile the conflicting investment policies of participating plans, and, if possible, must vote proxies in proportion to the plans’ respective economic interests in the vehicle. In the alternative, the pooled vehicle may adopt a voting policy of its own and require plans to accede to that policy as a condition of investing in the fund. In that case, the fiduciary of each plan must determine that the pooled vehicle’s policy is consistent with Title I of ERISA and the Investment Duties Regulation before deciding to participate in the fund. [Rule 404a-1(d)(4)(ii).]

- **Compliance Tip:** If you want to avoid the onerous process of proportionate voting for a pooled investment vehicle, be sure to adequately disclose your proxy voting guidelines to ERISA plan investors and obtain their consent to those guidelines as a condition of investment.

## IV. The Use of Proxy Advisers and Other Proxy Service Providers

Proxy voting is a resource-intensive activity. One way to make the process more manageable is to engage the assistance of a proxy adviser or other service provider. Outsourced services can assist with the administrative side of proxy voting, including gathering proxy statements, tracking shareholder meetings and ballot issues, and assisting with the mechanics of voting and reporting. Some proxy advisers function as discretionary vote managers, while others provide research, analysis and voting recommendations based either on the proxy adviser's benchmark or specialty voting guidelines (e.g., labor, climate or faith-based policies) or on the investment manager's own custom voting guidelines. While proxy advisers and other service providers can assist investment managers in meeting their proxy voting obligations, the use of such services has compliance implications.

A. An adviser is not relieved of its fiduciary duties simply because it hires another party to perform an advisory function. In the proxy voting context, this means that an adviser cannot outsource its fiduciary voting obligations to a proxy adviser or other service provider. In fact, the engagement of a proxy adviser or other service provider is itself a fiduciary act requiring the exercise of care and loyalty.

B. Before contracting with a proxy adviser or administrative proxy service, an investment adviser must conduct sufficient due diligence to determine that the proposed engagement is in the best interests of the manager's clients. Due diligence should include a reasonable inquiry into:

1. The adequacy and quality of the service provider's staffing and technology;
2. The service provider's cybersecurity hygiene;
3. The manner in which the proxy adviser formulates its proxy voting guidelines, the sources of information it uses, its engagement with issuers and third parties and its data integrity, quality control and error correction practices;
4. The proxy adviser's mechanisms for alerting clients about changes in vote recommendations based on the receipt of additional information, including information from issuers and shareholder proponents;
5. The independence of the proxy adviser's vote recommendations, which requires an understanding of the proxy adviser's business and the nature of conflicts of interest that business presents;

6. The sufficiency of the proxy adviser's conflict of interest policies and procedures;

7. The sufficiency of the proxy adviser's disclosure practices regarding its relationships with issuers, shareholder proponents and other parties with an interest in the subject proxy votes, and the ease of accessing such disclosure; and

8. Proxy advisers' and administrative voting services' treatment of material non-public information about clients' portfolio holdings and how the investment manager intends to vote client proxies.

C. The proxy service engagement process should include an exit strategy. This includes ensuring that upon termination of a service contract, sensitive client and adviser data will be appropriately safeguarded or destroyed. It also includes ensuring continued access to required books and records maintained by the terminated service provider.

D. Once outsourced proxy voting assistance is procured, the adviser must continue to monitor the service provider's integrity and competence, which might change over time. Ongoing monitoring might include:

1. Receiving periodic certifications of the service provider's compliance with its internal policies and procedures, including policies and procedures regarding conflicts of interest;

2. Receiving notification of material changes to information previously supplied; and/or

3. Periodic meetings with key personnel.

E. The adviser must also monitor a proxy adviser's vote recommendations to reasonably ensure that they are in clients' best interests. The adviser does not have to flyspeck every bit of advice it receives, but it cannot disengage from the voting process and blindly follow the proxy adviser's recommendations.

➤ **Compliance Tip:** If you use standing voting instructions on a proxy adviser's automated voting platform, protect yourself against charges of "robo-voting"<sup>3</sup> by:

---

<sup>3</sup> "Robo-voting" is a pejorative term used by some issuers, their spokesfolks and politicians of a certain persuasion to describe a situation in which an institutional investor blindly follows a proxy adviser's vote recommendations.

- Reviewing a sample of pre-populated votes on routine ballot issues to confirm the votes align with the applicable voting guidelines; and
- Conducting a more thorough analysis of the proxy adviser's vote recommendations regarding novel or highly contentious issues to confirm that the recommendations align with clients' best interests.

Depending on what you find, consider whether you should override the proxy adviser's vote recommendation.

- **Compliance Tip:** If, after you cast a vote, you become aware of additional material information about a ballot issue, consider whether you should change your vote, if possible.
- **Compliance Tip:** If you select a proxy adviser's benchmark or specialty voting policies, be sure to stay on top of changes to those policies to ensure that they continue to serve the best interests of your clients.

F. The ERISA Investment Duties Regulation also addresses the use of outsourced proxy voting services.

1. An ERISA fiduciary must exercise prudence and diligence in the selection and monitoring of persons, if any, selected to advise or otherwise assist with exercises of shareholder rights. This includes research providers, proxy advisers and those who provide administrative, recordkeeping or reporting services. [Rule 404a-1(d)(2)(ii)(E).]
2. A fiduciary may not adopt a practice of following the recommendations of a proxy adviser or other service provider without determining that the voting guidelines of such party are consistent with the fiduciary's obligations described in Rule 404a-1(d)(2)(ii)(A) through (E). [Rule 404a-1(d)(2)(iii).]

## V. Hot Topics, Emerging Risks and Trends

### A. Form N-PX Reporting

Beginning in 2024, institutional investment managers who are required to file reports under Securities and Exchange Act of 1934 (Exchange Act) Rule 13f-1 must annually report their precatory say-on-pay proxy votes using the same Form

N-PX that registered investment companies use to report their entire voting records.<sup>4</sup>

### 1. *New Requirement for Investment Managers*

Exchange Act Rule 14Ad-1 requires an institutional investment manager to report information about the following types of votes for each security as to which the manager exercised voting power:

- a. Votes to approve the compensation of named executive officers;
- b. Votes to determine the frequency of such votes (*i.e.*, every 1, 2 or 3 years); and
- c. Votes to approve executive compensation in extraordinary transactions (*i.e.*, “golden parachute” compensation in connection with mergers or acquisitions).

### 2. *Terminology*

a. An “institutional investment manager” includes an investment adviser who invests in securities on its clients’ behalf. [Exchange Act § 13(f)(6)(A).]

- Note that off-shore 13F filers are also subject to the new N-PX requirements.

b. “Voting power” means “the ability, through any contract, arrangement, understanding, or relationship, to vote a security or direct the voting of a security, including the ability to determine whether to vote a security or to recall a loaned security.” [Rule 14Ad-1(d)(1).]

c. The “exercise” of voting power means the use of voting power “to influence a voting decision with respect to a security.” [Rule 14Ad-1(d)(2).] An investment manager may exercise voting power by voting or by influencing a vote using its own independent judgment.

- Although common sense would dictate that advisers who expressly disclaim voting authority in their advisory agreements or Form ADV should not be subject to the N-PX filing requirement, the SEC rejected the common-sense approach. Investment managers who have no authority to

---

<sup>4</sup> Section 951 of the Dodd-Frank Act added a new Section 14A to the Exchange Act to require public companies to hold non-binding shareholder advisory votes relating to certain executive compensation issues. Section 14A(d) requires public reporting of such votes. As noted above, fund reporting obligations derive from Company Act Rule 30b1-4.

vote client proxies, and, in fact, do not vote, are nevertheless obliged to file an annual Form N-PX “Notice Report” to confirm they have nothing to report. A Notice Report is also filed where the manager has, but did not exercise, voting authority for any say-on-pay ballot issue during the reporting period.

- **Compliance Tip:** Determining whether an investment manager “exercises” proxy voting authority is not an intuitive process. For example, a manager who votes in accordance with its own voting guidelines is deemed to exercise voting power, even where the client has selected those guidelines, while a manager who votes according to a client’s say-on-pay guidelines is not, unless the manager exercises its own judgment in applying the client’s guidelines. The proposing release regarding the new N-PX requirements offers examples of what the SEC deems to be the exercise of voting authority. [Exchange Act Rel. No. 93169, Company Act Rel. No. 34389 (Sep. 29, 2021) at 21-25.] Do your best, and at least make sure you take a consistent approach in what you report.

### *3. Joint Reporting*

In light of the broad interpretation of “exercising” voting power, more than one investment manager will sometimes have reporting obligations for the same vote. In such cases, the managers may jointly report the subject votes, with one manager filing a “Voting Report” on Form N-PX that contains the required vote information and the other manager(s) filing a “Notice” Report” on Form N-PX omitting that information. An institutional manager who reports some of its own votes and relies on other manager(s) or fund(s) to report other votes would file a “Combination Report” on Form N-PX.

- a. Where two or more managers jointly report say-on-pay votes for the same securities, the manager that files the N-PX Voting Report must identify the other manager(s) on whose behalf the filing is made. Each non-reporting manager must file an N-PX Notice Report identifying each manager reporting on its behalf.
- b. A manager is not required to report proxy votes that are reported on a Form N-PX filed by a registered investment company. The fund must identify each manager on whose behalf it is reporting votes and each manager must file a Notice Report identifying the fund that is reporting the manager’s votes.

c. Affiliated institutional investment managers may jointly file a single Form N-PX even if the managers do not exercise voting power over the same securities.

d. The number of shares being reported on behalf of another manager must be reported separately from the number of shares the reporting manager reports on its own behalf. Furthermore, where the reporting manager reports for different groups of managers, each group's shares must be reported separately. Likewise, a fund must separately report shares that are reported on behalf of different managers or groups of managers. If the fund offers multiple series, it must report each one's voting record separately.

e. Note that while joint reporting by institutional investment managers is *permitted*, it is not *required*. Where multiple managers exercise voting authority over the same securities, each manager may file its own N-PX Voting Report with the required information. In that case, there is no need to cross-reference the other managers who report the same votes.

#### 4. *Scope and Content*

a. Although the say-on-pay reporting requirement applies only to managers subject to Section 13(f) of the Exchange Act, the Commission declined to harmonize the scope of the N-PX and 13F reporting requirements. For example, the N-PX requirements are not limited to the kinds of securities managers report on 13F; N-PX does not include 13F's *de minimis* exemption for securities holdings of fewer than 10,000 shares and less than \$200,000 aggregate fair market value; and a manager may be required to report votes on Form N-PX for securities it omits from Form 13F because it does not have investment discretion over them.

b. Form N-PX consists of a Cover Page, a Summary Page, a Proxy Voting Record and a signature block.

i. The Cover Page identifies the institutional investment manager or fund filing the Form N-PX and type of report being filed (Voting, Notice or Combination); indicates whether an investment manager requests confidential treatment regarding one or more votes that are omitted from the report (see discussion below); and, if applicable, identifies other persons reporting for the filing manager.

ii. The Summary Page identifies the institutional managers whose votes are being included on this filing (other than the

filing manager or fund), if any. For reports filed by a fund, the Summary Page also includes information about individual series of that fund, if any.

iii. For investment managers, the Proxy Voting Record lists the information that must be disclosed for each shareholder vote over which the manager exercised voting power during the reporting period. For funds, it itemizes the information required for each matter relating to a portfolio security considered at any shareholder meeting held during the reporting period for which the fund was entitled to vote. In addition to identifying the security and shareholder meeting in question, the reporting manager or fund must identify and categorize the matter being voted on. Form N-PX includes a list of ballot categories to choose from. For institutional managers, the relevant category is “Section 14A say-on-pay votes.” Fund reporting covers a much broader range of topics, including: director elections, say-on-pay matters, audit-related issues, investment company matters, shareholder rights and defenses, extraordinary transactions, capital structure, compensation issues other than say-on-pay, corporate governance, environment or climate, human rights or human capital/workforce, diversity, equity and inclusion (DEI), other social issues and other matters.

- **Compliance Tip:** In identifying the matters voted on, you must use the same language, in the same order, as that found on the issuer’s proxy card. If there is no proxy card (e.g., the vote is not subject to U.S. proxy rules), you must briefly identify the matter voted on, taking care not to use unfamiliar abbreviations.

iv. In addition to the foregoing, the voting record must include the following information:

(a) For fund reports, whether the ballot item was proposed by the issuer or a security holder:

(b) The number of shares voted;

- **Compliance Tip:** You may use the number of voted shares reflected in your records at the time of filing. If you have not received confirmation of actual votes cast by the time you file, you may report the number of

shares you instructed to be cast. Indicate “0,” if no shares were voted.

(c) The number of shares that the reporting person loaned (directly or indirectly through a voting agent) and did not recall;

(d) How the shares were voted (for, against, withhold, or abstain), and if votes were cast in multiple directions, the number of shares voted each way;

(e) Whether the disclosed votes represented votes for or against management’s recommendation;

➤ **Compliance Tip:** If there was no management recommendation, state “None” for this item.

(f) If applicable, the identity of each institutional manager on whose behalf the voting report is being filed (other than the person filing this report);

(g) If applicable, the fund series that was eligible to vote the security; and

(h) Any other information the reporting person would like to provide about the matter or how it voted, provided that such other information does not impede the understanding or presentation of the required information.

### *5. The Mechanics of Reporting*

Form N-PX reports must be filed electronically through the EDGAR system, no later than August 31<sup>st</sup> of each year for the most recent 12-month period ending on June 30,<sup>th</sup> except as discussed in the Transition Rules section below.

➤ **Compliance Tip:** The initial reports on the new version of Form N-PX are due by August 31, 2024, covering the period of July 1, 2023 to June 30, 2024.

### *6. Requesting Confidential Treatment*

Investment managers may request confidential treatment of their proxy voting information in the same manner and subject to the same standards that apply to confidential treatment requests under Exchange Act § 13(f), and consistent with Exchange Act Rule 24b-2. Requests for confidential treatment must be filed electronically, through EDGAR.

1. Confidential treatment may be justified to protect information that is the subject of a pending or granted 13F confidential treatment request. Confidentiality would not be justified, however, simply because the manager has a nondisclosure agreement with a client regarding portfolio information. An investment manager requesting confidential treatment must provide enough factual support for its request to enable the SEC to make an informed judgment as to the request's merits. [Form N-PX, Instructions for Confidential Treatment Requests, Instruction 5.]

2. Confidential treatment of proxy voting information may not extend beyond one (1) year from the date that the Form N-PX report is required to be filed. Except in extraordinary circumstances, within six (6) business days of the expiration of the period for which the SEC has granted confidential treatment (or of the notification of the SEC's denial of a confidentiality request), the manager must file an N-PX amendment reporting the subject information, with a mandatory legend identifying the reason for the filing. [*Id.*, Instructions 6 - 8.]

## 7. Transition Rules

- a. A Form N-PX need not be filed for the 12-month period ending June 30<sup>th</sup> of the calendar year in which the manager's initial Form 13F filing is due.
- b. Nor must an N-PX be filed with respect to any shareholder vote at a meeting that occurs after September 30<sup>th</sup> of the calendar year in which the manager's final Form 13F filing is due. In that case, the manager must file an N-PX for the stub period of July 1<sup>st</sup> – September 30<sup>th</sup> by March 1<sup>st</sup> of the following calendar year.

## B. The Outsourcing Rule Proposal

Proposed Advisers Act Rule 206(4)-11 would impose a series of prescriptive requirements on an adviser's selection and monitoring of both affiliated and unaffiliated service providers, including proxy voting services. The proposal would also impose extensive new recordkeeping and disclosure requirements on advisers relating to outsourcing. Among other things, an adviser would be obliged to obtain each service provider's reasonable assurance that it can and will coordinate with the adviser for purposes of the adviser's legal and regulatory compliance. Moreover, service providers who create and/or maintain books and records for an investment adviser would be obliged to do so in a manner that satisfies the Advisers Act recordkeeping rule.

## C. ESG

ESG has become the blue touch paper of investment management and, by extension, of proxy voting. Although there is no universally accepted definition of the term, there

are plenty of strong and divergent opinions on the proper role of environmental, social or corporate governance factors in fiduciary investment management. The best way for an investment adviser to keep from getting scorched is to thoughtfully design and implement an approach to ESG, clearly disclose that approach to clients, and keep good records.

### *1. The Federal Regulatory Approach*

For the moment, the SEC and the DOL are taking an even-handed approach to ESG, recognizing that such factors may have economic consequences or may otherwise be considered in a manner consistent with the fiduciary duties of care, loyalty and prudence.

a. In 2022, the SEC proposed new disclosure requirements for investment advisers and registered investment companies relating to their ESG investment practices. In light of increased investor demand for ESG investment strategies, the proposed requirements are “designed to create a consistent, comparable, and decision-useful regulatory framework for ESG advisory services.” [Advisers Act Rel. No. 6034 (May 25, 2022).] As it relates to proxy voting, the proposal:

i. Would amend Item 17.A of the Form ADV disclosure brochure to require advisers that have specific voting policies or procedures that include one or more ESG considerations when voting client securities to include a description of which ESG factors they consider and how they consider them. Where the adviser maintains different ESG-relevant proxy policies for different strategies or clients, those differences would have to be described. Advisers also would have to disclose whether they allow clients to direct their own votes on ESG-related voting matters.

ii. Would amend Forms N-1A and N-2 to require layered disclosure of a registered investment company’s practices regarding the incorporation of ESG considerations in proxy voting and other shareholder engagement. [Proposed Item 4(a)(2)(ii)(B), Instruction 4 of Form N-1A and Proposed Item 8.e.(2)(B), Instruction 4 of Form N-2.]

b. As noted above, Form N-PX now requires investment companies to make granular disclosure of proxy votes on ESG ballot items relating to the environment or climate, human rights, DEI and other social and governance issues.

c. With the repeal of the Trump-era version of the ERISA Investment Duties Regulation, the DOL has also adopted a neutral stance on ESG.

As discussed above, an ERISA fiduciary must base its proxy vote determinations on factors the fiduciary reasonably determines are relevant to a risk-return analysis, which may include the economic effects of climate change and other ESG factors. [Rule 404a-1(d)(2)(ii)(A).]

## 2. *State Initiatives*

State approaches to the ESG implications of proxy voting can be classified as red or blue.

a. *State Retirement Plans and Other Public Funds.* Some states forbid the consideration of ESG factors in the investment process for public funds, while other states require or permit the consideration of such factors if they are material. Some states prohibit investment in, or require divestment from, fossil fuel companies or weapons manufacturers, while other states prohibit such practices or even boycott financial services firms that adopt disfavored practices on hot-button issues like climate or gun control. These restrictions and mandates can be baked into law or made part of the state's investment or proxy voting policy statement or custom voting guidelines.

b. *All Investors.* Some red states have turned to antitrust or blue sky laws to attack ESG practices more broadly. For example, Missouri has adopted a blue-sky rule requiring state registered advisers and state-registered investment adviser representatives (IA Reps) of federally registered advisers to make disclosure to clients and receive written consent prior to incorporating ESG factors into investment decisions. This rule is being challenged in court, but is effective while the litigation proceeds.

c. *Additional Tactics.* In addition to laws, rules and investment or voting policy statements, some states are using investigations, subpoenas, letters from groups of like-minded attorneys general and similar tactics to discourage ESG investing or intimidate financial service providers who are perceived to be "woke."

## 3. *Congressional Initiatives*

Congressional Republicans have launched a number of missiles at ESG. These include bills to amend the Advisers Act and ERISA to restrict the use of non-pecuniary factors in investment decision-making; the House Financial Services Committee's formation of a Republican ESG Working Group; and an investigation by the House Judiciary Committee into the antitrust implications of allegedly collusive agreements to "promote ESG goals." Given the

unbridgeable political divide on the Hill, none of these efforts has been productive, but the ongoing threat to advisers cannot be ignored.

#### *4. International Initiatives*

The attitude toward ESG outside the United States is dramatically different than it is here. In Europe and elsewhere, investment managers are encouraged or required to incorporate ESG considerations into their investment practices. Advisers serving non-U.S. clients may be directed to comply with the United Nations Principles for Responsible Investment (U.N. PRI), national stewardship codes or other investment or proxy voting standards that are anathema to some politicians and regulators in the U.S.

- **Compliance Tip:** Regardless of your views on ESG, you must be mindful of the risks these considerations pose to your business. One way to manage risk is to document a reasoned process for determining if and when ESG factors have an economic consequence and if and when they may otherwise be relevant to an investment decision, including a decision regarding proxy votes. Effectively disclose this process to clients and consider obtaining client consent in the investment management agreement or otherwise.
- **Compliance Tip:** Be vigilant with public employee retirement plans or other public funds. If such clients do not supply custom voting policies, make sure you understand all constraints and mandates the applicable state may have imposed on the consideration of ESG factors. These requirements are moving targets, so make sure you stay on top of legislative and regulatory developments.
- **Compliance Tip:** Don't forget that NSMIA (the National Securities Markets Improvement Act of 1996) prohibits states from imposing substantive securities law regulation on federally registered investment advisers and their supervised persons. This means that the states are forbidden to regulate federal advisers' and their IA Reps' consideration of ESG factors in voting client proxies. As noted above, one state's attempt to exercise jurisdiction it does not have is currently being litigated.
- **Compliance Tip:** Wildly divergent attitudes toward ESG may make it challenging to use only one set of proxy voting guidelines for all clients. Consider selecting different policies to meet different client needs, or, if you use a single set of guidelines,

consider making room for different approaches to ballot items that include ESG considerations. You might also consider giving clients the right to direct their votes on ESG matters or to vote these matters themselves.

- **Compliance Tip:** If you use the services of a proxy adviser, make sure you select voting guidelines that align with each client's interests. If you use standing instructions on an electronic proxy voting platform, consider either reserving the right to manually vote ESG ballot items or at least review the vote recommendations for those items before the votes are cast.
- **Compliance Tip:** Pay special attention to ESG issues when conducting your compliance reviews of proxy voting. Among other things, make sure you have complied with client's specific voting instructions and otherwise have satisfied whatever obligations you have assumed regarding votes that entail ESG considerations.
- **Compliance Tip:** Accept the fact that it may not be possible to keep everyone happy. Complying with one state's divestment mandates may violate another state's anti-boycott mandates. As unpalatable as it may seem, sometimes the wiser course is to stay out of the political cross-fire and turn risky business away.

#### D. Pass-Through Voting

Pass-through voting is a mechanism by which investors in a mutual fund or other pooled investment vehicle are given in say in how the proxies of the pooled funds' portfolio securities are voted.

1. As noted above, registered investment companies disclose their proxy voting policies and procedures in their registration statements and file annual reports of their voting records so investors can consider this information in making investment decisions. Under ERISA, managers of pooled investment vehicles that hold assets of more than one employee benefit plan must, to the extent permitted by law, vote proxies in proportion to the participating plans' respective economic interests in the vehicle, unless accession to the pooled vehicle's own proxy policies is made a condition to investment. Pass-through voting is a way to give investors more direct control over the proxy voting decisions made on their behalf.
2. Clients with separately managed accounts (SMAs) already have pass-through voting rights. Because they own the securities in their accounts, they also own the right to vote proxies for those securities. They can

exercise this right either by opting to vote their own proxies, by selecting the proxy voting guidelines their adviser uses, or by directing votes on particular types of issues, if their adviser permits. That said, the technology being developed to enable pass-through voting for collective vehicles may make it easier to give SMA clients a greater say in how their votes are cast without making them assume responsibility for their proxy voting altogether.

3. Pass-through voting comes in many flavors. In some cases, it is limited to institutional investors, while in other cases it is made available to retail investors as well. It is typically used for index funds or other passive investment vehicles but can also be used for other types of collective vehicles. It can afford investors the right to dictate votes on a pro-rata ownership basis, or can be a “softer” process, in which the manager surveys investors to get a sense of their preferences on a range of core proxy issues but continues to exert ultimate decision-making authority over the vote. Where investors dictate proxy votes for a proportionate share of the collective vehicle, they may use their own voting guidelines or may direct the use of a proxy adviser’s benchmark or specialty voting policies or their manager’s custom voting policies.

4. Proponents of the practice fall at both ends of the political spectrum, although the reasons for their support are certainly not aligned. The perceived benefits of pass-through voting (depending on one’s perspective) include:

- a. Democratization of shareholder voting by allowing asset managers’ votes to more accurately reflect their clients’ views;
- b. Improved transparency in fund corporate governance;
- c. Reducing the hegemony of the largest institutional investment managers and the influence of proxy advisers and their perceived liberal biases;
- d. Minimizing the influence of ESG factors on voting decisions; and
- e. Facilitating “values” voting, including the promotion of ESG principles.

5. Of course, not everyone is a fan of this practice. The perceived drawbacks of pass-through voting include:

- a. High implementation costs that exceed likely benefits;
  - Skeptics note that, left to their own devices, few retail investors vote their proxies or demonstrate any interest in doing so. Indeed, many individual investors buy mutual

funds and ETFs precisely because they do not want to be bothered with the details of managing their assets.

- Ironically, the individual investors who are most likely to avail themselves of pass-through voting are the ones who care most about sustainability, climate and DEI.

b. A more difficult and costly investor relations process;

- If a large number of investors want a say in how their proxies are voted, issuers may have to undertake more individual shareholder engagements.

c. Increased influence of proxy advisers; and

- In order to make pass-through voting operationally feasible, many pass-through investors will use standing voting instructions based on proxy advisers' benchmark or specialty policies.

d. Risk of missed votes or inability to get a quorum for shareholder meetings.

- Proxy voting is already a race against the clock due to the compressed nature of proxy season. Adding more steps to the process will make it harder for the adviser to meet voting deadlines.

6. The future of pass-through voting is difficult to predict. Today, it is more popular in Europe than in the U.S., but that could change if the pilot programs by the largest asset managers prove popular and if advances in technology reduce the cost and operational burdens of the process. Or, the politicians could intervene. In 2022, Senate Republicans introduced a bill (S. 4241, the "INDEX Act,") to amend the Advisers Act to require advisers of passively managed funds and SMAs to arrange for pass-through voting under certain circumstances. The bill went nowhere, but it could be resurrected and take flight, depending on which way the political winds blow.

- **Compliance Tip:** Given the political climate, it may be wise to solicit some form of client input regarding proxy voting, even if you do not want to shoulder the burdens of full pass-through voting. Consider adding an acknowledgement or direction of the applicable proxy voting guidelines to your advisory agreement, or

some questions about voting preferences (at least with regard to ESG) to the client's investment policy statement.

- **Compliance Tip:** Certain proxy advisers are offering pass-through voting assistance to institutional clients. If you want to provide this option to your clients without assuming all the attendant operational burdens, you may be able to outsource at least part of the process.

### E. Votes for Sale

Another idea that promises to disrupt traditional notions of proxy voting is to allow investors to sell their proxy voting rights, while retaining ownership of the securities generating those rights. At least one company has created a marketplace for this purpose. [Alexander Osipovich, *Votes for Sale! A Startup is Letting Shareholders Sell Their Proxies*, WALL ST. J. (Jan. 21, 2024), <https://www.wsj.com/finance/stocks/buy-my-vote-a-startup-is-letting-shareholders-sell-their-proxies-122f0eb9>.]

The upside to this idea is that it allows individual investors to monetize voting rights they are otherwise unlikely to use. The downside is . . . everything else. Decoupling voting rights from share ownership is a risky endeavor that a fiduciary should approach with an abundance of caution.

# 2024 / Investment Adviser Compliance Conference

MARCH 6-8 / WASHINGTON, DC

EFFECTIVE STRATEGIES & BEST PRACTICES

## Ethics for Advisers: Compliance with Fiduciary Standards – Part 2

Steve Farmer / Confluence Investment Management

Caroline P. Jankowski / Operose Advisors LLC

Robert Saperstein / Guggenheim Investments

Stephanie Avakian / WilmerHale (Moderator)

1

1



2024 / Investment Adviser  
Compliance Conference

EFFECTIVE STRATEGIES  
& BEST PRACTICES

### Panel Agenda

- Protection of material nonpublic information (MNPI) and prevention of insider trading
- Whistleblower considerations
- Best practices

2

2



## Insider Trading

- What is it?
- What is MNPI?
- What regulations apply?
  - Advisers Act Section 204A, Rule 204A-1
    - Written policies and procedures to protect MNPI
    - Code of ethics
  - Exchange Act Section 10(b), Rule 10b-5
- Enforcement developments
- Exams

3

3



## MNPI Considerations

### Best Practices:

- Robust policies that are tailored to your business
- Easy to understand and easy to remember
- Give Examples
- Training
  - Initial
  - Annual

### Additional Strategies:

- Barriers
- Restricted Lists
- Testing and Surveillance

4

4



## Hypothetical

ABC Securities, an affiliate of our firm in a different information barrier, contacted one of our Portfolio Managers (PM) on a no-names basis to see if our firm had an interest in participating in a refinancing opportunity. ABC Securities knew from Bloomberg that the firm is an existing lender.

5

5



## Hypothetical

As a compliance professional, you learn that one of your PMs has inadvertently disclosed non-public information to select investors.

6

6



## Whistleblower Considerations

- SEC Whistleblower Program
- Internal reporting / responding to reports
- Enforcement developments
- Rule 21F-17 considerations – confidentiality provisions
  - Separation / employment agreements
  - Code of conduct

7

7



## Whistleblower Considerations

### Best Practices

- Reporting process
- Response process
- Anti-retaliation / protection of confidentiality
- Communication
- Review agreements with confidentiality provisions

8

8



## Hypothetical

- Refer back to the earlier scenario regarding the distribution of MNPI.
- A new junior member of the PM team stops a member of the Compliance Department in the hall and mentions that he thinks a senior PM has been sharing MNPI with investors. As a junior member, the reporting individual is concerned about hurting his standing on the team by reporting the senior individual to Compliance.

9

9



## Hypothetical

As Chief Compliance Officer, the initial report in our fact pattern was presented to you and you delegated the matter to your deputy to investigate. Your deputy quickly responds that the matter will be investigated. However, after several weeks, you still have not received an update about how the deputy's investigation is going.

10

10



11