Simpson Thacher

Regulatory and Enforcement Alert

SEC Risk Alert Highlights COVID-19 Compliance Risks and Considerations for Investment Advisers and Broker-Dealers

August 14, 2020

The Office of Compliance Inspections and Examinations ("OCIE") of the U.S. Securities and Exchange Commission ("SEC") recently published a Risk Alert (the "Risk Alert")[1] highlighting certain COVID-19-related issues, risks, and practices relevant to SEC-registered investment advisers and broker-dealers (collectively, "Firms"). The Risk Alert, which is the result of ongoing outreach with Firms undertaken by OCIE in its effort to assess the impact of COVID-19, provides OCIE's summaries and observations in the following areas: (i) protection of investors' assets; (ii) supervision of personnel; (iii) practices relating to fees, expenses, and financial transactions; (iv) investment fraud; (v) business continuity; and (vi) protection of investor and other sensitive information. Below is a summary of the observations and recommendations identified in the Risk Alert and some key takeaways for Firms.

Key Takeaways

- The Risk Alert provides a helpful outline of potential COVID-19-related risks and challenges. Firms should consider whether enhancements to their compliance programs may be needed to address those risks and challenges. With a potentially long-term shift to a remote work environment, for example, a Firm's oversight of its employees face new challenges. Firms may wish to consider enhancements to their supervisory policies and procedures, including monitoring of communications or transactions. This is particularly apt if employees are using personal devices instead of Firm-issued equipment.
- A key theme of the Risk Alert is that as business activities and practices evolve in response to COVID-19 (and, by extension, other events), compliance policies and procedures should evolve with them. Given the increased use of videoconferencing, for example, OCIE suggests that Firms assess their policies and procedures regarding the sharing of sensitive information via unsecure web-based video chat. The Risk Alert also identifies cybersecurity and business continuity planning as key risks in the COVID-19 era, and identifies policy enhancements that Firms should consider in these areas.
- OCIE contemplates that Firms might face increased financial pressures to compensate for lost revenue in the current environment. Firms should continue to vigilantly review their fee and expense calculations as well as related policies and investor disclosures to ensure that fees and expenses are calculated and

[1] *Select COVID-19 Compliance Risks and Considerations for Broker-Dealers and Investment Advisers*, Risk Alert, SEC OCIE (August 12, 2020).

allocated in accordance with such policies and disclosures. Similarly, due to the potential for increased pressure on Firms to maintain positive valuations, especially private fund sponsors that are raising new funds, Firms should consider enhancing their compliance monitoring of valuations and ensure valuations are consistent with stated valuation policies and procedures.

Protection of Investor Assets

Firms have a responsibility to ensure the safety of their investors' assets and to guard against theft, loss, and misappropriation. OCIE staff has observed that some Firms have modified their normal operating practices regarding collecting and processing investor checks and transfer requests. OCIE provides the following recommendations:

- Firms are encouraged to review their practices, and make adjustments, where appropriate, including in situations where investors mail checks to Firms and Firms are not picking up their mail daily. Firms may consider, for example, disclosing to investors that checks or assets mailed to the Firm's office location may experience delays in processing until personnel are able to access deliveries at that office location.[2]
- OCIE also encourages Firms to review and make any necessary changes to their policies and procedures around disbursements to investors, including where investors are taking unusual or unscheduled withdrawals from their accounts, particularly COVID-19-related distributions from their retirement accounts. In particular, Firms may want to consider implementing additional steps to validate the identity of the investor and the authenticity of disbursement instructions, including whether the person is authorized to make the request and the accuracy of bank account names and numbers.[3]

Supervision of Personnel

Firms have an obligation to supervise their personnel, which includes overseeing supervised persons' investment and trading activities.[4] As Firms make significant changes to respond to COVID-19—such as shifting to Firm-wide telework conducted from dispersed remote locations, dealing with significant market volatility and related issues, and responding to operational, technological, and other challenges—OCIE encourages Firms to closely review and, where appropriate, modify their supervisory and compliance policies and procedures.

For example, OCIE staff suggests that Firms consider modifying their practices to address:

---

[2] Investment advisers and certain broker-dealers have an obligation to promptly transmit investor checks. *See* Investment Advisers Act of 1940 ("Advisers Act") Rule 206(4)-2 and Exchange Act 15c3-3-(k)(2), respectively.

[3] OCIE also suggests that Firms consider recommending that each investor identify a trusted contact person, particularly for seniors and other vulnerable investors.

[4] Advisers Act Rule 206(4)-7 (the "Compliance Rule") requires SEC-registered investment advisers to adopt and implement written policies and procedures that are reasonably designed to prevent violations of the Advisers Act. FINRA Rule 3110 requires FINRA member broker-dealers to establish and maintain a system to supervise the activities of each associated person that is reasonably designed to achieve compliance with applicable securities laws and regulations, and with applicable FINRA rules. The Risk Alert notes that strong compliance programs incorporate legal requirements and essential controls that are periodically reviewed and updated.

- Supervisors not having the same level of oversight and interaction with supervised persons when working remotely.
- Supervised persons making securities recommendations in market sectors that have experienced greater volatility or may have heightened risks for fraud.
- The impact of limited on-site due diligence reviews and other resource constraints associated with the reviewing of third-party managers, investments, and portfolio holding companies.
- Communications or transactions occurring outside of the Firms' systems due to personnel working from remote locations and using personal devices.
- Remote oversight of trading, including reviews of affiliated, cross, and aberrational trading, particularly in high volume investments.
- The inability to perform the same level of diligence during background checks when onboarding personnel—such as obtaining fingerprint information and completing required Form U4 verifications—or to have personnel take required examinations.[5]

Fees, Expenses, and Financial Transactions

The recent market volatility and the resulting impact on investors' assets and the related fees collected by Firms may have increased financial pressures on Firms and their personnel to compensate for lost revenue. The Risk Alert explains that while these incentives and related risks always exist, the current situation may have increased the potential for misconduct regarding the following:

- Financial conflicts of interest, such as: (1) recommending retirement plan rollovers, workplace plan distributions, and certain retirement account transfers; (2) borrowing or taking loans from investors and clients; and (3) making recommendations that result in higher costs to investors and that generate greater compensation for supervised persons.
- Fees and expenses charged to investors, such as: (1) advisory fee calculation errors, including valuation issues that result in over-billing of advisory fees;[6] (2) inaccurate calculations of tiered fees, including failure to provide breakpoints and aggregate household accounts; and (3) failure to refund prepaid fees for terminated accounts.
- Notably, OCIE staff suggests that Firms may wish to review their fee and expense policies and procedures and consider enhancing their compliance monitoring, particularly by:

[5] *See, e.g.,* Order Under Section 17A and Section 36 of the Securities Exchange Act of 1934 Extending Temporary Exemption from Specified Provisions of the Exchange Act and Certain Rules Thereunder, Exchange Act Release No. 89170 (June 26, 2020) and related FINRA FAQs.

[6] The SEC has brought enforcement actions against advisers for causing the overvaluation of certain holdings maintained in clients' accounts, which also may result in clients paying higher asset-based advisory fees and inflated portfolio performance returns (*see, e.g.*, In re Semper Capital Management, Advisers Act Release No. 5489 (April 28, 2020) (settled)).

- Validating the accuracy of their disclosures, fee and expense calculations, and the investment valuations used.
- Identifying transactions that resulted in high fees and expenses to investors, monitoring for such trends, and evaluating whether these transactions were in the best interest of investors.
- Evaluating the risks associated with borrowing or taking loans from investors, clients, and other parties that create conflicts of interest. Advisers seeking financial assistance should also consider if doing so will result in an obligation to update disclosures on Form ADV Part 2.[7]

Investment Fraud

OCIE staff has observed that times of crisis or uncertainty can create a heightened risk of investment fraud through fraudulent offerings. The Risk Alert suggests Firms should be cognizant of these risks when conducting due diligence on investments and in determining that the investments are in the best interest of investors.[8] Firms and investors who suspect fraud should contact the SEC and report the potential fraud.

Business Continuity

Firms are required to adopt and implement compliance policies and procedures that are reasonably designed to prevent violation of the federal securities laws. As part of this process, Firms should consider their ability to operate critical business functions during emergency events. Due to the pandemic, many Firms have shifted to predominantly operating from remote sites, and these transitions may raise compliance issues and other risks that could impact protracted remote operations. The Risk Alert provides the following examples of such compliance issues and risks:

- Firms' supervisory and compliance policies and procedures utilized under "normal operating conditions" may need to be modified or enhanced to address some of the unique risks and conflicts of interest present in remote operations. For example, supervised persons may need to take on new or expanded roles in order to maintain business operations. These and other changes in operations may create new risks that are not typically present.
- Firms' security and support for facilities and remote sites may need to be modified or enhanced. Relevant issues that Firms should consider include, for example, whether: (1) additional resources and/or measures for securing servers and systems are needed; (2) the integrity of vacated facilities is maintained; (3) relocation infrastructure and support for personnel operating from remote sites is provided; and (4) remote location data is protected.

[7] *See* Division of Investment Management Coronavirus (COVID-19) Response FAQs, Question II.4. (Posted April 27, 2020).

[8] The SEC has suspended trading for many issuers due to false and misleading claims (*e.g.*, purporting to have cures, vaccines, or curative drugs for COVID-19 infections, or access to personal protective equipment, testing, or other preventatives such as hand sanitizers).

OCIE encourages Firms to review their business continuity plans to address these matters, make changes to compliance policies and procedures, and provide disclosures to investors if their operations are materially impacted, as appropriate.

Protection of Sensitive Information

Firms have an obligation to protect investors' personally identifiable information ("PII"). OCIE staff has observed that many Firms require their personnel to use videoconferencing and other electronic means to communicate while working remotely. The Risk Alert notes that these practices create vulnerabilities around the potential loss of sensitive information, including PII, which can be attributed to, among other things: (1) remote access to networks and the use of web-based applications; (2) increased use of personally-owned devices; and (3) changes in controls over physical records, such as sensitive documents printed at remote locations and the absence of personnel at Firms' offices.[9] OCIE also recommends that Firms pay particular attention to the risks regarding access to systems, investor data protection, and cybersecurity. In particular, Firms should assess their policies and procedures and consider the following:

- Enhancements to their identity protection practices, such as by reminding investors to contact the Firms directly by telephone for any concerns about suspicious communications and for Firms to have personnel available to answer these investor inquiries.
- Providing Firm personnel with additional training and reminders, and otherwise spotlighting issues, related to: (1) phishing and other targeted cyberattacks; (2) sharing information while using certain remote systems (*e.g.*, unsecure web-based video chat); (3) encrypting documents and using password-protected systems; and (4) destroying physical records at remote locations.
- Conducting heightened reviews of personnel access rights and controls as individuals take on new or expanded roles in order to maintain business operations.
- Using validated encryption technologies to protect communications and data stored on all devices, including personally-owned devices.
- Ensuring that remote access servers are secured effectively and kept fully patched.
- Enhancing system access security, such as requiring the use of multifactor authentication.
- Addressing new or additional cyber-related issues related to third parties, which may also be operating remotely when accessing Firms' systems.[10]

[9] The Risk Alert further notes that these practices create more opportunities for fraudsters to use phishing and other means to improperly access systems and accounts by impersonating Firms' personnel, websites, and/or investors. *See* OCIE, Risk Alert: Cybersecurity: Ransomware Alert (July 10, 2020).

[10] *See, e.g.*, OCIE, Cybersecurity and Resilience Operations (January 2020).

For further information about this Alert, please contact one of the following attorneys or your regular Simpson Thacher contact.

NEW YORK CITY

Nicholas S. Goldin
+1-212-455-3685
ngoldin@stblaw.com

Michael J. Osnato, Jr.
+1-212-455-3252
michael.osnato@stblaw.com

Michael W. Wolitzer
+1-212-455-7440
mwolitzer@stblaw.com

Allison Scher Bernbach
+1-212-455-3833
allison.bernbach@stblaw.com

Meredith J. Abrams
+1-212-455-3095
meredith.abrams@stblaw.com

Manny M. Halberstam
+1-212-455-2388
manny.halberstam@stblaw.com

WASHINGTON, D.C.

David W. Blass
+1-202-636-5863
david.blass@stblaw.com

Meaghan A. Kelly
+1-202-636-5542
mkelly@stblaw.com

Anna-Kay O. Richards
+1-202-636-5552
anna-kay.richards@stblaw.com