

CORONAVIRUS RESOURCE CENTER

OCIE Publishes COVID-19 Risk Alert Focused on Investment Advisers and Broker-Dealers

August 19, 2020

On August 12, 2020, the Office of Compliance Inspections and Examinations (“OCIE”) of the U.S. Securities and Exchange Commission (the “SEC”) published a risk alert (the “Risk Alert”)¹ outlining its recommendations to SEC-registered broker-dealers and investment advisers on operational, technological and commercial challenges due to the effects of COVID-19. The Risk Alert follows OCIE’s announcement earlier in 2020 that it would engage with SEC registrants to address COVID-19-related regulatory and compliance issues in efforts to ensure that operations could be conducted in a manner consistent with normal operations and health and safety measures. Given OCIE’s observations, the Risk Alert is a timely reminder for firms to assess their experiences with and responses to COVID-19 and make any necessary updates to their compliance policies and procedures.

The Risk Alert did not identify any of the observations as relating specifically to private fund managers² and their related broker-dealers, and certain of the areas below—such as check processing and client identification for disbursements—may be more applicable to investment advisers and broker-dealers with retail clients. Private fund managers nevertheless should review the areas below and, consistent with the Risk Alert, take active steps to assess their practices appropriately.

Protection of Investors’ Assets. In light of the current environment, OCIE suggests that firms consider making changes in the following areas:

¹ Risk Alert: Select COVID-19 Compliance Risks and Considerations for Broker-Dealers and Investment Advisers (Aug. 12, 2020), available at <https://www.sec.gov/files/Risk%20Alert%20-%20COVID-19%20Compliance.pdf>.

² Compare to OCIE’s risk alert of June 23, 2020 specifically addressed to private fund managers: Risk Alert: Observations from Examinations of Investment Advisers Managing Private Funds (June 23, 2020), available at <https://www.sec.gov/ocie/announcement/risk-alert-private-funds>.

-
- Disbursement of funds to investors, including by (i) implementing additional steps to validate an investor's identity and authorization to request disbursements or transfers and (ii) recommending that investors have trusted contact persons, which may be of heightened importance for retail investors.
 - Collection and processing of investor checks and transfer requests, especially where the firm may experience delays in accessing email and deliveries. Of note, OCIE recommends assessing material impacts and considering whether disclosure of any such delays should be made to investors.

Supervision of Personnel. In light of market-wide shifts to teleworking and the related effects on the level of oversight and interaction with supervised persons working remotely, OCIE encourages firms to review their policies and procedures with a focus on the following areas:

- Effects of limited on-site due diligence reviews and other resource constraints associated with reviewing third-party managers, investments and portfolio companies.
- Communications and transactions by supervised persons effected remotely, including by use of personal devices.
- Oversight of supervised persons making securities recommendations in sectors experiencing greater volatility or heightened risks for fraud or trading in high-volume investments or investments that may require affiliated, cross and aberrational reviews.
- Ability to perform due diligence and background checks of new personnel and inability of new personnel to take necessary examinations.

Practices Relating to Fees, Expenses and Financial Transactions. OCIE cautions of a heightened risk of misconduct or errors in the following areas:

- Financial conflicts of interest, including when a firm borrows or takes loans from investors or when it recommends investments or products that the firm or its personnel is soliciting or that could result in higher costs to investors.
- Fees and expenses charged to investors, including overbilling due to valuation errors, failure to provide breakpoints or aggregating household accounts, and not refunding prepaid fees for terminated accounts.

In light of the foregoing, OCIE recommends that firms review their policies and procedures related to fees and expenses with a focus on the following areas:

- Accuracy of disclosures, fee and expense calculations, and investment valuations.
- Identification of transactions that result in high fees and expenses, monitoring of such trends and evaluation of whether these transactions are in the best interest of investors.
- Evaluation of conflicts of interest associated with borrowing or taking loans from investors and any related obligations to update disclosures on Form ADV Part 2.

Investment Fraud. OCIE warns market participant of the heightened risk of fraudulent offerings when conducting due diligence of investments.

Business Continuity Plans. As firms are testing their business continuity plans and their ability to operate critical business functions remotely, OCIE encourages firms to review their continuity plans, update their policies and procedures, and make any necessary disclosures of material changes to investors. Specifically, OCIE recommends the evaluation of:

- Observed risks and conflicts of interest involved in working remotely, including new and expanded roles by personnel in order to maintain business operations.
- Security and support for facilities and remote sites, including (i) whether additional resources or measures are required to secure servers and systems, (ii) the integrity and maintenance of vacated facilities, (iii) the provision of infrastructure and support for personnel working remotely, and (iv) the protection of data.

Protection of Sensitive Information. In light of remote access to firm networks, increased use of personal devices by firm personnel, changes in controls over physical records, and an increase in phishing and other examples of improper access to a firm's systems and information, OCIE recommends that firms review their policies and procedures to consider:

- Enhancements to identity protection, such as by encouraging investors to contact firms by phone if they observe suspicious activity.
- Additional trainings and reminders to firm personnel related to (i) phishing and other targeted cyberattacks, (ii) use of unsecured video, audio or email communications to share information, (iii) encryption of documentation, and (iv) proper destruction of physical records at remote locations.

- Heightened reviews of personnel access rights and controls as they change their roles.
- Use of validated encryption technologies and enhancements to system access security, such as by requiring multifactor authentication.
- Security of remote access servers and assessment of new or additional risks related to third parties.

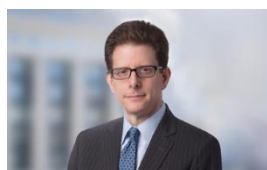
* * *

For more information regarding the legal impacts of the coronavirus, please visit our [Coronavirus Resource Center](#).

Please do not hesitate to contact us with any questions.



Kenneth J. Berman
Partner, Washington, D.C.
+1 202 383 8050
kjberman@debevoise.com



Robert B. Kaplan
Partner, Washington, D.C.
+1 202 383 8060
rbkaplan@debevoise.com



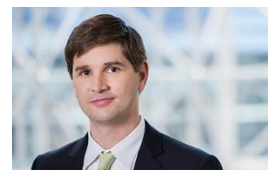
Marc Ponchione
Partner, Washington, D.C.
+1 202 383 8290
mponchione@debevoise.com



Julie M. Riewe
Partner, Washington, D.C.
+1 202 383 8070
jriewe@debevoise.com



Jeff Robins
Partner, New York
+1 212 909 6526
jirobins@debevoise.com



Gregory T. Larkin
Counsel, Washington, D.C.
+1 202 383 8064
gtlarkin@debevoise.com



Norma Angelica Freeland
Associate, New York
+1 212 909 6110
nafreeland@debevoise.com