SEC RISK ALERT: COVID -19 COMPLIANCE RISKS AND CONSIDERATIONS

The SEC issued a Risk Alert on August 12, 2020, in response to the broad and varied effects of COVID-19 on SEC registrants that have been faced with new operational, technological, commercial, and other challenges and issues. In many cases, these challenges and issues have created important regulatory and compliance questions and considerations for SEC registrants. OCIE has identified several COVID-19-related issues, risks, and practices relevant to SEC-registered investment advisers and broker-dealers (collectively, "Firms") that are addressed below. Additionally, market volatility related to COVID-19 may have heightened the risks of misconduct in various areas that the staff believes merit additional attention. The purpose of the Risk Alert is to share some of these observations with Firms, investors, and the public generally. OCIE's observations and recommendations fall broadly into the following six categories:

(1) PROTECTION OF INVESTORS' ASSETS
(2) SUPERVISION OF PERSONNEL
(3) PRACTICES RELATING TO FEES, EXPENSES, AND FINANCIAL TRANSACTIONS
(4) INVESTMENT FRAUD
(5) BUSINESS CONTINUITY
(6) THE PROTECTION OF INVESTOR AND OTHER SENSITIVE INFORMATION

PROTECTION OF INVESTOR ASSETS

Each Firm is responsible for ensuring the safety of its investors' assets and guarding against theft, loss, and misappropriation. In light of the current environment, the staff has observed that some Firms have modified their normal operating practices regarding collecting and processing investor checks and transfer requests. OCIE encourages Firms 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 want to update their supervisory and compliance policies and procedures to reflect any adjustments made and to consider 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 the mail or deliveries at that office location. 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.

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 bank account names and numbers are accurate; and
- **Recommending that each investor has a TRUSTED CONTACT PERSON IN PLACE**, particularly for seniors and other vulnerable investors.
- **Update Policies and Procedures as described above.**

SUPERVISION OF PERSONNEL

Firms are required to supervise their personnel, including providing oversight of supervised persons' investment and trading activities. A Firm's supervisory and compliance program should include policies and procedures ***tailored to its specific business activities and operations and should be amended as necessary to reflect the Firm's current business activities and operations***. As Firms need to make significant changes to respond to the health and economic effects of 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, Firms may wish to modify their practices to address the following:

- **SUPERVISORS NOT HAVING THE SAME LEVEL OF OVERSIGHT AND INTERACTION** with supervised persons 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 **REVIEWING OF THIRD-PARTY MANAGERS, INVESTMENTS, AND PORTFOLIO HOLDING COMPANIES**.
- **COMMUNICATIONS OR TRANSACTIONS OCCURRING OUTSIDE OF THE FIRMS' SYSTEMS** due to personnel working remotely locations and using personal devices.
- **REMOTE OVERSIGHT OF TRADING**, including reviews of affiliated, cross, and 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, completing required Form U4 verifications, or have personnel take requisite examinations.

FEES, EXPENSES, AND FINANCIAL TRANSACTIONS

Firms have obligations to consider and inform investors about the costs of services and investment products, and the related compensation received by the Firms or their supervised persons. The recent market volatility and the resulting impact on investor assets and the related fees collected by Firms may have increased financial pressures on Firms and their personnel to compensate for lost revenue. While these incentives and related risks always exist, the current situation may have increased the potential for misconduct regarding:

- **Financial conflicts of interest, such as:**
  - **Recommending retirement plan rollovers** to individual retirement accounts, workplace plan distributions, and retirement account transfers into advised accounts or investments in products that the Firms or their personnel are soliciting;
  - **Borrowing or taking loans from investors and clients**; and
  - Making **recommendations that result in higher costs to investors** and generate greater compensation for supervised persons, such as investments with termination fees that are switched for new investments with high up-front charges or mutual funds with higher-cost share classes when lower-cost share classes are available.
- Fees and expenses charged to investors, such as:
  - **Advisory fee calculation errors,** including valuation issues that result in over-billing of advisory fees;
  - **Inaccurate calculations of tiered fees**, including failure to provide breakpoints and aggregate household accounts; and
  - **Failures to refund prepaid fees** for terminated accounts.

Firms may wish to review their fees and expenses policies and procedures and consider enhancing their compliance monitoring, particularly by:

- **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, as this may impair the impartiality of Firms' recommendations. Also, ***if advisers seek financial assistance, this may result in an obligation to update disclosures on Form ADV Part 2.***

INVESTMENT FRAUD

The staff has observed that times of crisis or uncertainty can create a heightened risk of investment fraud through fraudulent offerings. 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. ***Firms and investors who suspect fraud should contact the SEC and report the potential fraud.***

BUSINESS CONTINUITY

Individual firms are required to adopt and implement compliance policies and procedures 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, including:

- **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. **If relevant practices and approaches are not addressed in business continuity plans and/or Firms do not have built-in redundancies for essential operations and key person succession plans, mission-critical services to investors may be at risk.**

OCIE encourages Firms to review their 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 must protect investors' personally identifiable information ("PII"). The staff has observed that many Firms require their personnel to use videoconferencing and other electronic means to communicate while working remotely. While these communication methods have allowed Firms to continue their operations, these practices create:

- Vulnerabilities around the potential loss of sensitive information, including PII. These risks are attributed to, among other things:
  - Remote access to networks and the use of web-based applications;
  - Increased use of personally-owned devices;
  - Changes in controls over physical records, such as sensitive documents printed at remote locations and the absence of personnel at Firms' offices.

The Safeguards Rule of Regulation S-P requires every SEC-registered broker-dealer and investment adviser to adopt written policies and procedures to address administrative, technical, and physical safeguards for the protection of investor records and information. The Identity Theft Red Flags Rule of Regulation S-ID requires certain firms 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.

- More opportunities for fraudsters to use phishing and other means to improperly access systems and accounts by impersonating Firms' personnel, websites, and/or investors.

OCIE 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:

- **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 TRAININGS AND REMINDERS,** and otherwise spotlighting issues, related to:
  - Phishing and other targeted cyberattacks;
  - Sharing information while using certain remote systems (e.g., unsecure web-based video chat);
  - Encrypting documents and using password-protected systems; and
  - Destroying physical records at remote locations.
- **CONDUCTING HEIGHTENED REVIEWS OF PERSONNEL ACCESS RIGHTS AND CONTROLS** as individuals take on new or expanded roles 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.

***Source:** **Click here for a complete copy of the latest SEC RISK ALERT**