CHECKLIST BASED ON OCIE RISK ALERT ON SELECT COVID-19 COMPLIANCE RISKS AND CONSIDERATIONS

PROTECTION OF INVESTOR ASSETS

Collecting and Processing Investor Checks and Transfer Requests

- Review Firm practices, and make appropriate adjustments, including to where investors mail checks (and presumably securities) to the Firm
- Update supervisory and compliance policies and procedures to reflect any adjustments to receipt and handling of checks in light of change of pickup of checks
- Consider disclosing to investors that checks or securities mailed to the Firm's office may experience delays in processing until personnel are able to access the mail or deliveries

Disbursements to Investors

- Review and make any necessary changes to policies and procedures, to address where investors are taking unusual or unscheduled withdrawals, particularly COVID-19-related distributions from retirement accounts
- Consider additional steps to validate the identity of investors and the authenticity of disbursement instructions, including as to whether the person is authorized to make the request and the bank account names and numbers are accurate
- Consider recommending that each investor have a trusted contact person particularly for seniors and other vulnerable investors

SUPERVISION OF PERSONNEL

- Review and, as appropriate, modify supervisory and compliance policies and procedures to reflect significant changes to respond to health and economic effects of COVID-19 (e.g., 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)
- Consider modifying Firm practices to address:
  - Supervisors not having the same level of oversight and interaction with supervised persons working remotely
  - Supervised persons making securities recommendations in market sectors experiencing greater volatility or having heightened risks for fraud
  - Impact of limited on-site due diligence reviews and other resource constraints when reviewing of third-party managers, investments, and portfolio holding companies
  - Communications or transactions occurring outside of Firm 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
  - Inability to perform the same level of diligence during background checks when onboarding personnel (e.g., obtaining fingerprint information and completing required Form U4 verifications or to have personnel take requisite examinations)

FEES, EXPENSES, AND FINANCIAL TRANSACTIONS

- Review fees and expenses policies and procedures adopted to compensate for lost revenue and related potential for misconduct vis a vis conflicts or computation of fees and expenses and consider enhancing monitoring by:
  - Validating the accuracy of disclosures, fee and expense calculations, and investment valuations
  - Identifying transactions resulting in high fees and expenses to investors, monitoring for such trends, and evaluating whether these transactions are 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 (and raise FINRA Rule 3240 questions)

INVESTMENT FRAUD

- Be cognizant of heightened risk of fraudulent offerings when conducting due diligence and in determining that an offering is in the best interest of investors
- Report suspected potential fraud to the SEC

BUSINESS CONTINUITY

- Review and, as appropriate, make changes to Firm continuity plan and related compliance policies and procedures, and disclosures to reflect material impact to operations:
  - Consider whether Firm supervisory and compliance policies and procedures need to be modified to address unique risks and conflicts with remote operations (e.g., supervised persons may need to take on new roles to maintain business operations)
  - Consider whether security and support for facilities and remote sites need to be modified, including (1) additional resources or measures for securing servers and systems; (2) maintenance of integrity of vacated facilities; (3) relocation infrastructure and support for personnel operating from remote sites; and (4) protection of customer and firm data at remote locations

PROTECTION OF SENSITIVE INFORMATION

- Monitor risks with systems access, investor data, and cybersecurity and related policies and procedures and consider:
  - Enhancements to identity protection practices (e.g., reminding investors to contact the Firm directly by telephone for any concerns about suspicious communications and for Firm personnel to be available to answer 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 Firm systems