SEC Outreach Programs
November 2020

The SEC held two compliance outreach programs last week, the first a national program highlighting findings from OCIE's Risk Alert on Adviser Compliance Programs and including updates from the Division of Investment Management and Enforcement Division. Following are highlights from the main panels. Additional comprehensive notes from the outreach program are available from the CORE Team.

- Information Security & Operational Resiliency
  - SEC Exam & Enforcement Programs and the Division of Investment Management continued operations in a remote environment throughout much of 2020 and plan to continue to do so through the beginning of 2021
  - Most firms examined or contacted by the SEC through outreach programs have similarly worked effectively remotely during COVID
  - SEC staff have engaged in various interactions with the industry to understand market implications from COVID and are considering extending additional relief for certain matters such as in-person board meeting requirements
  - SEC examiners have seen an uptick in cybersecurity attacks during COVID and have issued recent risk alerts regarding concerns
  - The SEC has a Cyber Unit in its Enforcement program that works together with SEC exam staff to evaluate security breaches at financial firms and impacting the markets
  - The SEC's guidance and relevant risk alerts can be accessed from the Cyber Spotlight webpage at https://www.sec.gov/spotlight/cybersecurity
- Undisclosed Conflicts of Interest
  - SEC guidance in June codified the fiduciary duty standard to which all advisers are subject and highlighted the requirement for full and fair disclosure that is sufficiently specific to allow informed consent
  - SEC exam and enforcement staff have focused on undisclosed conflicts related to cash management/sweep accounts resulting in remuneration or fee reduction for the adviser
  - SEC exam and enforcement staff have also focused heavily on mutual fund share class cases in which advisers recommended share classes that resulted in higher compensation and failed to seek best execution – Firms were given an opportunity to self-report for a lighter enforcement settlement
  - The SEC Private Funds Unit risk alert highlighted common undisclosed conflicts for private funds including: Allocation of investment opportunities; Financial relationships with investors/clients; relationships with service providers and fees and expenses – Stay tuned for Part 2 in coming months
- Registered Investment Company Issues
  - SEC staff recently issued guidance requiring derivative risk management programs for mutual funds including risk-based stress testing, board oversight and SEC reporting

- SEC staff further issued a proposal related to fair value of mutual fund assets requiring Board oversight of valuation risks, requirements to select and apply appropriate valuation methodologies with periodic review, testing and adjustments and evaluation of pricing services
- SEC enforcement actions against registered funds have targeted undisclosed financial conflicts for order flow arrangements, cross transactions, valuation cases and false and misleading statements

- Hot Topics
  - Exam and enforcement staff have engaged in educational and other efforts related to teacher retirement plans
  - Exam and enforcement efforts have targeted "robo advisers" and misleading statements regarding automated processes
  - SEC staff continue to explore digital assets and compliance issues related to crypto currency strategies, including valuation, custody, liquidity, efficiency of arbitration and potential manipulation
  - With a variety of guidance from different constituents on ESG, examiners are likewise focused on ESG strategies, disclosures and practices
  - SEC exam staff have begun evaluating newly filed Form CRS and are following up on potential inconsistencies and incorrect responses in such filings
  - SEC staff are working together with the industry and continuing an exam initiative to assess preparedness for the transition away from LIBOR

The Fort Worth Office outreach program covered many of the same compliance program observations as the national program and the recent OCIE Risk Alert. It was noted that exam staff pay particular attention in examinations to the support and resources firms provide to their CCO and take note if there are frequent changes in CCO or if the CCO is not integrated into the fabric of all aspects of the firm's business in order to address and consider potential compliance implications. Fort Worth staff provided additional tips in response to the uptick in cybersecurity attacks as follows:

- Firms should spend time and effort with professional assistance evaluating cyber risks and designing policies and procedures to minimize those risks
- With evolving privacy policies in states and other jurisdictions, firms may have an affirmative compliance duties and notification requirements with respect to breaches and attacks, sometimes even unsuccessful attacks
- Firms should pay particular attention to security and resiliency policies and procedures of third-party vendors
- Training and scenario planning is critical to ensure you have a plan for how to respond and know who you need to contact in the event of a security breach when time is paramount
- Making ransomware payment may be a violation AML rules if made to a high-risk country