Board iQ
A Financial Times Service

SEC Enforcement's New Leadership and (Likely) Priorities

October 10, 2017

Lorraine Echavarria is a partner at WilmerHale.

Fund board directors may be wondering what to expect from the new leaders of the Securities and Exchange Commission. A new chairman has been appointed, nominations for two new commissioners have been made to fill long-vacant seats and new co-directors now lead the Division of Enforcement.

An important signpost comes from recent and repeated comments by the new chair, Jay Clayton, which emphasize the long-term interests of retail investors, a group he refers to as "Mr. and Mrs. 401(k)." Interest in this group would be an organizational shift in focus from certain non-traditional investment opportunities, such as private equity funds, to more conventional investment vehicles, such as mutual funds.

It also appears that enforcement lawyers will turn away from their "broken windows" tactic of charging many technical violations to deter more significant misconduct. Instead, the division will go after clear wrongdoing that could measurably harm investors.

Consistent with that, new SEC enforcement leadership will likely prioritize three issues relevant to fund directors: undisclosed or overcharged fees, rogue trading conduct and cyber security.

Fees, Fees, Fees

Undisclosed fees present the possibility of direct and measurable economic harm to retail investors.

Some firms have already been penalized for charging undisclosed or hidden excessive fees. For example, State Street subsidiaries paid a $32.3 million penalty related to alleged "hidden and unauthorized mark-ups and commissions" associated with transition management services, the SEC announced in September. Transition management services are provided to customers changing investment advisers or strategies.

In a separate matter a week later, the SEC alleged breach of fiduciary duty related to undisclosed "avoidable" fees against an investment subsidiary of SunTrust Banks. The commission alleged that clients were placed in more expensive mutual fund share classes with 12b-1 fees instead of in less expensive share classes in the same mutual fund that did not have such fees.

The SEC has scrutinized bundled fees, such as wrap-fee programs, in the past, and the topic is likely to continue to gain attention. Overpayment of fees or expenses can be quantified, and the commission can require a fund complex to repay investors directly under its Fair Fund authority. This gives the SEC a satisfying result to tout in its actions.

Rogue Trading

Rogue trading by individual advisers can range from misappropriating customer funds or unauthorized trading to insider trading. The SEC will keep these practices at the forefront of its priority list.

The commission recently began homing in on cherry-picking. This is when financial advisers allocate profitable trades to preferred funds – often where their own investments are held or those of a preferred class of investors – and send less profitable or losing trades to other accounts. Funds held by retail investors lose, in a measurable and actual amount.

Cherry-picking is relatively easy for the SEC to focus on because it relies entirely on data for evidence. Now that the agency routinely collects significant data and can crunch that information, enforcement staff can readily find and prove patterns of misconduct. The SEC can then prove its case without relying on more subjective types of evidence.

Directors should require fund advisers to maintain policies designed to prevent, detect and halt these rogue trading practices. Boards should confirm that management and fund service providers have internal trading surveillance programs that are designed to ensure best execution and fulsome disclosure. The policies should also establish reasonable checks and balances on trading decisions.

These trade surveillance programs could monitor the lifecycle of trades from order placement to settlement and provide a clear audit trail that could be reproduced for compliance reviews if needed. Surveillance programs may include pre-trade compliance checks. They can also prevent late allocations of trading or require managers to review trade movement and analyze transaction costs after trades settle to ensure best execution.

Cyber Security as Investor Protection

Grave investor harm looms in cyber-security breaches. Investors' personal information can be revealed, or the complex can lose control over investment decisions. The safeguards rule (Rule 30(a) of Regulation S-P) requires investment advisers and broker-dealers to adopt written policies

and procedures reasonably designed to protect the security and confidentiality of customer information, records and account access. SEC enforcement officials likely will use that rule to make sure fund shops are protected against harm from hackers. Cyber-security oversight by fund directors should confirm that advisers possess these written policies and that they cover timely reporting of a breach to the fund board and, subsequently, investors.

Although an adequate compliance program that satisfies requirements of the safeguards rule may not prevent malicious attacks, such policies may limit the scope or harm from them. The safeguards rule also gives the SEC jurisdiction over cyber-security efforts, which allows the regulator to execute on mandates from its leadership prioritizing the issue.

Takeaways

Fund directors should focus on fees and their disclosure practices, compliance programs rooting out malevolent trading patterns, and cyber-security risks. Then when something goes wrong, a complex can point to a robust compliance program in responding to the SEC's anticipated scrutiny.