The HEDGE FUND LAW REPORT
The definitive source of actionable intelligence on hedge fund law and regulation

www.hflawreport.com Volume 9, Number 37 September 22, 2016

INSIDER TRADING

Seward & Kissel Private Funds Forum Explores How Managers Can Mitigate Improper Dissemination of Sensitive Information (Part One of Two)

By Michael Washburn

Fund managers in the heightened regulatory environment of 2016 need to be acutely aware of the dangers of running afoul of regulators' standards and expectations in numerous areas. In particular, the SEC has focused on safeguards that managers employ to prevent the dissemination of sensitive information and to ensure it is not used for improper trading. This was among the critical issues addressed by one of the panels at the second annual Private Funds Forum produced by Seward & Kissel and Bloomberg BNA, held on September 15, 2016.

Moderated by Seward & Kissel partner Patricia Poglinco, the panel included Rita Glavin and Joseph Morrissey, partners at Seward & Kissel; Laura Roche, chief operating officer and chief financial officer at Roystone Capital Management; and Scott Sherman, general counsel at Tiger Management. This article, the first in a two-part series, reviews the panel's discussion about risks associated with the inflow and outflow of material, nonpublic information (MNPI), as well as steps that fund managers can take to prevent its improper use. The second article will discuss the types of conflicts of interest targeted by the SEC, the current progress of the SEC's whistleblower program and the difficulty of prosecuting insider trading.

For coverage of the 2015 Seward & Kissel Private Funds Forum, see "*Trends in Hedge Fund Seeding Arrangements and Fee Structures*" (Jul. 23, 2015); and "*Key Trends in Fund Structures*" (Jul. 30, 2015). For additional commentary from Glavin, see "*FCPA Compliance Strategies for Hedge Fund and Private Equity Fund Managers*" (Jun. 13, 2014). For more from Sherman, see "*RCA Asset Manager Panel Offers Insights on Hedge Fund Due Diligence*" (Apr. 2, 2015).

Preventing the Spread of Sensitive Information

The SEC has cracked down on how firms handle MNPI, with the use of that information posing a greater risk than ever. These risks are particularly evident in the areas of buy-side communications and customized research, where a high volume of sensitive proprietary information comes into play on a daily basis.

There are two basic scenarios in which firms may fail to meet their obligations, Morrissey explained:

1. when a firm's own information is released into the world; and
2. when a firm receives information from peer firms or service providers.

Outflows of Information

Whenever information leaves a firm, Morrissey emphasized that it needs to be through a conscious, carefully managed decision on the firm's part. An important step to ensuring this occurs, according to Sherman, is for firms to be careful about the manner in which they disclose positions that are held by clients until they are fully sized. "Some of the things that I've seen include not disclosing short positions," he explained, "and not disclosing long positions until they are publicly filed, whether on a Form 13F or otherwise."

Morrissey identified a real-life scenario that illustrates the potential risk for the free flow of client information to occur when a firm interacts with third parties. When a given firm has existing positions in portfolio companies and talks to other peer firms holding positions in the same companies, the firm must take particular care that no issues arise with regard to Section 13 and Form D filings on those positions.

The HEDGE FUND LAW REPORT
The definitive source of actionable intelligence on hedge fund law and regulation
www.hflawreport.com Volume 9, Number 37 September 22, 2016

One step utilized by Sherman and his colleagues to this end is to avoid talking about the timing and sizing of trading positions. Talking about these things on a general, or macro, level is widely done and considered an acceptable practice if done correctly, he stipulated. But when it comes to talking about the specific timing and sizing of positions, potential concerns can arise. This has been an increased focus of the SEC recently.

If client information is improperly dispensed, several dangers can arise. The first is the threat that the information will be used by outside actors. If third parties gain access to proprietary information before the firm has acted on that information on its clients' behalf, they may be able to "front run" a trade or otherwise use that information in the market to put the firm's clients at a disadvantage.

An additional risk, Sherman explained, is that a firm could be accused of taking investment opportunities away from its clients. Once again, careful documentation of the research process is key. Documenting actions based on policies and procedures enables the firm to rebut any presumption or accusation about trading taking place at the expense of clients as a result of such communications, he said.

Moreover, when documenting trades that a firm makes, there is an increased focus on the relationship between a firm's disclosures and the actual positions it takes. For example, if a firm's disclosure says it has certain positions, but the firm takes a name from another buy-side firm and puts that name in its book, that will pose problems at the enforcement level.

Inflow of Information

An important, overarching issue identified by Morrissey concerning the receipt of sensitive information from third-party sources, regardless of their nature, is for firms to take steps to ensure that information has been obtained properly and legally. Each source of the third-party information presents its own unique struggles in this regard.

Data Scraping

One third-party source of information utilized by analysts, as described by Sherman, is the practice of "data-scraping," or pulling information from web pages and other electronic sources. This is essentially information located in the underlying source code behind the main portals of web pages, he explained.

Sherman said that a firm's responsibility in gathering this type of information is to ensure that there are no restrictions on how it can be utilized. To determine whether any use restrictions exist, he explained, firms and their analysts need to refer to the privacy policies and terms of use policies for the web pages subject to the data scraping.

It is important for a firm to train its analysts to review these web page policies when data scraping and bring them to the attention of the firm's compliance team, Sherman continued, so they can carefully consider whether the activities the firm would engage in with the information would violate these restrictions.

Morrissey echoed these sentiments, identifying this as a situation where due diligence becomes of prime importance. Emphasizing the need for clearly defined policies and procedures for the use of MNPI and the sources of that information, he said, "You really have to do your homework and be sure you know what you're bringing in under your tent."

Service Providers

Another source of MNPI is a firm's interactions with peer firms or service providers. To ensure that these do not result in the firm unwittingly obtaining such information, Sherman stressed the need to perform thorough due diligence with respect to outside service providers. It is important to know, in depth, the providers that your firm is using to obtain information, he explained. "This includes getting ahold of the service providers' policy manuals and their policies and procedures, as well as finding out what training their employees receive."

Additionally, Roche emphasized that a firm needs to provide its policies and procedures to service providers it utilizes so that they understand the firm's standards and requirements for handling sensitive information. Sometimes a manager may be dealing with a sole service provider without a big legal team, or even just one individual who does research for the firm. In that case, it will be necessary to make sure that individual service provider reviews the internal policies of the firm and manager with which he or she is working to understand what is and is not permissible, she continued.

If a manager is comfortable that the service provider's policies and procedures pass muster and that the provider is suitably apprised of the firm's policies, Morrissey said, then the next step is to draw up a written contract with the service provider. This agreement should be drafted, he explained, to ensure that the service provider will not funnel information to the manager that has been obtained in violation of the law and confidentiality obligations. Additionally, and just as importantly, the agreement should ensure that there are sufficient remedies available to the firm in the case of a breach.

Mitigation Through Internal Policies and Training

In order to balance the risks of the possible illegal disclosure of sensitive information with the perceived possible value of interacting with other players in the market, Morrissey said it is of critical importance for firms to document all of their policies and protocols, just as they would with any of their other key practices. He clarified that this approach should be utilized by a firm regardless of what it chooses to do in this area – whether it decides to forbid outright, or to allow, the outflow and inflow of sensitive communications.

In support of this notion, Sherman emphasized that "there is no 'one-size-fits-all' approach, but a manager certainly has to tailor these policies and procedures to the firm's specific needs and the types of communications that its analysts are having with other adviser firms."

Even if the policies are tailored to the actions of analysts, Roche emphasized the critical importance of educating the analyst team on the importance of seeking compliance approval for the information they receive. An added benefit, she explained, is that regular compliance training sessions with staff may help answer questions on their minds and even possibly address issues that they may not have contemplated.

Once a research analyst brings a matter to the attention of the compliance department, the CCO should reach out to the compliance personnel and speak with them about the firm's policies and procedures so that they can make any necessary changes to the internal documents, she explained. Ultimately, the firm must put its compliance division to work to make sure that the activity measures up to those policies and procedures, and that they continue to evolve with the practices of the firm.