Hedge Fund Law Report
An Acuris company

hflawreport.com

January 27, 2022

INSIDER TRADING

# Implications of Recent Insider Trading and MNPI Cases for Hedge Fund Managers (Part One of Two)

By Helen Kim, *Hedge Fund Law Report*

In addition to staying aware of SEC guidance, rulemaking, statements, risk alerts and other overt indicators of the regulator's areas of focus, hedge fund managers should also keep up to date on enforcement actions that may more subtly suggest the SEC's key concerns. For example, two fairly unique SEC enforcement actions announced in fall 2021 have caused CCOs to think anew about insider trading and material nonpublic information (MNPI).

Those actions and other issues were addressed in a Practising Law Institute panel moderated by Gibson Dunn partner Mark K. Schonfeld. The panelists included Eric M. Albert, CCO and legal counsel at Holocene Advisors, LP; Kenneth J. Burke, head of compliance and senior counsel at Vista Credit Partners Management, LLC; and Igor Rozenblit, founder and partner at Iron Road Partners and former Co-Head of the SEC's Private Funds Unit. This article, the first in a two-part series, covers the discussion of those enforcement actions and their implications for hedge fund managers. The second article will summarize key takeaways from the discussion on current compliance challenges involving ESG investing and conflicts related to business expansion, as well as early goals for incoming CCOs.

For more from Schonfeld, see "Regulatory and Employment Concerns for Managers Reopening Their Offices" (Aug. 6, 2020).

## App Annie

In September 2021, the SEC announced that App Annie Inc., an alternative data provider for the mobile app industry, and its co-founder, had agreed to pay more than $10 million to settle securities fraud charges for engaging in deceptive practices and making material misrepresentations about how the company's alternative data was derived. It was the first SEC enforcement action charging an alternative data provider with securities fraud.

According to the September 14, 2021, settlement order, App Annie assured companies that their data would be aggregated and anonymized before being used by a statistical model to generate estimates of app performance, but in fact, it used non-aggregated and non-anonymized data to make its model-generated estimates more valuable to trading firms. App Annie also misrepresented to its investment firm customers that it generated estimates consistent with consents it obtained from companies that shared their confidential data.

©2022 Hedge Fund Law Report. All rights reserved.

See "SEC Action Against Alternative Data Vendor Is Warning to Fund Managers" (Oct. 14, 2021).

## Potential Implications for Fund Managers

Although the SEC in this case charged a data vendor, it is possible that many users of App Annie data observed how accurate the data was, Rozenblit mused, raising the question of whether the Commission will pursue fund managers for either knowingly or negligently using data they should have known was obtained in breach of a duty.

The representations made by App Annie to its investment firm subscribers were, in part, the basis for the alleged violation, Schonfeld observed. Big questions for firms using alternative data are whether there are circumstances in which the level of due diligence conducted on the data vendor may cause SEC staff to view the subscriber as reckless or negligent in using the vendor's data and whether representations are sufficient to protect against a lesser level of diligence.

See "SEC Compliance and Enforcement Expectations for Private Funds Under Chair Gensler" (Oct. 7, 2021).

There are some cases in which relying solely on reps and warranties is not advisable, Rozenblit observed. Even if the SEC does not bring a case against a fund manager, alternative data is a high-risk area and could be the focus of investigations, Burke warned.

## Tips for Diligencing Alternative Data Vendors

The case challenges CCOs to work closely with data science and investment teams, as well as the internal manager of vendor relationships, to perform thorough, probing and well-documented due diligence, Albert suggested. Compliance must be involved from the earliest stages as new vendors are being assessed or onboarded. Before allowing a set of back-tested data into the firm, CCOs should send written due diligence questionnaires (DDQs) and have phone conversations with representatives of the alternative data provider, he added.

### Understand the Vendor

Specifically, Albert continued, CCOs need to understand who the vendor is by asking questions such as:

1. how long it has been in business;
2. how long it has been selling data to investment firms;
3. what its current client base looks like;
4. who its officers and executives are;
5. who its legal and compliance personnel are; and
6. who its outside counsel is.

Compliance teams should review the vendor's internal compliance programs, including its compliance manuals, policies and any litigation or regulatory issues.

### Check Data Provenance

Next, CCOs should determine the vendor's data provenance by determining where the underlying data comes from and whether the vendor has the right to use it and sell it to investment firms, with the knowledge that investment firms will be using the data as part of their investment processes. As part of that analysis, Albert elaborated, CCOs should know whether all of the data is publicly available, is

©2022 Hedge Fund Law Report. All rights reserved.

the product of web scraping or derives from other collection efforts. CCOs should also know whether the data includes MNPI.

CCOs should not merely ask the questions – they should consider asking for copies of the contracts, even if redacted, that the data vendors have with the downstream data sources, Albert recommended.

**Assess Vendor's Data Privacy Framework**

Compliance teams should assess the alternative data provider's attention to and observation of applicable data privacy laws, rules and regulations, including how it aggregates and anonymizes the data. CCOs need to ensure that personally identifiable information (PII) is not passed through to the firm by the vendor.

Finally, Albert said that compliance teams should work together with their IT or information security teams to understand how the vendor processes, stores and transmits the data.

Some vendors resist due diligence that digs in so deeply, Rozenblit cautioned. Risk rating vendors is useful in scenarios in which vendors are reluctant to provide certain information or documents, he suggested. Credit card data, for example, is on the riskier end of the spectrum, whereas satellite data is potentially less risky.

See "A Checklist for Fund Managers to Ensure Adequate Vendor Management" (Sep. 9, 2021); "The Importance of Exercising Due Diligence When Hiring Auditors and Other Vendors" (Jun. 21, 2018); and "Best Practices for Due Diligence by Hedge Fund Managers on Research Providers" (Mar. 14, 2013).

## Key Representations in Vendor Contracts

Alternative data vendors should be required to represent that they have the right to use and sell the data and that the fund manager has the right to use that data as part of its investment decision making, Albert recommended. Vendors should also represent that they are in compliance with applicable laws, rules and regulations, as well as that they understand the PII issues and will not be transmitting PII.

See our two-part series on drafting data privacy and security provisions in vendor agreements: "Assessing the Risks" (Apr. 1, 2021); and "Negotiating Critical Provisions and Responding to Incidents" (Apr. 8, 2021).

## Updates to Internal Manuals, Policies and Procedures

CCOs should consider inserting an alternative data section in the firm's compliance manual to set out policies and procedures specific to alternative data providers, such as diligence steps, contractual protections and a written DDQ form. Training about compliance issues regarding alternative data – either ad hoc training for data scientists and investment analysts or an additional segment of the annual compliance and insider trading training – is also a good idea, Albert said.

See our two-part series on compliance training: "SEC Expectations and Substantive Traps to Avoid" (Sep. 23, 2021); and "Who Conducts the Training and Five Traps to Avoid When Providing Training" (Sep. 30, 2021).

Ongoing surveillance and monitoring of alternative data providers is also a critical part of compliance procedures. Refreshing due

©2022 Hedge Fund Law Report. All rights reserved.

diligence periodically or holding meetings with the firm's data science team to understand how the data flow is happening are two ways to monitor vendors, Albert suggested. Due diligence that was conducted in the beginning of a vendor relationship is not necessarily relevant for the entire life of the relationship, Rozenblit agreed.

See "Key Compliance Considerations for Fund Managers Using Alternative Data" (Jan. 9, 2020); as well as our two-part series on best practices for using alternative data: "Data Gathering and Managing Data Providers" (Feb. 6, 2020); and "Mitigating Regulatory and Other Risks" (Feb. 13, 2020).

## Materiality of Alternative Data

The SEC views alternative data on a risk-based basis, Rozenblit explained. Examiners may take into account the following indicia when considering whether data is material:

1. *Cost*: Cost is assumed to be correlated with the usefulness of the data, and the more useful the data is, the more likely it is to be material.
2. *Accuracy*: To the extent a firm is testing the data and can determine how predictive it is for the target metric, the accuracy of the data also feeds into the risk analysis.
3. *Confidentiality*: If a data vendor offers to sell a data set to a small group of customers for an increased fee, it could be viewed as an indication of MNPI.

The safest approach is to assume all data is material and then determine what is nonpublic, Rozenblit recommended. Any data from a publicly available source is probably lower risk. In many situations, there are no clear answers, so seeking advice from counsel can protect decisions made around materiality, duty and use of data issues, he added.

See "AIMA Report Outlines Adoption, Challenges and Prospects for Use of Alternative Data by Hedge Fund Managers" (Jun. 4, 2020); and "Report Calls for Transparency and Development of Standards in the Alternative Data Market" (Apr. 30, 2020).

# *Panuwat*

In SEC *v. Matthew Panuwat*, the SEC alleged that Panuwat, then head of business development at Medivation, a biopharmaceutical company, purchased stocks options in Incyte, another biopharmaceutical company, within minutes of learning highly confidential information about the planned acquisition of Medivation by Pfizer. According to the August 17, 2021, complaint, Panuwat knew that the acquisition of Medivation would increase Incyte's stock price.

*Panuwat* is the first instance of the SEC litigating a so-called "shadow trading" case. Panuwat learned material information about his employer that he used to trade in the stock of a different company that was likely to be affected by the news. Fund managers managing public and private positions can be regularly or sporadically receiving MNPI that could easily have implications for other companies and sectors, Schonfeld noted.

## Implications Could Be Far-Ranging

*Panuwat* may be an uncommon set of facts and circumstances, Rozenblit and Schonfeld agreed. The breadth of potential implications is wide, however, and the defense bar may try to obtain additional information from the SEC

©2022 Hedge Fund Law Report. All rights reserved.

about the Commission's views, Burke said. It is highly unlikely that the case stands for the proposition that an employee cannot trade in anything in which MNPI has some bearing, Schonfeld opined, but it is a very litigable issue.

Although the action was filed recently, compliance teams and outside counsel should consider this additional theory of liability as part of the MNPI issues they handle, Albert recommended.

See "'Shadow Trading' Theory of Insider Trading and the Implications for Private Fund Managers" (Sep. 23, 2021).

## Suggested Compliance Response

CCOs should review information barrier and restricted list policies, Albert suggested. Significantly expanding restricted lists, however, may be impractical, Rozenblit and Schonfeld agreed.

Employee training – whether through an ad hoc session for investment professionals or as part of the firm's annual compliance training – should include discussions of *Panuwat*, as well as refreshers on the scope of confidentiality agreements and non-disclosure agreements that the firm enters into when receiving MNPI, Albert advised. Portfolio managers and analysts must understand that they should involve legal and compliance before using MNPI from one company to trade in a different company.

Rozenblit suggested enhancing training on the definitions of duty and insider trading and emphasizing the idea that information unrelated to a transaction can be viewed as MNPI. Data obtained from portfolio activities that is then used to make trades or investments in other parts of the portfolio should be analyzed, he added. If the data is MNPI, users of the data should ensure they have the data source's permission to use it in that manner.

If there are ways to surveil for trading patterns that could indicate potential shadow trading, CCOs should consider investing time and energy into implementing those methods, Albert suggested.

For more on both enforcement actions, see "SEC Focus on Private Fund Managers: Alternative Data and 'Shadow Trading' (Part One of Two)" (Dec. 2, 2021).

©2022 Hedge Fund Law Report. All rights reserved.