Davis Polk

Spoofing Rule Governing Commodities Trading Survives Constitutional Vagueness Challenge in the Seventh Circuit

August 14, 2017 | Client Update | 7-minute read

In a closely watched **case**, the Seventh Circuit last week affirmed the felony conviction of Michael Coscia, a New Jersey high frequency trader, rejecting his arguments that the anti-spoofing provision in the Commodity Exchange Act under which he was charged is unconstitutionally vague and that the evidence in the record did not support his spoofing conviction. Coscia, the owner of Panther Energy Trader, was sentenced in 2016 to three years in prison after a jury found him guilty of committing six counts of spoofing and six counts of commodities fraud on the CME Group Markets and ICE Futures Europe. We focus on Coscia's spoofing conviction, since it is a relatively new statutory basis of liability, as compared to the more traditional liability based on commodities fraud.

The Dodd Frank Act amended the Commodity Exchange Act in 2010 to explicitly provide that spoofing is a violation of federal law and to make a knowing violation of the anti-spoofing prohibition a felony. Each felony count of spoofing carries a maximum sentence of 10 years imprisonment and a $1 million fine.

While spoofing can take many forms, it typically involves placing a large order that is not intended to be executed on one side of the market, away from the market clearing price, to create an illusion of demand at the artificially elevated or depressed price (the "spoofing order"), while simultaneously placing a small order that is intended to be executed on the other side of the market, at an advantageous price that is not the market clearing price unless the market were to move in reaction to the spoofing order. The anti-spoofing provision in the Commodity Exchange Act defines spoofing as "bidding or offering with the intent to cancel the bid or offer before execution." The provision has been criticized by traders and other industry observers, who have contended that the overbroad language could potentially pick up many types of legitimate trading. Significantly, the Seventh Circuit's panel opinion authored by Judge Ripple provided some guidance to distinguish unlawful spoofing from lawful trading in which orders are intended to be cancelled under specific conditions, but are nonetheless designed to be executed and are executable under other conditions.

– ***Intent to Cancel.*** Both the federal district court in which Coscia was tried and the Seventh Circuit focused in their rulings on the anti-spoofing statute's intent to cancel requirement, stating that it requires the prosecution to prove intent and knowledge. As Judge Ripple noted, this requirement undermines any argument that the statute fails to give ordinary people fair notice of the conduct it punishes or invites arbitrary enforcement:

"Importantly, the anti-spoofing statute's intent requirement renders spoofing meaningfully different from legal trades such as "stop-loss orders" ("an order to sell a security once it reaches a certain price") or "fill-or-kill orders" ("an order that must be executed in full immediately, or the entire order is cancelled") because those orders are designed to be executed upon the arrival of certain subsequent events. Spoofing, on the other hand, requires, an intent to cancel the order at the time it was placed. The fundamental difference is that legal trades are cancelled only following a condition subsequent to placing the order, whereas orders placed in a spoofing scheme are never intended to be filled at all."

– ***Proving Intent – Architecture of The Trading Algorithm and Testimony of Algorithm Designer.*** The Seventh Circuit discussed the design of the trading algorithm used by Coscia and noted that the criteria used to cancel the large orders was consistent with a finding that the algorithm was "specifically designed to cancel [the spoofing orders] if they ever risked actually being filled." Also in evidence was testimony given at trial by the programmer, who stated

that he was instructed by Coscia to design a program that could act "[l]ike a decoy," which would be "[u]sed to pump the market."

- ***Trading Record.*** In finding that a rational trier of fact could have found that Coscia acted with intent to cancel the large orders at the time he placed them, the Seventh Circuit also considered Coscia's actual trading record that was introduced at trial. This data showed a dramatically skewed execution rate between Coscia's small orders and large orders, and that Coscia's track record deviated from industry averages. For example:
  - On the CME, approximately 1 in 3 orders (about 36%) of Coscia's small, non-spoofing orders were filled, whereas less than 1 in 1,000 (about 0.08%) of his large, spoofing orders were filled; and
  - Coscia's order-to-trade ratio (ratio between his orders and executed trades) was 1,600%, whereas other market participants ranged an average of 90% to 260%.

Regulators have been active recently in pursuing spoofing cases [1]. Coscia and his firm were originally the subject of a CFTC enforcement action in July 2013. More recently, in January 2017, the CFTC brought an enforcement action against **Citigroup Global Markets Inc.** ("CGMI"), involving alleged spoofing. CGMI agreed to pay a $25 million civil penalty, take certain corrective actions, and cooperate with the CFTC and other governmental bodies in investigations related to the subject matter. In another alleged spoofing case, on August 7, 2017, the CFTC brought an enforcement action against **The Bank of Tokyo-Mitsubishi** ("BTMU"), in which BTMU agreed to pay a $600,000 civil penalty and cooperate with the CFTC and other governmental agencies in related investigations. In both the CGMI and BTMU settlement orders, while there was a finding that traders engaged in spoofing, there was no specific analysis of how and why the trading strategies used by those traders manifested an illegal intent to cancel, as opposed to a lawful intent to cancel associated with legitimate trading strategies.

Implications for Traders, Firms and Their Advisors
While there is still significant uncertainty as to where regulators and the courts will draw the line between legitimate trading and spoofing, below are some practical steps that could be taken to help mitigate risk and to better position parties in the event of a regulatory or criminal inquiry or investigation:

- Given the courts' focus on intent, traders and firms should take care to articulate and document the purpose of particular trading strategies. Where a particular strategy or algorithm involves placing orders with pre-programmed cancellation triggers, it will be important to explain their purpose and the reasons why they are legitimate, and why the canceling of trades is not intended for manipulative or disruptive purposes. The process should be vetted and documented as early as possible, rather than being an after-the-fact, check-the-box exercise, where the final documentation may be inconsistent with earlier internal emails, recorded conversations or other communications and discussions.
- Training of traders, algorithm designers and other related personnel will be critical to explain to them key legal concepts and developments in this area.
- In light of the enhanced use of technology by exchanges, regulators and prosecutors to investigate and prosecute cases, firms should consider enhancing their own internal capabilities for monitoring and detecting potentially problematic trading behavior.

We remind our readers of, and provide an easy-to-access link to, the **CFTC's interpretive guidance on spoofing**[2].

[1] The securities laws do not explicitly define prohibited spoofing; however, they do prohibit market manipulation and fraudulent conduct in connection with the offer and sale of securities. The SEC has been active in investigating and bringing cases on the basis of manipulative or disruptive trading behaviors such as spoofing and layering. Most recently, the SEC filed a complaint on March 10, 2017 in the Southern District of New York against Avalon FA Ltd., a Ukrainian trading firm based in Kiev, its principals, and U.S. broker-dealer, Lek Securities Corporation, and its CEO, Samuel Lek, alleging participation in and aiding and abetting of layering and cross-market manipulation schemes in violation of Sections 9(a)(2), 10(b), and 20(a) of the Exchange Act and Rule 10b-5 and Section 17(a) of the Securities Act. According to the SEC, Avalon openly "touted itself" as a destination for traders who wished to engage in "layering", a type of spoofing in which orders are placed but later cancelled after others buy or sell securities at artificial prices based on the appearance of substantial supply or demand in the market. The case remains pending before Judge Denise Cote.

[2] The CME and ICE Futures have also issued guidance on spoofing. See CME Market Regulation Advisory Notice on Disruptive Practices relating to CME Rule 575 and ICE Futures U.S. Guidance on Disruptive Trading Practices. Unlike the CFTC and federal prosecutors, the exchanges have taken the position that only a mens rea of "recklessness" need be proven to find a violation.

If you have any questions regarding the matters covered in this publication, please reach out to any of the lawyers listed below or your usual Davis Polk contact.

Stefani Johnson Myrick
+1 202 962 7165
stefani.myrick@davispolk.com

Annette L. Nazareth
+1 202 962 7075
annette.nazareth@davispolk.com