Bloomberg Law®

Securities Regulation & Law Report™

ENFORCEMENT

The Blackest Box: How the Government Tries to Squeeze Algorithmic Traders in Spoofing Cases and Ways to Break Free

BY DAVID MCGILL AND BENJAMIN SAUTER

Now that the long-rumored wave of new spoofing cases has materialized, futures traders should familiarize themselves with what it takes to mount an effective defense against charges brought by the Justice Department. Obviously, in cases in which the DOJ has the benefit of written communications (such as emails, chats, or texts) and technical records (such as proprietary source code and configuration files) evidencing a clear strategy to place orders with unconditional intent to cancel before execution, then even the most sophisticated and skilled defense attorney is unlikely to dissuade the DOJ from bringing charges, let alone prevail at trial. But, in many cases, direct evidence of trader intent is unavailable or at least ambiguous. These cases create an opportunity to combat allegations of spoofing with data-driven defenses.

David McGill is a litigator and investigator with Kobre & Kim whose practice resides at the intersection of finance and technology.

Benjamin Sauter is a Kobre & Kim litigator who focuses on cutting-edge financial products and services disputes.

The Government Squeeze Play in Contested Spoofing Cases

The Commodity Exchange Act defines spoofing as ''bidding or offering with the intent to cancel the bid or offer before execution.'' 7 U.S.C. § 6c(5)(C). Putting aside the threshold question of whether this statutory definition is unconstitutionally vague — a question this firm petitioned the U.S. Supreme Court to review in *United States v. Coscia* — the DOJ and its civil counterpart, the Commodity Futures Trading Commission, often evaluate a trader's intent in placing orders with reference to a few surface-level trading characteristics, such as the speed and volume trading activity, cancellation rates, and the extent to which a trader placed orders on both sides of the bid-offer spread. Yet, for those with even a passing familiarity of the futures markets, the government's seemingly myopic focus on these characteristics makes little sense: After all, the futures markets are dominated by high-speed and high-volume trading conducted through complex algorithms, most of which generate cancellation rates exceeding 90 percent, and include market-making strategies and/or hedging functionality that systematically produce order activity on both sides of the order book.

 ISSN 0037-0665

Unfortunately, for judges and jurors unfamiliar with the nuances of the futures markets, evidence of a trader repeatedly placing and canceling orders within milliseconds on both sides of the market sure looks like a credible factual predicate for a high-tech scheme. And while skilled defense attorneys can do much to educate courts and jurors as to the ubiquity of these characteristics and other realities of the futures market, the suspicions that gaudy order and cancellation statistics generate are not easily abated. Likewise, for the average juror used to interacting with traditional markets in traditional ways, the near-constant expression of a simultaneous desire to both buy and sell seems counterintuitive and indicative of some nefarious intent.

Making matters worse, the government has the advantage of cherry-picking instances of order activity from pools of many thousands to frame its charges. Rest assured, trading instances are carefully scrutinized and specifically selected for the purpose of portraying the defendant in the worst possible light. The government thus seeks to have it both ways: It uses high-level statistics to showcase high rates of rapid cancellations in select markets (which they also choose), while also attempting to handcuff defendants to examples of trading activity that are difficult to defend in isolation. This is a scary box for algorithmic traders to find themselves in.

Breaking Free of the Government Box

So, with the government squeezing traders into the box from both sides, what, if anything, can traders do to break free from misguided spoofing allegations? Well, as the old saying goes, if you can't win the game, change the rules. Ultimately, an effective spoofing defense requires shifting the battlefield away from the characteristics and trades the government chooses and onto terrain where the defense has an opportunity to showcase trading characteristics and transactions that undermine government allegations and evince an intent to execute.

First, where the government places a specific trading algorithm at issue, it is more than fair game for the defense to illustrate the ways in which the algorithm (and its data trail) reveal the trader's intent to execute. While evidence of a high number of fills can be helpful, traders who find themselves in the government's crosshairs are typically on the high end of marketwide cancellation rates. So overemphasizing the number of fills in absolute terms can create credibility problems and expose the defense witnesses to aggressive cross-examination and government rebuttal. For that reason, it is usually more effective to delve deeper into the order data and focus on concepts (and supporting data) that go beyond cancels and fills. For example:

- Resting Time
  - o Futures markets are among the fastest and most liquid in the world. And, in most spoofing cases, the government accuses the defendant of conducting a series of high-speed pump fakes designed to get other market participants to move in one direction, so that the defendant can move in the other and soak up liquidity at a favorable price. But allegations of spoofing schemes orchestrated in this way run into trouble when the defense can adduce evidence, through statistical sampling and exemplars, that the trader and algorithm in question left orders resting and available for execution for lengths of time within or beyond market norms.
- Queue Positioning
  - o Particularly in the most liquid of futures markets, such as those for U.S. Treasury futures contracts, government witnesses would likely concede that large, aggressive orders can hit the market at any moment. Indeed, prices fluctuate on a near-constant basis in these markets. For a price to change, the entire supply for a given price level — often consisting of hundreds of contracts — has to be absorbed by one or more aggressive orders. Thus, evidence that a trading algorithm was designed to position orders at top of book (i.e., the best available price) tends to suggest that the trader intended his orders to be subject to a high risk of execution. And if the defense can produce evidence that a trader (or algorithm) sought to systematically gain priority in the order queue, the overall effect can be quite destructive to government's efforts to prove the trader's intent was to avoid getting filled.
- Partial Fills; Orders Left Open
  - o Available CFTC guidance confirms that partial-fill activity is supportive of intent to execute. *See* Antidisruptive Practices Authority, 78 FR 31890-01 (May 28, 2013). But although evidence of partial fills can support an inference of intent to execute, evidence that a trader (or algorithm) left an order resting in the market even after it was partially filled is very strong evidence of intent to execute. From a defense point of view, any trader who truly desired to cancel their orders before execution would surely act on that desire as soon as his or her orders started getting hit. Leaving the remaining quantity of an order open and resting in the queue after partial execution is the exact opposite of what one would expect a trader to do if he did not want to execute.
- Automated Hedging Functionality
  - o The government tends to focus its enforcement efforts on the most aggressive traders in the marketplace. While this creates certain challenges for the defense when the government inevitably puts forward a comparative statistical study and casts the defendant as a rogue ''outlier,'' it also creates opportunities on a trade-by-trade basis. For example, the government often seeks to make a statistical showing as to the frequency with which ''large'' orders were placed and rapidly canceled in the market, but often lost in the analysis is the precise technical explanation for this activity. Wherever possible, the defense should put forward evidence of these cancellations being triggered by automated hedging functionality. Typically, ''auto-hedge'' functions are preprogrammed to cancel orders based on detection of changes in objective market conditions. While such evidence does not directly speak to the logic behind the order placement, it nonetheless proves that the decision to cancel was not predetermined, but rather a byproduct of evolving market conditions. This is the antithesis of spoofing.

Ultimately, although defending spoofing allegations in futures cases comes with no shortage of challenges, traders who find themselves in the government's crosshairs must align themselves with counsel capable of developing and advancing defenses grounded in the technology and order data that's under scrutiny. To be sure, the defense themes described above represent

  SRLR ISSN 0037-0665

only a subset of the possibilities: There are many others that cannot be described here without revealing proprietary trading strategies. And just as designing a profitable trading strategy requires detailed understanding of the markets and collaboration with knowledgeable developers, implementing an effective defense strategy to break free from spoofing charges likewise requires shared expertise, creativity, and teamwork among traders and counsel.