MARKET REGULATION SERVICES

Case Study

SEC CONCERNS ON SPOOFING

FIRM PROFILE

A Hedge Fund conducting high-speed algorithmic trading in listed equities. The Fund has had regulatory investigations on spoofing in the past. Average daily volumes are approximately individual 9,000 executions.

MOST APPLICABLE RULES

Section 17(a) of the Securities Act as well as Sections 9(a)(2) and 10(b) of the Exchange Act and Rule 10b-5.

BUSINESS NEEDS

The Fund required an independent third-party review and attestation in regards to their trading activities to use in a response to an SEC investigation. Of particular concern was the period 30 minutes and less prior to the market close and the trading activity around "market on close" imbalances. The Fund did not have adequate systems to properly analyze these occurrences.

PROVIDED SOLUTIONS

After initial conversations, we asked for and received a large dataset of electronic trading-related records, including orders, fills, rejections, and cancellations with all the relevant time stamps and metadata. We created a database structure and query engine to look for the sequences of events whereby spoofing would have to occur. The initially very large dataset could then be reduced down to a workable dataset based on the result of our custom filtering engine. The filtered combinations of orders and other relevant data could then be analyzed with a set of reports generated from the dataset.

Upon completion of the initial results, it was determined that instances of spoofing may have occurred, but the root cause in this case could not be determined without conducting a code review on the relevant trading algorithms. It may have been that the observed instances of possible spoofing were merely due to time discrepancies between the Fund and the Exchanges or it may be legitimately a result of specific programmatic code. Upon acceptance and approval of a proposal to conduct a code review, a full review of the relevant algorithmic code was conducted.

Our independent review determined that the specific algorithms at play had substantial error and event logging functionality at key points in the logical decision making processes. Therefore, if intentional spoofing was occurring it would be well documented in those log files as exceptions to key logical decision points in the algorithms. We requested the log file data for analysis.

The log file analysis we conducted did not show events occur at key decision points that would point to deliberate spoofing. Upon further analysis of all materials it was concluded that the identified potential spoofing instances were a result of very small differences in systems clocks. The time differences between the executing terminal, the local servers, and the exchange were just enough to create anomalies in the data that would look like spoofing. The independent review was completed to the satisfaction of the client who appreciated the comprehensive analysis that they could use in their SEC response.

*Please note specific facts in this case have been altered to protect client confidentiality.