Market Abuse Case Studies

BAZUR Spol. S.R.O. Spoofing

Market Abuse Case Study No: 010	Name: BAZUR Spol. S.R.O. (BAZUR) Spoofing
Offence: Spoofing and engaging in a manipulative and deceptive scheme resulted in the violation of the Commodity Exchange Act and Commodity Futures Trading Commission (CFTC) regulations	**Detection Control:** MAST Layering/ Spoofing Metric

TradingHub

BAZUR Spol. S.R.O. Spoofing

1. Key Facts and Overview

In December of 2021, the Commodity Futures Trading Commission (CFTC) announced the U.S. District Court for the Northern District of Illinois entered a consent order, resolving CFTC charges that Roman Banoczay Jr. (Banoczay Jr.) of Bratislava, Slovakia, as an agent of Roman Banoczay Sr. (Banoczay Sr.) and their company, BAZUR Spol. S.R.O. (BAZUR) engaged in spoofing and in a manipulative and deceptive scheme to defraud the Chicago Mercantile Exchange (CME) Crude Oil futures market in violation of the Commodity Exchange Act and CFTC regulations.

The CFTC order imposed a $750,000 civil monetary penalty against Roman Banoczay Jr. and prohibited all three defendants from trading in commodity markets and/or registering with the CFTC in any capacity for two years. Additionally, the CFTC order required them to cease and desist from violating the Commodity Exchange Act's prohibitions on spoofing and manipulative and deceptive schemes to defraud.

2. Findings and Allegations

The CFTC order noted that Banoczay Sr. held trading accounts at a futures commission merchant headquartered in Greenwich, Connecticut. These accounts included a primary account in the name of Banoczay Sr. and two subaccounts, one in the name of Banoczay Sr. and another in the name of BAZUR. However, Banoczay Jr. entered orders and executed trades through the accounts and was the only person who did so. Banoczay Sr. and BAZUR authorised and were aware of Banoczay Jr.'s trading.

During a four-week period in early 2018, Banoczay Jr. repeatedly engaged in spoofing (bidding or offering with the intent to cancel the bid or offer before execution) while placing orders for and trading Crude Oil futures contracts on the CME's exchanges. Banoczay Jr. placed thousands of orders with the intent to cancel them, to send false signals of increased buying or selling interest designed to trick market participants into executing the orders that he wanted to be filled.

Banoczay Jr.'s spoofing came after several significant trading losses. Specifically, he lost over $289,000 on January 10, $624,000 on January 24 and $87,000 on January 26. Following these large losses, Banoczay Jr. started implementing his spoofing strategy on January 16. From that point through the end of January, he engaged in between 7 and 77 spoofing events daily. In February, Banoczay Jr.'s spoofing continued and increased. By February 2, he was executing 76 to 340 spoofing events per day until February 12, when he engaged in more than 700 spoofing events in a single day. After that, his futures commission merchant put a hold on his account.

During that period, Banoczay Jr. engaged in approximately 2,000 distinct spoofing events. These 2,000 events encompassed more

than 19,000 individual spoof orders. Banoczay Jr.'s spoofing was successful in helping to offset his earlier trading losses. For example, from February 2 through February 12, he earned more than $332,000 in profits over eight days of trading.

The CFTC order noted the spoofing scheme followed a pattern where Banoczay Jr. would enter a small order, typically between one and forty lots, for Crude Oil futures that he intended to execute. Within seconds before or after entering the small order, he would rapidly place a series of much larger spoof orders at various price levels on the opposite side of the market. He would then cancel his spoof orders within seconds of filling his genuine order. The spoof orders accounted for a far greater total volume than the genuine orders. The average ratio of spoof order lots to genuine order lots was about 8-to-1.

The CFTC found that Banoczay Jr.'s spoof orders were intended to send a false signal to the market or, at a minimum, were entered with reckless disregard to the fact that entering these orders would send a false signal to the market. Furthermore, these signals also injected false information about supply and demand into the market. Banoczay Jr. knew or recklessly disregarded that the false information about supply and demand would lure market participants into trading against his orders on the opposite side of the market, thus enabling him to get filled sooner, at a better price, or in larger quantities than he otherwise would.

The CFTC order noted that Roman Banoczay Jr.'s conduct violated Sections 4c(a)(5)(C) and 6(c)(1) of the Act, 7 U.S.C. §§ 6c(a)(5)(C), 9(1), and Regulation 180.1(a)(1), (3), 17 C.F.R. § 180.1(a)(1), (3) (2022), which prohibit engaging in any trading, practice, or conduct that is, is of the character of, or is commonly known as, "spoofing," i.e., bidding or offering with the intent to cancel the bid or offer before execution. See United States v. Coscia, 866 F.3d 782, 795–96 (7th Cir. 2017) (affirming conviction for spoofing where evidence showed that the defendant entered three orders with the intent to cancel before execution). The regulations also prohibit using or employing, or attempting to use or employ, any manipulative device, scheme, or artifice to fraud, or engaging, or attempting to engage, in any act, practice, or course of business, which operates or would operate as a fraud or deceit upon any person, in connection with a contract of sales of any commodity for future delivery on or subject to the rules of a registered entity. See, e.g., Skudder, 2022 WL 17752392.

Although Banoczay Jr. was the only individual who placed and cancelled these spoof orders, the court found that Banoczay Sr. and BAZUR are vicariously liable for Banoczay Jr.'s violations because he served as their agent and committed these violations within the scope of his agency.

Detecting Spoofing with MAST

The consent order provides several examples of the market abuse performed by Banoczay Jr., for example, on January 25th 2018. A representation of this scenario has been run through MAST. The screenshot illustrates how the MAST website presents the scenario:
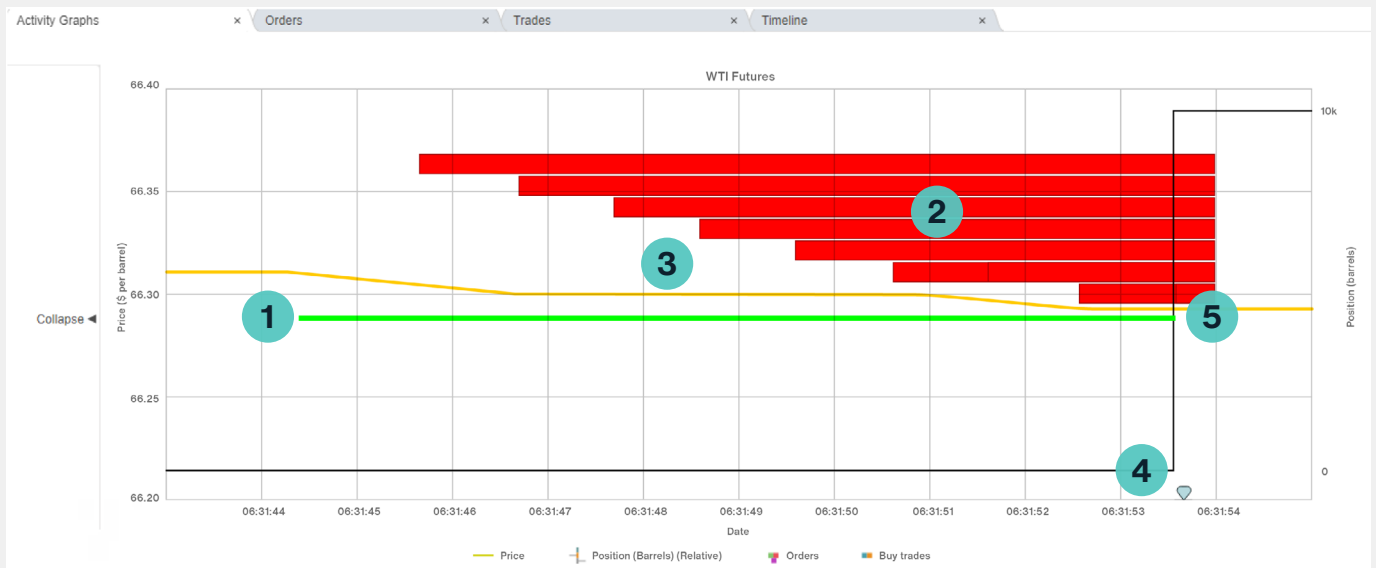
1. The genuine buy order for 10 futures contracts is placed by Banoczay Jr. and represented as a green bar in the MAST graph.

2. Banoczay Jr. places a series of larger orders to sell 40 futures contracts, which are represented by red bars.

3. The yellow line shows the mid-price for the instrument, which trends downwards during this period.

4. The buy order is filled which results in Banoczay Jr. taking a position of 10k barrels.

5. The spoof orders are quickly cancelled after the genuine order has been filled.

How MAST Recognises Price Manipulation

MAST's Cross-Product Layering/Spoofing metric detects spoofing by measuring the degree to which the market impact of a potential spoof order benefits any transactions on the other side of the market. It balances this benefit with the risk to the trader of placing a spoof order, namely the cost to them of having to unwind an unwanted execution.

By measuring market impact, MAST is able to recognise that Banoczay Jr.'s non-bona fide orders exerted downward pressure on the instrument's price. This led to the cancellation of buy orders in the market above his buy order and moved his resting order closer to the front of the queue, ultimately allowing his buy order to be filled. The metric derives its materiality score, for instance, by considering both the benefit to the buy order and the hypothetical cost of having to unwind his large spoof sell orders.

Advance your surveillance function

Improve your detection of market abuse, reduce false positives and prioritise high-risk alerts.

Reach out to learn more.

🌐 tradinghub.com/MAST

✉ tradesurveillance@tradinghub.com