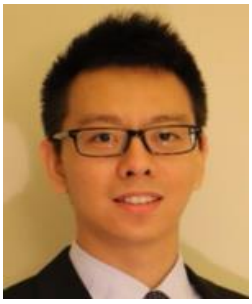
Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

An Update On Spoofing And Its Challenges

By **Ilan Guedj and An Wang** (March 16, 2018, 12:14 PM EDT)

Ilan Guedj



An Wang

Spoofing[1] is a type of trading behavior in which traders attempt to create an artificial impression of market conditions by posting orders without intending to execute the orders. Recently, we have seen an increasing number of convictions and settlements involving spoofing, as well as a step-up in enforcement by regulators. This article reviews recent developments in litigation and the challenges in identifying spoofing activities.

Recent Developments in U.S. v. Michael Coscia

In the landmark spoofing case U.S. v. Michael Coscia, the founder and trader at Panther Energy Trading LLC, Coscia, was indicted in October 2014 for six counts of spoofing in 2011 in foreign exchange, metal and other commodity futures.[2] Coscia was found guilty and sentenced to three years in prison in July 2016.[3]

In November 2016, Coscia appealed on the grounds of (1) the "unconstitutionally" vague anti-spoofing provision, (2) the lack of adequate notice, and (3) the lack of evidence supporting the conviction. In August 2017, the Seventh Circuit rejected all these challenges. In particular, to address Coscia's third argument, the appellate court cited, among other statistics, Coscia's stark order-to-trade ratio of 1,592 percent, in comparison to other market participants' 91-264 percent range.[4]

In February 2018, Coscia took his appeal to the U.S. Supreme Court, again based on the grounds of unconstitutional vagueness of the provision, and whether intent alone can convert bona fide trades into fraud.

On his second point, Coscia argued and cited the CEO of the Chicago Mercantile Exchange that "bids and offers on the electronic platform do not create an appearance of 'false market depth' as all bids and offers ... [are] true and actionable ..." Thus, based on Coscia's argument, as long as orders are "true and actionable," they are "not false, deceptive, or fraudulent."[5]

In the petition, Coscia also compared spoofing orders to "iceberg" or "hidden quantity" orders, pointing out that they are also designed to conceal "the true extent of supply or demand," yet the U.S. Commodity Futures Trading Commission and the U.S. Department of Justice have agreed that they are permissible.[6] Just like a real iceberg, an iceberg order only shows a small portion above the water,

while “hiding” the rest of its mass. In other words, an iceberg order allows the trader to display only a preset and often very small quantity of the total amount, potentially disguising a large order in the order book. An iceberg order will be executed by increments of the preset display quantity until it is fully filled or canceled.

To demonstrate the exceptional importance of the questions at-issue, Coscia emphasized that “... the decision ... leaves the commodity futures markets utterly unclear as to what trading activity is permissible, and what trading activity is a deferral felony punishable by imprisonment,” and that “there is an equally shared interest [among participants and regulators] in ensuring that market participants have the clarity they ‘deserve.’”[7]

Recent Developments in Other Litigations

On Sept. 13, 2017, the DOJ pressed a criminal charge against former UBS trader, Andre Flotron, for engaging in spoofing on the Commodity Exchange Inc., or COMEX, gold and silver futures market. The complaint pointed out that Flotron placed large orders for precious metals futures at certain price levels with the intent to cancel before execution to create a false appearance of abundant supply or demand in order to move market price.[8] On Jan. 26, 2018, the CFTC filed a civil complaint against Flotron for spoofing.[9] Flotron was indicted in the DOJ criminal suit on Jan. 30, 2018.[10]

On the same day, the CFTC also filed a civil complaint against two former Deutsche Bank traders for allegedly engaging in spoofing in the metals futures market.[11] According to the complaint, James Vorley and Cedric Chanu spoofed on COMEX and the New York Mercantile Exchange, or NYMEX, for gold, silver, platinum and palladium futures numerous times from May 2008 through at least July 2013; they also allegedly taught an unnamed subordinate trader how to spoof.

Chat-room conversations cited in the complaint are consistent with “typical” textbook spoofing. Having learned the spoofing technique from Vorley and Chanu, the subordinate trader said to another trader at another financial institution, “[B]asically [I] sold out … just by having fake bids … [in] the futures … [I] just spam bids below … to clear my offer.”

In addition, chat-room conversations are highly suggestive of cross-trader spoofing; that is, one trader places spoofing orders to facilitate another trader’s executions. Chanu allegedly coordinated with another unnamed trader at Deutsche Bank to spoof. Shortly after the unnamed trader placed the spoofing order to help Chanu, the unnamed trader said, “[S]o glad [I] could help ... got that up 2 bucks.” The unnamed trader continued: “[T]hat does show u how easy it is to manipulate so[me]times.” Chanu replied, “[Y]eah yeah of course.” The unnamed trader continued: “[T]hat was alot of clicking.” Chanu replied: “[B]asically you tricked … the algor[i]thm.” The last response clearly shows the intent of the spoofing order is to deceive other market participants into transacting based on the false perception.

In October 2017, the CFTC fined a Dubai trading firm, Arab Global Commodities, $300,000, alleging that one of its traders spoofed on the COMEX copper futures market. Arab Global Commodities agreed to pay the civil monetary fine and fired the trader who allegedly engaged in spoofing.[12]

On Jan. 29, 2018, the DOJ and the CFTC charged seven individuals and three banks with deceptive trading executed in U.S. commodities markets. The eight individuals include the aforementioned James Vorley, Cedric Chanu, and five additional individuals — Edward Bases, John Pacilio, Jiongsheng Zhao, Krishna Mohan and Jitesh Thakkar, the owner of the software company that allegedly built a trading platform specifically designed to enable spoofing. The three banks are Deutsche Bank, UBS and HSBC.

While the DOJ announced criminal charges and indictments against the seven individuals, the CFTC rolled out combined civil fines of $46.6 million with the banks, in which Deutsche Bank agreed to pay $30 million, UBS agreed to pay $15 million, and HSBC agreed to pay $1.6 million.[13]

Challenges in Identifying Spoofing

Trades get routinely canceled — sometimes traders make an error and have to cancel the order, and often, market conditions change enough to change the trader's mind. Therefore, an important challenge in identifying spoofing is separating legitimate calculations from those that likely were intended to manipulate the market. To establish spoofing, several aspects of the data must be carefully analyzed.

First, order types and type-specific information must be reviewed carefully. For example, iceberg orders are types of orders that can be used in conjunction with spoofing. Just like a real iceberg, an iceberg order shows only a small portion above the water, while "hiding" the rest of its mass. In other words, an iceberg order allows the trader to display only a preset and often very small quantity of the total amount and gets executed by increments of the preset display quantity until it is fully filled or canceled. This feature allows the trader to disguise the true volume of the order that can potentially be large enough to influence market price.

Second, how large is large enough for the volume of the spoofing order to be able to impact perceived market conditions? This question has to be answered within the context of the specific market one is investigating. Moreover, the spoofing order need not be one single gigantic order. In a technique called "layering," traders can place multiple small-volume orders to build up a substantial position in order to create a false sense of imbalance in the market.

Third, the timeline of the actions is crucial in establishing intent. Depending on the prevailing trading frequency in the market, the time elapsed from the placement to the cancellation of a spoofing order can range from milliseconds to minutes. Thus, in analyzing spoofing, it is crucial to obtain a deep and comprehensive understanding of the overall market condition and market-specific trading patterns.

Conclusion

Spoofing is a type of manipulative trading behavior prohibited jointly by the Dodd-Frank Act and the Commodity Exchange Act. In recent years, the DOJ, the CFTC and other regulators have increased their coordination and effort in cracking down on spoofing and market manipulation, yielding an increasing number of criminal indictments and civil settlements. To analyze spoofing and investigate intent, many aspects such as order type, order volume, timeline and prices must be studied comprehensively to arrive at meaningful conclusions.

Ilan Guedj, Ph.D., is a principal with Bates White LLC in Washington, D.C., where he specializes in providing economic analysis and expert testimony in the areas of securities and finance and anti-competitive activities in financial markets. An Wang, Ph.D. is a senior economist with Bates White in Washington and provides economic analysis in the areas of securities and finance and anti-competitive activities in financial markets.

[1] “Layering” is a more specific form of spoofing in which traders place multiple orders that they do not intend to execute. See a recent SEC action on the topic: Jon Hill, “Broker-Dealer Seeks ‘Layering’ Docs from FINRA for SEC Suit,” Law360, Feb. 9, 2018.

[2] U.S. v. Coscia, No. 1:14-cr-00551 (D. N. Ill., Oct. 1, 2014).

[3] See Department of Justice, U.S. Attorney’s Office for the Northern District of Illinois’s Release, “High-Frequency Trader Sentenced to Three Years in Prison for Disrupting Futures Market in First Federal Prosecution of ‘Spoofing.’”

[4] U.S. v. Michael Coscia, No. 16-3017 (U.S. Court of Appeals for the Seventh Circuit, Aug. 7, 2017).

[5] Michael Coscia v. the U.S., No. 17A527 (Supreme Court).

[6] Michael Coscia v. the U.S., No. 17A527 (Supreme Court).

[7] Michael Coscia v. the U.S., No. 17A527 (Supreme Court).

[8] U.S. v. Flotron, No. 3:17-mj-01467 (D. D. C., Sep. 13, 2017).

[9] CFTC v. Flotron, No. 3:18-cv-00158 (D. D. C., Jan. 26, 2018).

[10] U.S. v. Flotron, No. 3:17-mj-01467 (D. D. C., Jan. 30, 2018). This indictment supersedes U.S. v. Flotron, No. 3:17-cr-00220-JAM, (D. D. C., Sep. 26, 2017).

[11] CFTC v. Vorley et al., No. 1:18-cv-00603 (D. N. Ill., Jan. 26, 2018).

[12] In re: Arab Global Commodities DMCC, Docket no. 18-01 (U.S. Commodity Futures Trading Commission, Oct. 10, 2017).

[13] Dunstan Prial, “3 Banks to Pay Combined $47M in CFTC Spoofing Settlement,” Law360, Jan. 29, 2018.