

## What To Expect From The 2nd Criminal Spoofing Trial

By Jeffrey Brown, Conrad Johnson and Brendan Herrmann

(April 10, 2018, 1:01 PM EDT)

A judge in the District of Connecticut paved the way last month for what the U.S. Department of Justice has described as “the second spoofing case that will go to trial in the country.”[1] By denying the defendant’s motion to dismiss the criminal conspiracy charge against him, the court set the stage for a trial to begin on April 16.[2] Potential U.S. Supreme Court review of the validity of the nation’s first spoofing conviction has not deterred the DOJ and the U.S. Commodity Futures Trading Commission from launching a wave of new criminal and civil spoofing cases against numerous defendants in a self-styled “spoofing takedown” this January.[3] Indeed, recent developments suggest that regulators are more willing than ever to try spoofing cases based on supposed patterns observed in market data even without contemporaneous communications that suggest an intent to engage in manipulative trading.

### Overview of Spoofing

“Spoofing” is a manipulative trading practice sometimes employed by participants in the futures and other commodities markets that carries both civil and criminal penalties. Congress passed a civil prohibition against spoofing as part of Dodd-Frank’s amendments to the Commodity Exchange Act,[4] and a separate provision of the CEA creates felony criminal exposure for traders who “knowingly” violate the prohibition against spoofing.[5] The DOJ can also criminally charge traders who engage in spoofing under the more traditional wire fraud and securities/commodities fraud provisions of the criminal code.[6]

At bottom, the CEA’s anti-spoofing provision prohibits “bidding or offering with the intent to cancel the bid or offer before execution.”[7] The conventional manipulative strategy behind spoofing involves a trader placing orders on both sides of the market (i.e., simultaneous orders to buy and to sell) while desiring to trade orders on only one side. The trader intends to use the opposite-side orders not to trade, but to create the illusion of price movement that leads other market participants to trade with the desired orders at a more favorable price than the trader would have been able to achieve without placing the opposite-side orders. A typical component of such a spoofing strategy is placing many more orders on the



Jeffrey Brown



Conrad Johnson



Brendan  
Herrmann

opposite side of the market, thereby creating a market imbalance to falsely convince other traders that the price is about to move in accordance with that perceived supply or demand.

The CFTC and the DOJ each believe that algorithmic traders are especially susceptible to being tricked by spoofing strategies. High-frequency algorithmic trading is prevalent in the commodity futures markets, and these algorithms typically make immediate trading decisions in reaction to short-term fluctuations in the imbalance of an exchange's visible order book — i.e., large discrepancies between visible orders to buy and orders to sell. As such, algorithmic traders can be induced quickly to trade with a spoofing trader before the algorithm can assess or detect that the spoofing trader's large opposite-side orders do not represent true market supply and demand. Many CFTC and DOJ spoofing cases, in fact, rely on algorithmic traders' allegations that a competitor's actions were intended to be manipulative.[8]

### **The Flotron Decision**

In separate cases each filed in the District of Connecticut, the DOJ and CFTC have alleged that Andre Flotron, a precious metals trader at a large global bank, engaged in a pattern of spoofing that lasted more than five years between July 2008 and November 2013 and spanned his tenures at the bank's Connecticut and, later, Switzerland offices.[9] Flotron allegedly adopted what the DOJ believes to be a prototypical spoofing strategy by using double-sided orders on the COMEX exchange operated by the CME Group to create a market imbalance.[10] Flotron supposedly used iceberg-type orders to disguise the true size of his desired orders and thereby exaggerate this imbalance.[11] He allegedly believed that this imbalance provoked a favorable reaction by algorithmic traders.[12] The DOJ moved quickly to arrest Flotron, a resident of Switzerland, upon learning that he arrived in the United States temporarily to visit his girlfriend living in New Jersey.

After a prior successful motion to dismiss some of the DOJ's charges in the superseding indictment on venue grounds,[13] Flotron further moved to dismiss the sole remaining conspiracy charge on the merits. The court denied Flotron's motion to dismiss in its entirety and, in doing so, illustrated the difficult burden imposed on any defendant seeking to dispose of a spoofing charge without a full criminal trial. The court held that the DOJ's description that Flotron placed simultaneous small orders on one side of the market and larger orders on the other side — coupled with the bare allegation that Flotron intended to cancel the large orders after manipulating the market price rather than to trade them — was sufficient to take the case to trial.[14]

The indictment did not include any factual support for the DOJ's allegation that Flotron intended to cancel his opposite-side orders at the time that he placed them other than that the orders were eventually canceled. The CFTC's parallel complaint has alleged that Flotron placed his opposite-side orders at prices sufficiently distant from the prevailing market price to comfortably prevent their execution and further modified those orders as the market price approached their level. The DOJ's indictment, on the other hand, contained no such allegations that remove Flotron's intent to cancel from the realm of hindsight.[15]

In denying Flotron's motion to dismiss the conspiracy charge, the court relied heavily on a recent Seventh Circuit decision upholding the first criminal spoofing conviction, *United States v. Coscia*. [16] As in *Coscia*, the court rejected arguments that Flotron's opposite-side orders could not constitute spoofing as a matter of law because they were real orders subject to the real risk that other market participants would trade with them.[17] The court further rejected Flotron's attempt to distance himself from *Coscia*. [18] Flotron pointed out that as a manual trader, unlike *Coscia*, he never designed or used any preprogrammed algorithms to cancel his orders after only milliseconds or otherwise to make them near-

impossible to execute.[19] On the contrary, Flotron called attention to the fact that his opposite-side orders remained in the market, on average, for 23 seconds prior to cancellation, and sometimes longer than a full minute.[20] The court decided that these circumstances went to the weight of the DOJ's evidence and not the indictment's legal sufficiency.[21]

### **Spoofing Comes in Different Patterns with Different Proof**

The differences in the alleged trading patterns described in Flotron and Coscia demonstrate the wide variety of the activity a regulator can allege to be spoofing. In Coscia, the DOJ's allegations of spoofing were based on evidence that Coscia's opposite-side orders were preprogrammed at the time they were placed automatically to cancel themselves within fractions of a second, and to cancel these orders in their entirety if any of them was ever filled.[22] The allegations against Flotron, on the other hand, are based almost exclusively on a description of completely lawful market behavior: maintaining orders on both sides of the market to hedge a trader's overall position and keeping confidential the size of certain positions through the use of iceberg orders. In Flotron's case, this behavior is portrayed as impermissible largely because Flotron eventually canceled these orders and, therefore, must always have intended to cancel them. When viewing Flotron's behavior through this lens, the DOJ explicitly labeled his use of icebergs the "deceptive strategy." [23]

In the absence of preprogrammed indications that reveal the intent of a manual trader (like Flotron), the DOJ appears confident that it can persuade a jury of a trader's alleged preconceived intent to cancel by compiling aggregate trade data. Such data can supposedly show that a trader more frequently executed small trades and tended to cancel larger, opposite-side orders before they were filled. This evidence played a strong corroborating role in the Coscia trial,[24] and the DOJ has stated in the Flotron proceedings that "[t]he evidence in this case is data ... largely it is trading data that's taking place on this trading platform." [25]

With trade data as the centerpiece of a spoofing trial, the defendant's effective counterselection and counterpresentation of that data becomes key. A defendant must be prepared to meet a regulator's proffered data with a counteranalysis of a broader spectrum of trade considerations that presents a full picture of his trading activity. The DOJ has acknowledged that the data it intends to present in the Flotron trial was distilled from as many as 500,000 transactions occurring over a period of several years to select "roughly 1,050 possible spoofing episodes." [26] A true picture of a defendant's trading activity would, however, need to account for the full multiyear 500,000-transaction universe. Such an analysis can demonstrate the legitimacy of a trader's two-sided strategy by showing that not all order placement and trade outcomes fit the regulator's spoofing archetype.

To account for the limitation that after-the-fact market data may, at best, shed ambiguous light about a trader's intent, a spoofing case will inevitably rely on the statements of witnesses who interacted with the defendant. In the absence of the contemporaneous incriminating communications that are the hallmark of many criminal spoofing complaints,[27] this proof is often provided through live witness testimony by co-workers or trade counterparties. The Flotron trial is sure to feature both, including a subordinate trader whom Flotron allegedly trained to spoof. Of particular note is the fact that at least three employees from different counterparty firms who testified against Coscia are slated to testify against Flotron.[28] This anticipated testimony suggests that the DOJ is increasingly comfortable building a spoofing case on the credibility of allegations made by competing traders.

### **Conclusion**

The upcoming Flotron criminal trial and corresponding civil complaint demonstrate that the DOJ and CFTC have the appetite to bring spoofing cases, including criminal charges, against commodity futures traders based largely on patterns observed in trade data. This data may be supplemented by the allegedly incriminating testimony of witnesses, some of whom may be adverse trade counterparties readily willing to attribute their trade losses to a deceptive strategy. This second criminal spoofing trial is sure to impact the coordinated wave of new criminal and civil spoofing cases filed against numerous individuals earlier this year, and it could further inform the Supreme Court's decision whether to accept a petition for certiorari seeking to overturn the first spoofing conviction. Even if the petition is denied, an eventual Second Circuit decision in the Flotron case could present tension between the circuits that could lead the Supreme Court to step in and provide greater guidance in an area of law that financial and legal professionals alike have found difficult to navigate.

---

*Jeffrey A. Brown is a partner at Dechert LLP in New York. He previously worked in the U.S. Attorney's Office for the Southern District of New York, where he was co-chief of the general crimes unit.*

*Conrad A. Johnson IV and Brendan Herrmann are associates in Dechert's New York office.*

*The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.*

[1] Status Conference Transcript, United States v. Flotron, No. 17-cr-220, Dkt. No. 38 at 15:19-20 (D. Conn. Nov. 6, 2017).

[2] United States v. Flotron, No. 17-cr-220, 2018 WL 1401986 (D. Conn. Mar. 20, 2018); Minute Entry, United States v. Flotron, No. 17-cr-220, Dkt. No. 161 (D. Conn. Mar. 24, 2018).

[3] U.S. Department of Justice, Acting Assistant Attorney General John P. Cronan Announces Futures Market Spoofing Takedown (Jan. 29, 2018)

[4] 7 U.S.C. § 6c(a)(5)(C).

[5] 7 U.S.C. § 13(a)(2).

[6] See 18 U.S.C. § 1343; 18 U.S.C. § 1348..

[7] 7 U.S.C. § 6c(a)(5)(C).

[8] See United States v. Coscia, 866 F.3d 782, 790 (7th Cir. 2017); Government's Witness List, United States v. Flotron, No. 17-cr-220, Dkt. No. 94 (D. Conn. Mar. 2, 2018).

[9] Complaint, United States v. Flotron, No. 17-cr-220, Dkt. No. 1 (D. Conn. Sept. 12, 2017); Superseding Indictment, United States v. Flotron, No. 17-cr-220, Dkt. No. 58 (D. Conn. Jan. 30, 2018); Complaint, C.F.T.C. v. Flotron, No. 18-cv-158, Dkt. No. 1 (D. Conn. Jan. 26, 2018).

[10] Superseding Indictment, United States v. Flotron, No. 17-cr-220, Dkt. No. 58 at ¶¶ 14-18 (D. Conn. Jan. 30, 2018).

[11] Complaint, United States v. Flotron, No. 17-cr-220, Dkt. No. 1 at ¶ 26 (D. Conn. Sept. 12, 2017).

[12] Id.

[13] United States v. Flotron, No. 17-cr-220, 2018 WL 940554 (D. Conn. Feb. 19, 2018).

[14] Flotron, 2018 WL 1401986, at \*3.

[15] Compare Complaint, C.F.T.C. v. Flotron, No. 18-cv-158, Dkt. No. 1 at ¶¶ 15, 20, 34, 41, 76, 83 (D. Conn. Jan. 26, 2018), with Superseding Indictment, United States v. Flotron, No. 17-cr-220, Dkt. No. 58 (D. Conn. Jan. 30, 2018).

[16] 866 F.3d 782 (7th Cir. 2017).

[17] Flotron, 2018 WL 1401986, at \*3.

[18] Id.

[19] Id.

[20] Def.'s Memorandum of Law in Support of Motion to Dismiss, United States v. Flotron, No. 17-cr-220, Dkt. No. 67 at 13 n.2 (D. Conn. Feb. 6, 2018).

[21] Id.

[22] Indictment, United States v. Coscia, No. 14-cr-551, Dkt. No. 1 at ¶¶ 10, 11 (N.D. Ill. Oct. 1, 2014).

[23] Complaint, United States v. Flotron, No. 17-cr-220, Dkt. No. 1 at ¶ 26 (D. Conn. Sept. 12, 2017).

[24] See United States v. Coscia, 177 F. Supp. 3d 1087, 1091, 1094-95 (N.D. Ill. 2016).

[25] Status Conference Transcript, United States v. Flotron, No. 17-cr-220, Dkt. No. 30 at 12:7-10 (D. Conn. Oct. 5, 2017).

[26] Status Conference Transcript, United States v. Flotron, No. 17-cr-220, Dkt. No. 47 at 9:20-24 (D. Conn. Dec. 4, 2017).

[27] See Complaint, United States v. Vorley & Chanu, No. 18-cr-35, Dkt. No. 1 at ¶¶ 30-31 (N.D. Ill. Jan. 19, 2018); Complaint, United States v. Bases & Pacilio, No. 18-cr-48, Dkt. No. 1 at ¶¶ 34, 38 (N.D. Ill. Jan. 25, 2018).

[28] Compare Coscia, 866 F.3d at 790, with Government's Witness List, United States v. Flotron, No. 17-cr-220, Dkt. No. 94 (D. Conn. Mar. 2, 2018).