January 07, 2019

Anti-Spoofing Enforcement: 2018 Year in Review

The past year brought a number of significant developments in anti-spoofing enforcement under the Commodity Exchange Act (“CEA”), beginning with the January 29, 2018 coordinated statements of the Commodity Futures Trading Commission (“CFTC” or “Commission”) and the Department of Justice (“DOJ”), signaling an increased commitment to this type of enforcement. That same day, the CFTC announced the creation of a new “Spoofing Task Force,” civil penalties against three banks totaling $46.6 million, and the filing of additional enforcement actions against six individuals.1 The DOJ likewise announced criminal charges for deceptive trading practices against eight individuals, seven of whom were also charged with spoofing.2 This “Spoofing Takedown” was the DOJ’s largest-ever criminal enforcement action in connection with the futures market and the CFTC’s largest parallel action taken with the criminal authorities.3

Since their January 2018 announcements, the DOJ and CFTC have actively pursued a number of criminal and civil anti-spoofing enforcement actions. Several of these actions were resolved with guilty pleas or through consent orders totaling millions of dollars in civil monetary penalties. Yet the only criminal spoofing matter to go to trial in 2018 (the second ever such trial) ended in an acquittal.4 Notwithstanding this setback, the DOJ and CFTC continued to initiate new and novel spoofing-related actions against companies and individuals.

This memorandum provides an overview of anti-spoofing enforcement in 2018 and the trends we expect to continue in 2019.

What is Spoofing?

The 2010 Dodd-Frank Wall Street Reform and Consumer Protection Act (“Dodd-Frank”) amended the CEA to add section 4c(a)(5)(C), which makes it “unlawful for any person to engage in any trading, practice, or conduct on or subject to the rules of a registered entity that . . . is, is of the character of, or is commonly known to the trade as, ‘spoofing’ (bidding or offering with the intent to cancel the bid or offer before execution).”5 Spoofing, therefore, is an intent-based violation that requires a showing that a trader placed a bid or offer with the intent to cancel it prior to execution. The CFTC has alleged the following pattern as indicative of spoofing: (1) a trader placed a small “genuine” or “resting” order at or near the market price; (2) the trader placed a large “spoof” order on the opposite side of the market at a level and/or of a size designed to create a false appearance of market supply or demand to increase the likelihood that the trader’s genuine order would trade; (3) once the genuine order began to trade, the trader then quickly canceled the opposite order before it could be executed by another market participant.6 Several spoofing-related cases
have involved orders that were placed and cancelled through the use of a computer algorithm designed to avoid execution. But neither the CFTC nor the DOJ has required the use of an algorithm: both have claimed spoofing where traders manually placed and cancelled the alleged spoof orders.

The CEA classifies spoofing as a “disruptive practice” that is civilly enforceable by the CFTC. The CEA also makes the “knowing” violation of the anti-spoofing provision a felony.

Criminal Anti-Spoofing Enforcement in 2018

The past year marked the final resolution of the first (and only) two federal criminal spoofing cases to go to trial: United States v. Coscia and United States v. Flotron. Criminal anti-spoofing enforcement was also on the rise in 2018. Prior to the DOJ’s January announcement of charges against seven individuals, the DOJ had only ever publicly charged three individuals with the crime of spoofing.

United States v. Coscia

Although tried and convicted of spoofing and commodities fraud in 2015, Michael Coscia, the principal of high-frequency trading firm Panther Energy Trading LLC, continued to pursue appeals of his conviction until May 14, 2018 when the U.S. Supreme Court denied his petition. The Seventh Circuit opinion upholding Coscia’s conviction is the only federal appellate decision on the CEA’s anti-spoofing provision.

With respect to his spoofing convictions, Coscia had argued on appeal to the Seventh Circuit that the anti-spoofing statute was void for vagueness and, in the alternative, that the evidence presented at trial did not support conviction. The Circuit Court rejected these arguments in a 2017 opinion, finding that the “anti-spoofing provision provides clear notice and does not allow for arbitrary enforcement” and that the spoofing conviction was “supported by sufficient evidence.”

In rebuffing Coscia’s constitutional challenge, the Seventh Circuit pointed to what it described as the CEA’s “clear” parenthetical definition of spoofing. According to the court, the existence of this definition put the trading industry, including Coscia, on notice and rendered Coscia’s arguments regarding the absence of an industry definition, legislative history or regulatory guidance irrelevant. The court further explained that the statute’s intent requirement “imposes clear restrictions on whom a prosecutor can charge with spoofing”: only those “whom [prosecutors] believe a jury will find possessed the requisite specific intent to cancel orders at the time they were placed.”

The Seventh Circuit’s holding that the record evidence supported Coscia’s spoofing conviction laid out something of a template for later enforcement. The court enumerated several pieces of circumstantial evidence presented at trial which, the court reasoned, could have “easily” led a rational trier of fact to find that Coscia placed bids or offers with the intent to cancel them before execution.
United States v. Flotron

Flotron was the second criminal spoofing-related case to go to trial. In a criminal complaint filed in 2017, the government alleged that over the course of five years, Andre Flotron, a Swiss citizen and former UBS precious metals trader, engaged in spoofing and trained a junior trader to spoof. In contrast to Coscia’s conduct, Flotron’s alleged strategy involved manual, as opposed to algorithmic, spoofing. Specifically, Flotron allegedly placed small, “iceberged” genuine orders opposite large, fully-visible spoof orders to exaggerate the visible market imbalance so as to more effectively trick other market participants’ trading algorithms.

On September 26, 2017, a federal grand jury in Connecticut returned a one-count indictment charging Flotron with conspiracy to commit wire fraud, commodities fraud and spoofing. On January 30, 2018, the government secured a superseding indictment that included one count of conspiracy and six substantive counts: three counts of spoofing and three counts of commodities fraud. But only weeks later, Flotron successfully moved to dismiss all of the substantive counts for lack of venue on the ground that the three trading episodes that served as their basis had no connection to Connecticut. The government moved to dismiss the remaining conspiracy count in order to re-file all of the charges in the Northern District of Illinois, where venue was proper, but its motion was denied as contrary to the public interest and in conflict with the government’s prior commitment to proceed speedily to trial in April 2018 in Connecticut.

The case proceeded to trial on the one remaining conspiracy count. Over the course of the trial, the government focused heavily on Flotron’s trading data, which it told the jury was “the best evidence of what he did and what he knew.” The government also presented testimony from two former-traders-turned-cooperators, one of whom testified that he learned to spoof by “watching over [Flotron’s] shoulder, and taking notes.” In contrast, Flotron’s defense emphasized that he was a manual trader in an increasingly algorithmic market, and the difficulty of proving intent through quantitative analysis.

The jury deliberated for only a few hours before returning a verdict of not guilty. Sandra Moser, Acting Chief of the DOJ’s Fraud Section, described the verdict as a “tough loss.”

Other Notable Criminal Actions

The Flotron criminal complaint was one of six complaints announced by the DOJ in January 2018. The five other complaints charged seven individuals with numerous offenses on the basis of their alleged spoofing-related conduct, including spoofing, wire fraud, commodities fraud and conspiracy. Four of the individuals were traders at major financial institutions, two were traders at commodities trading firms and one was the owner of a technology consulting firm.

So far, the DOJ has secured guilty pleas from two of these individuals (from traders Krishna Mohan and Jiongsheng Zhao) and indictments against the remaining five. In October 2018, in connection with
Mohan’s guilty plea, the DOJ announced that it was pursuing charges against two additional individuals who were alleged co-conspirators of Mohan’s in a $60 million commodities fraud and spoofing conspiracy. One of those two individuals also pled guilty.

On November 6, 2018, the DOJ announced that it secured a guilty plea from former precious metals trader John Edmonds, who admitted that he conspired with other traders at JPMorgan Chase & Co. (“JPMC”) to engage in spoofing in the precious metals futures markets. U.S. Attorney John H. Durhan said at the time that the investigation remains ongoing. On November 30, 2018, a court granted the government’s request for a six-month stay in a civil action against JPMC “in order to protect the integrity of its ongoing criminal investigation.” Edmonds is currently scheduled to be sentenced on June 19, 2019.

Civil Anti-Spoofing Enforcement in 2018

The past year also brought unprecedented CFTC anti-spoofing enforcement. In its 2018 fiscal year (October 2017 – September 2018) alone, the CFTC brought twenty-six manipulative conduct and spoofing cases — five times more than the previous annual average.

The January 2018 “Spoofing Task Force” Announcement

The CFTC’s January 2018 announcement identified eight anti-spoofing enforcement actions: the simultaneous initiation and settlement of three actions against financial institutions and the initiation of five additional actions charging six individuals and one company with spoofing in the futures markets.

Together, the three January financial institution resolutions involved over $46 million in civil monetary penalties: $30 million against Deutsche Bank AG and Deutsche Bank Securities Inc., $15 million against UBS AG, and $1.6 million against HSBC Securities (USA) Inc. According to the settlements, the CFTC found that the Deutsche Bank defendants engaged in spoofing, manipulated and attempted to manipulate prices, and failed to supervise; UBS engaged in spoofing and attempted to manipulate prices; and HSBC engaged in spoofing. Notably, in all three settlements, the CFTC lauded the firms’ cooperation and remedial measures, which “substantially reduced” the civil monetary penalties.

The six individuals against whom the CFTC announced civil enforcement actions all faced parallel criminal charges by the DOJ, announced on the same date, including Flotron. With respect to the civil action against Flotron, on December 20, 2018, a proposed consent order executed by the CFTC and Flotron was filed with the court that will resolve the Commission’s claims and impose on Flotron a $100,000 civil monetary penalty and one-year trading ban.

Other Notable Civil Actions

Since January 2018, the CFTC has resolved seven additional anti-spoofing enforcement actions, several of
which provide insight into the CFTC’s anti-spoofing enforcement strategy.  

**Victory Asset and Franko.** On September 19, 2018, the CFTC settled spoofing charges against Victory Asset, Inc. and one of its former traders, Michael D. Franko. According to the CFTC, Franko’s scheme involved both intra-market and cross-market spoofing, or “spoofing in one market to benefit a position in another market, where the price of the two markets is generally correlated.” Specifically, Franko is alleged to have exploited the general correlation between COMEX and London Metals Exchange copper futures contracts. In announcing the settlements, Director McDonald said, “the Commission can and will pursue spoofing and manipulation that stretches across different markets . . . and even international boundaries.” The orders require Victory and Franko to pay civil monetary penalties of $1.8 million and $500,000, respectively.

**Mizuho Bank.** On September 21, 2018, the CFTC settled spoofing charges against Mizuho Bank, Ltd. The CFTC alleged that a trader at Mizuho engaged in spoofing by “flashing” large orders in the market – i.e., quickly placing and canceling large orders to test the market’s reaction to the order. Unlike other CFTC spoofing-related settlements, the CFTC did not allege that Mizuho had entered any opposite genuine orders. Director McDonald said: “Spoofing is an unlawful trade practice that undermines the integrity of the market, because it injects false information into the market — information on which market participants may rely. That’s true whether the bad actor is motivated by a desire to manipulate the market for profit, or, as was the case here, to test the market’s reaction to certain types of orders.” The order requires Mizuho to pay a civil monetary penalty of $250,000.

**Bank of Nova Scotia.** On September 28, 2018, the CFTC settled spoofing charges against The Bank of Nova Scotia (“BNS”) resulting from BNS precious metals traders’ spoofing in the gold and silver futures markets. BNS received a “substantially reduced” $800,000 civil monetary penalty, in part because it self-reported the conduct at issue after being alerted to “certain problematic order activity” by its Futures Commission Merchant, conducted an internal review and terminated the trader. As with the spoofing settlements announced by the CFTC in January 2018, BNS’s “significant” cooperation and remedial measures (such as hiring a full-time surveillance monitor, updating its surveillance systems and enhancing spoofing training) were considered in determining the penalty. These settlements highlight the value the CFTC places on self-reporting and cooperation, particularly following the January 2017 revision to the CFTC’s cooperation credit guidelines for companies, which promised that companies “can expect concrete benefits in return for [] self-reporting, cooperation, and remediation.” This commitment is also reinforced by recent statements by Chairman Giancarlo, as well as Commissioner Behnam, who identified increased self-reporting and cooperation as enforcement tools that may have already led to a decline in the most brazen forms of spoofing.

**Gandhi.** Finally, on October 11, 2018, the CFTC settled spoofing changes against trader Kamaldeep Gandhi. In connection with the settlement, Gandhi admitted that “on thousands of occasions” he, individually and in coordination with others he identified to the CFTC, placed futures contract orders that
he planned to cancel before execution at the time the orders were placed. In addition to “iceberging” his genuine orders, Gandhi admitted that he used order splitters to enter randomly-sized opposite-side orders to further disguise his schemes from the market. This settlement is particularly notable because Gandhi’s penalty has yet to be determined. According to Director McDonald, Gandhi’s liability was bifurcated from his civil monetary penalty due to Gandhi’s continuing cooperation (pursuant to a formal Cooperation Agreement) with a “broader” CFTC investigation. As Director McDonald noted: “Gandhi’s case stands as an example of the sorts of tools we’ll employ to ensure we can use our cooperation program in the most effective way possible. I expect you’ll see more bifurcated orders in these types of cases going forward.”

Flotron, Gandhi, Franko, and other CFTC anti-spoofing enforcement actions in 2018, coupled with recent statements by CFTC Commissioners, highlight the CFTC’s focus on individual accountability. According to Chairman Giancarlo, across all of its enforcement actions, the CFTC has “prioritized individual accountability, with approximately 70% of [the CFTC’s] cases involving charges against individuals.” With respect to spoofing specifically, Director McDonald said: “[W]e will work hard to identify and prosecute the individual traders who engage in spoofing, but we will also seek to find and hold accountable those who teach others how to spoof, who build the tools designed to spoof, or who otherwise aid and abet the wrongdoing.” And, despite the jury’s acquittal of Flotron, the number of spoofing indictments and guilty pleas in 2018 shows that the DOJ also remains committed to bringing criminal charges against individuals.

**Conclusion**

The past year was a period of increased anti-spoofing enforcement by both the CFTC and the DOJ. Their actions, especially given the emphasis on self-reporting, cooperation, and remediation, as well as individual liability, highlight the importance of firms’ internal surveillance systems and controls designed to detect and deter spoofing, including clear policies and procedures, regular trainings, and the prompt, thorough investigation of potential misconduct.

Yet despite the recent increase in anti-spoofing enforcement activity, enforcement of the CEA’s anti-spoofing provision is still relatively new. The outcome of the remaining pending actions announced by the CFTC and DOJ in 2018 will likely further shape the anti-spoofing enforcement landscape going forward. We will continue to monitor and update you on these developments in 2019.

* * *
This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

Susanna M. Buergel  Jessica S. Carey  Roberto Finzi
+1-212-373-3553  +1-212-373-3566  +1-212-373-3311
sbuergel@paulweiss.com  jcarey@paulweiss.com  rfinzi@paulweiss.com

Michael E. Gertzman  Roberto J. Gonzalez  Brad S. Karp
+1-212-373-3281  +1-202-223-7316  +1-212-373-3316
mgertzman@paulweiss.com  rgonzalez@paulweiss.com  bkarp@paulweiss.com

Lorin L. Reisner  Elizabeth M. Sacksteder  Richard C. Tarlowe
+1-212-373-3250  +1-212-373-3505  +1-212-373-3035
lreisner@paulweiss.com  esacksteder@paulweiss.com  rtarlowe@paulweiss.com

Associates Maxwell A. H. Kosman and Phoebe H. King contributed to this Client Memorandum.


See, e.g., In re Arab Glob. Commodities DMCC, CFTC No. 18-01, 2017 WL 4605563 (Oct. 10, 2017) (describing a three-step spoofing pattern in which a trader (1) placed a small genuine order; (2) placed a large order or series of orders on the other side of the market with the intent to cancel them before they could be executed; and (3) cancelled the large orders as soon as some part of the genuine order began to fill); Trial Tr. at 27:7–18, United States v. Flotron, No. 3:17-cr-00220 (D. Conn. Apr. 16, 2018) (Prosecutors described Flotron’s spoofing pattern similarly, but as encompassing four steps, which they simplified to “order, trick, fill, kill”: (1) the placement of a real order, (2) the placement of a “trick” order, (3) fill of the real order, and (4) cancellation of the trick order).

7 U.S.C. § 6c(a)(5)(C). The CFTC has alleged violations of the anti-spoofing provision in tandem with other sections of the CEA and CFTC Regulations, including CEA § 6(c)(1) and Regulation 180.1 (manipulative or deceptive device), CEA § 6(c)(3) and Regulation 180.2 (price manipulation), and Regulation 166.3 (failure to supervise). See, e.g., In re Deutsche Bank AG, CFTC No. 18-06, 2018 WL 684634 (Jan. 29, 2018).


See DOJ January 29, 2018 Press Release (“Other than the individuals identified today, only three other individuals have ever been publicly charged with the crime of spoofing.”).

United States v. Coscia, 866 F.3d 782, 788–89 (7th Cir. 2017), reh’g and suggestion for reh’g en banc denied (Sept. 5, 2017), cert. denied, (U.S. May 14, 2018).

Id. at 785. Coscia also challenged his conviction for commodities fraud, arguing that it was not supported by sufficient evidence and that the trial court did not apply the correct materiality standard. The court rejected these arguments as well. Id.

11 Id. at 785.

12 Id. at 794.

13 Id. at 792–793.

14 Id. at 794 (emphasis added). See id. at 795 (“Importantly, the anti-spoofing statute’s intent requirement renders spoofing meaningfully different from legal trades such as ‘stop-loss orders’ (an order to sell a security once it reaches a certain price’) or ‘fill-or-kill orders’ (an order that must be executed in full immediately, or the entire order is cancelled’) because those orders are designed to be executed upon the arrival of certain subsequent events.”).

15 These included: (1) the fact that Coscia’s cancelled orders constituted an extremely high percentage of all cancelled orders on a relevant futures exchange during the period in question; (2) the disparity between the percentage of Coscia’s small orders that were filled and percentage of large orders that were filled on one of the exchanges; (3) testimony from the software engineer who built it that the algorithm Coscia used was designed to cancel spoof orders if they were ever at risk of being filled; (4) testimony from the software engineer to the effect that the program was designed to artificially inflate prices; (5) a study showing a significant disparity in the amount of time that Coscia left large orders open on the market and the amount of time other traders left large orders open on the market; and (6) a study showing that Coscia’s order-to-trade ratio vastly exceeded that of other market participants. Id. at 795–796.
An “iceberg” order is an order placed in the market such that only a portion of the total order is visible to other market participants at a time. When the first visible pre-set portion is filled, the same quantity automatically becomes visible in the market and the process repeats until the order is either filled in its entirety or cancelled.


Id. Each of the trading episodes that served as the basis for these counts occurred after Flotron had moved from Connecticut to Switzerland and were facilitated through the commodities exchange in Chicago.

The court denied Flotron’s attempt to dismiss the remaining conspiracy count of the superseding indictment. Notably, the court rejected Flotron’s attempt to factually distinguish his case from Coscia as “unconvincing.” Order, United States v. Flotron, No. 3:17-cr-00220 (D. Conn. Mar. 20, 2018). The court similarly rejected the argument that there was nothing false or deceptive about the spoof orders because they were available to be filled. According to the court, “the possibility that any of the alleged ‘trick’ orders might have been accepted or executed upon by someone else in the market does not legitimate the conduct as a matter of law.” Id.


Id.


35 Id.


40 In re Deutsche Bank AG, CFTC No. 18-06, 2018 WL 684634 (Jan. 29, 2018).

41 In re UBS AG, CFTC No. 18-07, 2018 WL 684636 (Jan. 29, 2018).

42 In re HSBC Secs. (USA) Inc., CFTC No. 18-08, 2018 WL 684635 (Jan. 29, 2018).

43 See In re Deutsche Bank AG, CFTC No. 18-06, 2018 WL 684634 (Jan. 29, 2018); In re UBS AG, CFTC No. 18-07, 2018 WL 684636 (Jan. 29, 2018); In re HSBC Securities (USA) Inc., CFTC No. 18-08, 2018 WL 684635 (Jan. 29, 2018). None of the banks admitted or denied the CFTC’s findings or conclusions.

44 See DOJ January 29, 2018 Press Release. The two individuals against whom the CFTC has not yet filed complaints are Edward Bases and John Pacilio.

In re Gandhi, CFTC No. 19-01, 2018 WL 5084650 (Oct. 11, 2018) (determination as to monetary sanctions reserved based on cooperation agreement); In re The Bank of Nova Scotia, CFTC No. 18-50, 2018 WL 4828376 (Sept. 28, 2018) ($800,000 civil monetary penalty); In re Mizuho Bank, LTD., 2018 WL 4628253 CFTC No. 18-38, (Sept. 21, 2018) ($250,000 civil monetary penalty); In re Geneva Trading USA, LLC, CFTC No. 18-37, 2018 WL 4628252 (Sept. 20, 2018) ($1,500,000 civil monetary penalty); In re Victory Asset Inc., CFTC No. 18-36, 2018 WL 4563040 (Sept. 19, 2018) ($1,800,000 civil monetary penalty); In re Franko, CFTC No. 18-35, 2018 WL 4563039 (Sept. 19, 2018) ($500,000 civil monetary penalty); In re Singhal, CFTC No. 18-11, 2018 WL 1782904 (Apr. 9, 2018) ($150,000). In addition, on December 7, 2018, the CFTC informed the District Court for the Southern District of Texas that it had reached an settlement in principal with trader Krishna Mohan. Notice of Settlement, CFTC v. Mohan, 4:18-cv-00260 (S.D. Tex. Dec. 7, 2018).


Rostin Behnam, Commissioner, U.S. Commodity Futures Trading Commission, Remarks of Commissioner Rostin Behnam before Energy Risk USA, Houston, Texas (May 15, 2018), https://www.cftc.gov/PressRoom/SpeechesTestimony/opabehnam6 (“Our own surveillance and use of more sophisticated technologies coupled with increased self-reporting and cooperation and the involvement of our criminal counterparts, have cumulatively contributed to the disappearance of some of the more obvious spoofing patterns.”).

In re Gandhi, CFTC No. 19-01, 2018 WL 5084650 (Oct. 11, 2018).


Id.

Giancarlo October 2, 2018 Speech.

McDonald January 29, 2018 Statement.