

[This article also appears in the Criminal Justice Section Newsletter, Fall 2019 edition.]

Market Manipulation in Milliseconds: Spoofing in Commodity Futures Exchanges

*Luke Cass*¹

Enforcement of the "Anti-Spoofing" provision of the Commodity Exchange Act, 7 U.S.C. § 1 *et seq.*, on the commodity futures exchanges is at a unique juncture where law and technology have seemingly intersected at the right place and at the right time. This article examines this seldom known, but increasingly used, criminal statute in its first prosecution and spoofing's potential to wreak havoc in commodity futures markets in a matter of seconds.

Background

The CME Group based in Chicago is the largest futures exchange in the world and operates the Chicago Mercantile Exchange (CME), the Chicago Board of Trade (CBOT), the New York Mercantile Exchange (NYMEX), and the Commodity Exchange, Inc. (COMEX). CME Group's trading is diverse and occurs on everything from lean hogs to Bitcoin futures, from copper to corn.

Despite the diversity of these goods, all futures contracts operate the same way.¹ The futures contract seller agrees to deliver the commodity in the future and is said to be in a "short" position.² The buyer agrees to accept delivery and is said to be in a "long" position.³ Most futures contracts are not "traded" in the normal sense of that word, rather, profits are collected off the difference in price between the original contract and the offsetting transaction. If the price of the future has declined, – usually because of market information indicating a drop in the price of the commodity, – the short profits. However, if the futures price has risen, the long profits.⁴ "Futures trading is a zero-sum game. Since money is made from the change in futures contract prices, and every contract has a long and a short, every gain can be matched with a corresponding loss."⁵

Trading on commodity futures exchanges presents significant risk. The U.S. Commodity Futures Trading Commission cautions that "[t]rading commodity futures and options is a volatile, complex and risky venture that is rarely suitable for individual investors or 'retail customers'" and "[m]any individuals lose all of their money, and can be required to pay more than they invested initially."⁶ The trading volume on these exchanges is colossal. This past May, CME Group reached its second-highest monthly trading volume ever, averaging nearly 24 million contracts *daily*.⁷ Greater still is the number of cancelled contracts or placed orders, which the former chief of the Securities and Exchange Commission estimated as being as high as 90 percent.⁸

¹ Luke Cass, a former federal prosecutor for over ten years, is a partner at Quarles & Brady, LLP and teaches White Collar Crime and Securities Fraud at the Georgetown University Law Center.

The days of floor brokers conducting the majority of trading on these exchanges from the inside of a “pit” or “ring,” shouting or gesticulating trades with hand signals – as made famous by Eddie Murphy and Dan Aykroyd in *Trading Places* – are largely long gone. Most trading now is done electronically, but trading volatility nonetheless persists with price fluctuations occurring in milliseconds. One former U.S. Senator described it as being a “wild west” trading environment.⁹ This perfect storm of factors including high-frequency and algorithmic trading has provided fertile ground for abuse in the form of spoofing.

The Anti-Spoofing Statute

Spoofing, which Congress criminalized in 2010 as part of the Dodd-Frank Wall Street Reform and Consumer Protection Act,¹⁰ is an illegal shortcut through the risky volatility of these markets. Title 7 of the United States Code, § 6c(a)(5)(C) makes it unlawful for “any person to engage in 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).”

Spoofing is illegal because it “can be employed to artificially move the market price of a stock or commodity up and down, instead of taking advantage of natural market events.”¹¹ A spoofing trader can create artificial supply and demand by “placing large and small orders on opposite sides of the market. The small order is placed at a desired price, which is either above or below the current market price, depending on whether the trader wants to buy or sell. If the trader wants to buy, the price on the small batch will be lower than the market price; if the trader wants to sell, the price on the small batch will be higher. Large orders are then placed on the opposite side of the market at prices designed to shift the market toward the price at which the small order was listed.”¹² “In short, the trader shifts the market downward through the illusion of downward market movement resulting from a surplus of supply. Importantly, the large, market-shifting orders that he places to create this illusion are ones that he never intends to execute; if they were executed, our unscrupulous trader would risk extremely large amounts of money by selling at suboptimal prices.”¹³

United States v. Coscia

United States v. Coscia, the first spoofing case ever brought, is instructive. Michael Coscia was a longtime commodities futures trader at a high-frequency trading firm.¹⁴ Coscia enlisted the help of a computer programmer to design two computer programs that would work in 17 different CME Group markets and three different European futures markets.¹⁵ Coscia’s high-frequency trading strategy allowed him to enter and cancel large-volume orders in a matter of milliseconds, which created an artificial supply and demand.¹⁶ Accordingly, Coscia was able to purchase contracts at lower prices or sell contracts at higher prices by artificially pumping and then deflating the market by placing and cancelling orders. “[W]ithin milliseconds of achieving the desired downward market effect,” Coscia cancelled the large orders.¹⁷ The computer programs detected

when conditions were ripest and operated through a system of trade orders and quote orders and the "entire series of transactions would take place in a matter of milliseconds."¹⁸

In August of 2011, Coscia employed this strategy with various futures commodities, including gold, soybean meal, soybean oil, high-grade copper, Euro FX and Pounds FX currency futures. In one instance involving copper futures, Coscia risked up to \$50 million by placing large orders, which drove the price up.¹⁹ The buy orders created the illusion of market movement in copper futures and Coscia sold the contracts at his desired price point.²⁰ Coscia then placed large volume orders to sell the contracts, which created downward momentum on copper future prices by fostering the appearance of abundant supply.²¹ This allowed Coscia to buy his small orders at the artificially deflated price.²² Coscia then immediately cancelled the large orders.²³ Coscia's whole process was repeated tens of thousands of times resulting in over 450,000 large contract orders.²⁴ This all took place in two-thirds of one second, earning Coscia profits of over \$1.4 million.²⁵

What makes spoofing criminal is the trader's intent when placing the order. "Prosecutors can charge only a person whom they believe a jury will find possessed the requisite specific intent to cancel orders at the time they were placed."²⁶ "Legitimate good-faith cancellation of partially filled orders" does not violate the anti-spoofing statute.²⁷ In Coscia's case, he would be guilty of spoofing if he knowingly entered trades with the present intent to cancel them prior to execution.²⁸ This is harder to prove than one might think and can lead to competing inferences. Coscia argued that his trades were "concededly conditional" and that his trading strategy was "virtually identical to other durational or contingent orders routinely permitted by exchange trading interfaces."²⁹ As Coscia pointed out, cancelled trades are common in the high-frequency trading world where 98% of orders are cancelled before execution.³⁰

A Chicago jury disagreed and convicted Coscia. The U.S. Court of Appeals for the Seventh Circuit affirmed the conviction and found that Coscia had the requisite criminal intent. The Court found that Coscia's conduct was spoofing based on several key pieces of evidence introduced at trial: (1) Coscia was responsible for 96 percent of all cancellations on the European exchange during the two months when he used the computer program; (2) on the Chicago Mercantile Exchange 35.61% of Coscia's small orders were filled, but only 0.08% of his large orders were filled; (3) the designer of the computer program offered devastating testimony that the computer programs were made to avoid large orders being filled and that "quote orders" were used to "pump" the market; (4) only 0.57% of Coscia's large orders were on the market for more than a single second, but 65% of Coscia's large orders were open on the market for more than a second; and (5) Coscia's order-to-trade ratio was 1,592% and that ratio for other market participants was between only 91% and 264%, which meant that Coscia's average order was far greater than his average trade.³¹ The Seventh Circuit found that while "no single piece of evidence necessarily establishe[d] spoofing" the proof taken together allowed jurors to determine that Coscia entered his orders with the intent to cancel them before execution.³²

Coscia argued that the anti-spoofing statute was impermissibly vague and attempted to equate his conduct with various legal trading strategies such as "stop-loss orders" (an order to sell when a certain price is reached), "fill-or-kill orders" (an order that must be filled immediately or it's fully cancelled), "partial-fill" orders (a pre-programmed order that cancels the balance of an

order once a portion is filled), "Good-til-date orders" (orders that cancel with a defined period of time), "ping orders" (small orders used to detect trading activity), or "iceberg" or hidden quantity orders" (orders designed to obscure the underlying supply or demand).³³ The Court, unpersuaded by these arguments, found that those trading strategies were markedly different from what Coscia did because they are designed to be executed under certain conditions whereas Coscia's large orders "were designed to *evade* execution" altogether.³⁴

Outlook

The U.S. Department of Justice's Fraud Section has made spoofing prosecutions a priority. In January of last year, the Department announced a spoofing takedown that charged eight individuals in six cases across three federal districts³⁵ and several spoofing trials are set for 2019.³⁶ As the then-Acting Assistant Attorney General of the Criminal Division stated, "The Criminal Division's message is clear. We are watching. We are closely monitoring the markets. And we will leave no stone unturned in our efforts to combat and eradicate illegal, fraudulent, and manipulative market conduct."³⁷ The record supports the rhetoric – in the past five years, the Department of Justice has brought a total of 12 spoofing cases against sixteen defendants.³⁸ In an August 20, 2019 press release for a trader's guilty plea in the Eastern District of New York, the trader admitted as part of his plea allocution that he "learned to spoof from more senior traders, and spoofed with the knowledge and consent of his supervisors."³⁹ The release noted that the trader was "cooperating" and twice described the investigation as "ongoing," suggesting that additional charges may be imminent.

In addition to the anti-spoofing statute and depending on the facts of the case, other statutes may come into play for similar market manipulation conduct such as 18 U.S.C. § 1348 (securities and commodities fraud), 18 U.S.C. § 1343 (wire fraud), and 7 U.S.C. § 13(a)(2) (commodity price manipulation). Coscia was also convicted of a § 1348 violation, which was affirmed despite Coscia having made no specific false statements or representations, which, while not required, is often compelling proof.⁴⁰

Despite mounting a vigorous defense, Coscia was found to have "*designed* a system that used large orders to inflate or deflate prices, *while also structuring that system to avoid the filling of large orders*."⁴¹ Coscia essentially made, pumped, and then dumped the market in milliseconds, profiting enormously in a matter of seconds. While Coscia's evidence of spoofing was circumstantial it was also clear and the U.S. Supreme Court denied his petition for certiorari.⁴² However, there may be closer calls in the near future. The second spoofing trial involving a Swiss trader in the District of Connecticut resulted in six of the seven counts being dismissed for lack of venue and an acquittal on the remaining charge.⁴³ This past spring federal prosecutors in Chicago dismissed spoofing charges against a software developer after his trial ended in a hung jury.⁴⁴ The software developer's \$24,200 program was alleged to have aided a trader with a \$40 million spoofing scheme of S&P 500 futures that caused a "flash crash" on the equity markets in May of 2010.⁴⁵

There may be more challenges in the future as high-frequency trading and technology continue to evolve. The introduction and use of artificial intelligence to effectuate high-frequency

trading could obfuscate spoofing's intent element and allow for a more persuasive defense about an individual's intent to cancel trades before execution.

Luke Cass, a former federal prosecutor for over ten years, is a partner at Quarles & Brady, LLP and teaches White Collar Crime and Securities Fraud at the Georgetown University Law Center.

¹ *Leist v. Simplot*, 638 F.2d 283, 286 (2d Cir. 1980), *aff'd sub nom.* *Merrill Lynch, Pierce, Fenner & Smith, Inc. v. Curran*, 456 U.S. 353, 102 S. Ct. 1825, 72 L. Ed. 2d 182 (1982).

² *Id.*

³ *Id.*

⁴ *See Cargill, Inc. v. Hardin*, 452 F.2d 1154, 1157 (8 Cir. 1971), *cert. denied*, 406 U.S. 932, 92 S.Ct. 1770, 32 L.Ed.2d 135 (1972).

⁵ *Leist*, 638 F.2d at 286.

⁶ <https://www.cftc.gov/ConsumerProtection/EducationCenter/FuturesMarketBasics/index.htm>

⁷ <https://www.prnewswire.com/news-releases/cme-group-reaches-second-highest-monthly-volume-ever-averaging-23-9-million-contracts-per-day-in-may-2019--300861265.html>

⁸ <http://fortune.com/2010/09/13/fast-trading-firm-hit-with-big-fine/>

⁹ *Id.*

¹⁰ Pub. L. No. 111-203, 124 Stat. 1376 (2010).

¹¹ *United States v. Coscia*, 866 F.3d 782, 787 (7th Cir. 2017), *reh'g and suggestion for reh'g en banc denied* (Sept. 5, 2017), *cert. denied*, 138 S. Ct. 1989, 201 L. Ed. 2d 249 (2018)

¹² *Id.*

¹³ *Id.*

¹⁴ *United States v. Coscia*, 100 F. Supp. 3d 653, 655 (N.D. Ill. 2015).

¹⁵ *Id.*

¹⁶ *Id.*

¹⁷ *Coscia*, 866 F.3d at 787.

¹⁸ *Coscia*, 100 F. Supp. 3d at 655.

¹⁹ *Coscia*, 866 F.3d at 788.

²⁰ *Id.*

²¹ *Id.*

²² *Id.*

²³ *Id.*

²⁴ *Id.*

²⁵ *Id.*

²⁶ *Id.* at 794.

²⁷ *Coscia*, 100 F. Supp. 3d at 658 (quoting 76 Fed. Reg. at 14,947).

²⁸ *Coscia*, 866 F.3d at 795.

²⁹ *Coscia*, 100 F. Supp. 3d at 658.

³⁰ *Id.* at 793.

³¹ *Id.* at 795-96.

³² *Id.* at 796.

³³ *Coscia*, 866 F.3d at 794,-95, 800.

³⁴ *Id.* at 800 (emphasis original); 2018 WL 741613, at *8.

³⁵ <https://www.justice.gov/opa/speech/acting-assistant-attorney-general-john-p-cronan-announces-futures-markets-spoofing>

³⁶ <https://www.justice.gov/criminal-fraud/file/1123566/download>

³⁷ *Id.*

³⁸ <https://www.cnbc.com/2019/08/20/another-ex-jp-morgan-precious-metals-trader-pleads-guilty-to-spoofing.html>

³⁹ <https://www.justice.gov/opa/pr/precious-metals-trader-pleads-guilty-conspiracy-and-spoofing-charges>

⁴⁰ *Coscia*, 866 F.3d at 796-97.

⁴¹ *Id.* at 797 (emphasis original).

⁴² *Coscia v. United States*, 138 S.Ct. 1989 (2018).

⁴³ <https://www.nytimes.com/2018/05/03/business/dealbook/spoofing-prosecuting-andre-flotron.html?searchResultPosition=9>

⁴⁴ <https://www.chicagotribune.com/business/ct-biz-spoofing-software-developer-charges-dropped-20190423-story.html>

⁴⁵ *Id.*