farmdoc DAILY

Department of Agricultural and Consumer Economics, University of Illinois Urbana-Champaign

Who's Spoofing Whom?

Paul Peterson

Department of Agricultural and Consumer Economics
University of Illinois

December 23, 2015

***farmdoc daily* (5):236**

Recommended citation format: Peterson, P. "Who's Spoofing Whom?" *farmdoc daily* (5):236, Department of Agricultural and Consumer Economics, University of Illinois at Urbana-Champaign, December 23, 2015.

Permalink: http://farmdocdaily.illinois.edu/2015/12/whos-spoofing-whom.html

Many opinions have been expressed by market participants in the weeks since a Chicago jury found Michael Coscia guilty of "spoofing" on November 3. This was the first criminal case on spoofing, and the first to be tried under the expanded definition of disruptive futures market trading practices in the Dodd-Frank Wall Street Reform and Customer Protection Act. Dodd-Frank defines spoofing as "bidding or offering with the intent to cancel the bid or offer before execution." Also see in the *farmdoc daily* article on May 6, 2015 for a detailed illustration of how spoofing works.

Securities Markets vs. Futures Markets

The Securities and Exchange Commission (SEC) has prohibited spoofing in the securities markets since 2001 under the general anti-fraud provisions of Section 17(a) of the Securities Act of 1933

> "It shall be unlawful… to employ any device, scheme, or artifice to defraud, or to obtain money or property by means of any untrue statement of a material fact.. or to engage in any transaction, practice, or course of business which operates or would operate as a fraud or deceit upon the purchaser."

and Section 10(b) of the Securities Exchange Act of 1934

> "It shall be unlawful for any person, directly or indirectly… [t]o use or employ, in connection with the purchase or sale of any security… any manipulative or deceptive device or contrivance…"

However, futures markets are not securities markets. They serve entirely different economic purposes, so just because something is used in one market doesn't necessarily mean it should be adopted by the other. In addition, from a purely practical standpoint it can be difficult to distinguish spoofing from legitimate futures trading activity. For instance, a futures trader may enter an order larger than necessary – say, an order to buy 200 contacts at a particular price when only 100 contracts are needed – and then cancel any unfilled portion as a way to guarantee that at least 100 contracts get filled. Similarly, a futures trader may enter an order to buy or sell at a particular price, and then adjust that price up or down as new information becomes

available. At what point does canceling or adjusting an unfilled order cross the line between legitimate trading and spoofing?

To make this determination, the Commodity Futures Trading Commission (CFTC) relies on guidelines including market context, patterns of trading activity, and indications of the trader's intended purpose. If the intended purpose is to overload the price quotation system, to delay the execution of another person's trades, to create the appearance of false market depth, or to create artificial price movements, then spoofing likely occurred.

Coscia's Computer Programs

Coscia's computer programs would place a small order on one side of the market followed by a large order on the opposite side of the market – for example, a buy order for a few contracts just below the market price, followed by a sell order for many more contracts just above the market price. The programs then would cancel the large order within a fraction of a second. However, the sudden appearance of the large sell order would create the impression of potentially heavy selling and cause other sellers to accept Coscia's buy order before prices moved even lower.

Coscia's programs would then reverse the process, placing a small sell order just above the market, followed by a large buy order just below the market that would be cancelled within a fraction of a second. This see-saw strategy would pick up small profits of only a tick or two on each trade, but could be repeated over and over to produce sizeable profits. In the government's complaint against Coscia, the six spoofing examples generated profits per trade of $175, $560, $100, $60, $112.50, and $62.50. However, during the 3-month period covered by this case, Coscia's total profits were estimated at nearly $1.6 million.

Civil and Criminal Charges

In 2013, Coscia settled civil charges involving these same trades, paying the CFTC a $2.8 million fine and waiving his rights against double jeopardy on any related criminal proceedings that might be brought against him. He also entered into separate settlements with CME and with the UK's Financial Conduct Authority. In October 2014, the federal government filed criminal charges against Coscia, consisting of six counts of spoofing and six counts of commodities fraud.

Proving Intent

A conviction for fraud (commodity or otherwise) requires proof of intent – in other words, prosecutors must show that the person actually meant to do it. Proving intent can be very difficult because it is impossible to know what a person is thinking, so the proof often involves documents or recorded conversations that reveal the person's thoughts. Recall that the Dodd-Frank definition of spoofing also involves intent – "bidding or offering with the *intent* to cancel the bid or offer before execution" – so prosecutors were required to show intent for all 12 counts.

Coscia's computer programs placed thousands of orders during this 3-month period. Fewer than 10% of the large orders were ever filled, compared to 40% of the small orders. Coscia testified at the trial that he "absolutely wanted to fill every order" but the evidence showed that the computer programs were designed to automatically cancel the large orders within 400 milliseconds, even when the market was moving in his favor and would have made those large orders profitable.

Therefore, the proof of intent came from the design of the computer programs. The jury reached a verdict after just an hour of deliberations: guilty on all six counts of spoofing, and guilty on all six counts of commodity fraud. Each spoofing count carries a maximum sentence of 10 years in prison plus substantial fines, and each fraud case carries a maximum sentence of 25 years in prison plus substantial fines. Sentencing is scheduled for March 17, 2016.

More on Spoofing

In our next installment we will look at two other spoofing cases waiting to go to trial, and examine some of the economic vs. legal issues surrounding spoofing.

References

Peterson, Paul. "Flash Crash, or Flash in the Pan?" *farmdoc daily* (5):83, Department of Agricultural and Consumer Economics, University of Illinois at Urbana-Champaign, May 6, 2015.

U.S. Commodity Futures Trading Commission. *In the Matter of Panther Energy Trading LLC and Michael J. Coscia, Respondents.* CFTC Docket No. 13-26. Accessed December 22, 2015. http://www.cftc.gov/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfpantherorder072213.pdf

U.S. District Court, Northern District of Illinois, Eastern Division. *United States of America v. Michael Coscia.* Accessed December 22, 2015. http://www.justice.gov/sites/default/files/usao-ndil/legacy/2015/06/11/pr1002_01a.pdf

U.S. Government Printing Office. *Federal Register* (78):102, May 28, 2013, pp. 31890-31897. Accessed December 22, 2015. https://www.gpo.gov/fdsys/pkg/FR-2013-05-28/pdf/2013-12365.pdf

U.S. Securities and Exchange Commission. *Securities Act of 1933.* Accessed December 22, 2015. https://www.sec.gov/about/laws/sa33.pdf

U.S. Securities and Exchange Commission. *Securities Exchange Act of 1934.* Accessed December 22, 2015. https://www.sec.gov/about/laws/sea34.pdf