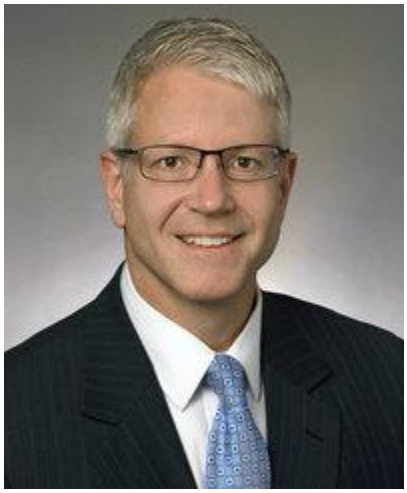
Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

A Look At The 1st Criminal 'Spoofing' Prosecution: Part 2

Law360, New York (April 21, 2015, 10:05 AM ET) --



Clifford C. Histed

On April 16, 2015, U.S. District Judge Harry D. Leinenweber in Chicago ruled, in the first criminal case of its kind, that the "spoofing" statute was not unconstitutionally vague, and that the spoofing and fraud indictment against futures trader Michael Coscia would not be dismissed.[1] In Part 1 of this article, we examined what guidance could be gleaned from what futures regulators have said about spoofing and what they have charged as spoofing, and discussed the Coscia criminal case.

In Part 2 of the article, we will examine the court's ruling, and discuss spoofing-type conduct in the context of practical guidance to traders about trade cancellation, and about avoiding and defending against exchange and government investigations. Under what circumstances will canceling a trade be considered a regulatory violation or, worse yet, a crime?

The Court's Decision

In denying Coscia's motion to dismiss the indictment, Judge Leinenweber explained that, when ruling on a motion to dismiss, a court reviews an indictment on its face, accepting all of its allegations at true, and that indictments are reviewed on a practical basis and in their entirety, rather than in a hypertechnical manner.[2] The court said, "In general, an indictment that tracks the words of a statute to state the elements [of the] crime is acceptable, provided that it states sufficient facts to place a defendant on notice of the specific conduct at issue,"[3] and that "[w]ithout question, this conduct [described in the indictment] tracks the language of the statute, and constitutes 'spoofing' as the statute defines that term: 'bidding or offering with the intent to cancel the bid or offer before execution.'"[4]

The court stated, "If a reasonable person would have been on notice that his or her conduct was at risk, and reasonable guidelines exist, the due process concerns are overcome," and that "Courts must strive to 'construe, not condemn, Congress' enactments' because of their strong presumptive validity."[5] The court referred to the CFTC's March 2011 proposed interpretive guidance, noted that it was issued five months before the offense conduct, and stated that the guidance suggests that there was some degree of consensus as to what conduct was included and excluded at that time.[6]

The court ruled that in a case where First Amendment rights are not at stake, which was the case here,

"the Court must assess whether the statute is unconstitutional as applied to Coscia's conduct, not to the conduct of 'hypothetical legitimate traders' who voiced concerns about the statute's applicability to practices such as partial-fill and stop-loss orders."[7] "A plaintiff who engages in some conduct that is clearly proscribed cannot complain of the vagueness of the law as applied to the conduct of others."[8]

The court stated that the spoofing provision's "intent to cancel" requirement was significant because, "When the government must prove intent and knowledge, these requirements do much to destroy any force in the argument that application of the statute would be so unfair that it must be held invalid."[9] The court ruled that the spoofing provision was not impermissibly vague as applied to Coscia because his alleged "intent to cancel" set his conduct apart from the legitimate trading practices Coscia described in his memorandum as also susceptible to being swept with the reach of the statute.[10]

Finally, the court rejected Coscia's argument that the six commodity fraud counts should be dismissed on the grounds that the indictment failed to allege that Coscia made any affirmative or implied misrepresentations to other market participants.[11] Even though the word "misrepresentation" is absent from indictment, the court observed that the indictment alleged that Coscia's trading conduct "created a false impression regarding the number of contracts available in the market," and "fraudulently induced other market participants to react to the deceptive market information," and was intended to "trick" and "mislead" them.[12]

The court ruled that it would not review the indictment in a "hypertechnical manner" because, "Statutory prohibitions against schemes to defraud are often worded broadly because Congress cannot anticipate each and every new context in which they might be carried out."[13]

Coscia now is faced with the choice of either pleading guilty or proceeding to trial and holding the government to its burden of proof. Coscia has the option, if the court and government agree, to enter a plea of guilty that is conditioned upon his right to appeal Judge Leinenweber's ruling to the Seventh Circuit Court of Appeals.[14] Of course, Coscia also would be entitled to appellate review if he is convicted at trial.

Current State of Futures Exchange Investigation and Enforcement

On August 29, 2014, CME issued Rule 575, a new rule prohibiting spoofing and other disruptive practices, which became effective Sept. 15, 2014. The market regulation advisory notice announcing the rule stated that spoofing always had been a violation of preexisting exchange rules, and referenced both the new Dodd-Frank provisions, and the Commodity Futures Trading Commission's May 28, 2013, interpretive guidance.[15] The 11-page advisory contained both FAQs and examples of prohibited activity.

Rule 575 states, "All orders must be entered for the purpose of executing bona fide transactions," and "No person shall enter or cause to be entered an order with the intent, at the time of order entry, to cancel the order before execution or to modify the order to avoid execution."[16] In contrast to the CFTC's May 28, 2013, policy statement that reckless trading would not constitute a spoofing violation, the CME guidance identifies recklessness as a sufficient level of intent to find a violation.[17] Moreover, the CME seemed to adopt a very expansive concept of recklessness:

Proof of intent is not limited to instances in which a market participant admits its state of mind. Where the conduct was such that it more likely than not was intended to produce a prohibited disruptive consequence without justification, intent may be found. Claims of ignorance, or lack of knowledge, are

not acceptable defenses to intentional or reckless conduct. Recklessness has been commonly defined as conduct that "departs so far from the standards of ordinary care that it is very difficult to believe the actor was not aware of what he or she was doing."[18]

Not only does CME have a new and specific spoofing rule, but it has a market surveillance, investigative and disciplinary infrastructure to detect and sanction violations of the rule. CME is carefully watching electronic futures trading in real time. It conducts its own in-house investigations and disciplinary hearings, refers matters to the CFTC and shares information with federal law enforcement agencies upon request.

CME's Market Regulation Department performs compliance functions for all four CME Group exchanges.[19] Market Regulation houses several units, including Market Surveillance, Investigations, Enforcement, and the Strategic and Technology Initiatives Group.[20] Market Surveillance's primary tools for monitoring trading are: (1) the Large Trader Reporting System; (2) the Sophisticated Market Analysis Research Technology (SMART) tool; and (3) the Regulatory Application for Processing In-Memory Data (RAPID) tool, which captures in real-time all order, trade and market data messaging information.[21] Further, as the CME Group's then-CEO told the CFTC in 2010:

CME Group's Market Regulation Department maintains an exceptionally detailed electronic audit trail that records and allows immediate, as well as historical, access to every order, modification, and cancellation, and every market data message and book state change, including all time stamps at the millisecond level. The audit trail also includes, among other data elements, the order instructions, account number, a unique identifier of the user who entered the order and whether the order was entered by a user employing an automated trading system.[22]

On Dec. 29, 2014, the ICE Futures U.S. exchange issued a disruptive trading practice rule and guidance that is very similar to those of the CME.[23] The CME and ICE guidance are "must reads" for traders and their supervisors, and risk management and compliance personnel.

Regulatory Guidance Applied in the Real World

How does the regulatory guidance play out in the real world of trading? The following examples of trading scenarios suggest how difficult it might be to determine the boundaries of what is violative spoofing, and what is not, and how a trader will be able to establish the legitimacy of trade cancellations. Each could appear to be defensible depending on the circumstances:

- ***Canceling orders in self defense***. If a trader comes to believe that another market participant has superior information or a better trading algorithm, and that her own market position is now at risk, is it spoofing for her to cancel her trades to avoid damage in the technology "arms race" that some traders feel the market has become? Historically, changing a trading position in reaction to external risks is expected and entirely permissible.

- ***Canceling orders in one market due to events in a different but related market***. A trader may use two trading systems that are linked and that trade in two related markets, such as E-mini S&P 500 futures, and SPY exchange-traded funds. If events in the securities market cause the futures trading system to cancel the futures orders, could that be considered spoofing or a rationale response to changing market conditions?

- ***Canceling orders no longer needed after requirements have been fulfilled***. Order execution is not guaranteed, so what if a trader bids for 500 futures contracts, while only needing to be filled on 100 contracts but also expecting in a tight market to get filled only on 100 of the 500 contracts she bids? If she succeeds in buying 100 contracts and cancels the remaining 400 bids, would that be spoofing? According to the CME, this would not be a spoofing violation, but it would be a violation of other exchange rules if the trader could not meet the financial obligations that would result from getting filled on all 500 contracts if that occurred.[24]

- ***Canceling orders after using them to gather market intelligence***. If a trader places bids or offers at various price levels, some of which are away from the current market price, only to gather information about other traders' willingness or desire to transact at those levels, is the trader spoofing if she cancels her orders after five minutes of observing the market's reaction? What if the orders are exposed to the market for only one minute? Ten seconds? One second? Though the trader may not have had any desire or intent to create an appearance of false market depth, or create artificial price movement, must she be able to show that she had a legitimate, good-faith intention to consummate trades in order to avoid allegations of spoofing?

- ***Canceling orders to test system parameters***. What if a trader has her computer trading system set to trade 100 contracts at a time, but wants to change it to 200 contracts? Is it spoofing to enter a 200-lot trade, just to see if the new settings are in effect, intending all the while to cancel the 200-lot trade? It does not appear that the trader attempted to create an appearance of false market depth, or create artificial price movements, but the trader also does not appear to have intended to consummate a trade. Yet, it would be difficult to see this conduct as a spoofing violation.

In each of these examples, the trader, her supervisors and colleagues, and the appropriate risk management, compliance and legal personnel would be well-served by contemporaneously conceiving, articulating and documenting the legitimate justification for the trade cancellations in the event they are later asked to explain them to regulators.

Considerations for Trading Firms Going Forward

Electronic trading is serious business, and most successful traders by now have implemented certain risk controls.[25] It is not only required by everyday business sense, but is expected by the regulators.[26] Issues to consider include: does the firm's operational and compliance strategy include an understanding and articulation of its reason for canceling trades? Is the firm's cancelation rate higher than market norms? Are the firm's trades exposed to the market long enough to allow for a real chance of execution? How long is "long enough" in the products and markets the firm trades?

One of the best ways to persuade investigators that a trader or firm lacks the intent required to find a spoofing violation is by showing that the trading strategy was carefully conceived, properly vetted, well-documented and faithfully monitored. If a trader canceled trades only after she reassessed her

strategies and their effect on the market, or so that she would be able to do so, the trader should be prepared to articulate that. Traders should think carefully ahead of time about how they would explain their trade cancellation if they were compelled by the exchange or CFTC to give a recorded statement, or if they were interviewed by an FBI agent or assistant U.S. attorney.

The futures exchanges have the burden of proving liability for spoofing by a preponderance of the evidence (more likely than not), and the rules of evidence do not apply in exchange hearings.[27] The exchanges have taken the position that they must prove only that a trader acted recklessly, but a lower level of intent (such as negligence) will not suffice to establish a violation. The CFTC also must prove liability by a preponderance of the evidence, and typically the rules of evidence will apply if they bring their action in federal court, and the CFTC has made clear that the statute requires proof of a level of intent that is higher than recklessness.

Finally, criminal prosecutors have the burden of proving guilt beyond a reasonable doubt, and the rules of evidence apply in federal trials, and they, like the CFTC, must prove that a defendant acted with an intent level higher than recklessness (i.e, knowingly).

In all of these settings, the prosecution must prove that a trader accused of spoofing intended to cancel trade orders at the time she entered the orders. They will have to prove that that the trader had a specific intent to cancel the order before another market participant could hit the order. Because the trading data ultimately will be available from the exchange and the trading firm, the prosecutor's challenge in all spoofing cases typically will be to prove intent.

How do the regulators and prosecutors prove intent? Often they will obtain and review electronic communications of the trader and her supervisors, colleagues or counterparties. Trading firm compliance programs should train and focus on the importance of careful business communication. It has been said that "emails are God's gift to the prosecutor." Traders, just like all business professionals, should be careful about what they say, and how they say it. Thoughtlessly phrased emails or text messages that take a few seconds or minutes to write, and firm-recorded telephone calls where people often speak too casually, may end up in a regulator's press release[28] or, even worse, as exhibits at trial.[29] Of course, prosecutors also sometimes use electronic surveillance such as wiretaps.

Rule enforcers also prove intent through the testimony of cooperating witnesses such as whistleblowers, disgruntled business partners or estranged loved ones, and even other traders who are cooperating with authorities in order to reduce their own legal exposure. Yes, that happens.

One of the most effective ways rule enforcers prove intent is through the use of a trader's own admissions given during exchange investigations, investigative or deposition testimony taken by regulators, or interviews with prosecutors and law enforcement agents. One of the most difficult decisions a person makes when facing the prospect of both regulatory and criminal actions is whether to explain their conduct to the regulators, or whether to assert their Fifth Amendment right to silence.

On one hand, if the person has a plausible and credible explanation for their conduct, and chooses to tell it to the regulator, the explanation may be credited with the result that the regulatory action is closed. But there also is a very good chance that the statement will be shared with criminal authorities if they request the statement. On the other hand, if the person chooses to assert their Fifth Amendment right to remain silent, they deprive criminal authorities of a potentially incriminating statement, but the regulator may be able to use that silence against the person in the regulatory case.

Before speaking with investigators — whether from the exchange, a regulatory agency or a criminal law enforcement agency — a trader should consult with legal counsel and carefully consider whether they have an explanation that is likely to withstand harsh scrutiny. It is important for traders to be able to articulate the purpose of a trading strategy, and to explain how the strategy was not intended to disrupt the market.

Conclusion

Traders watch markets, but markets also watch traders. Counterparties are watching, and are ready to become government informers or whistleblowers, or file private lawsuits, against traders whose conduct harms them. The exchanges are watching, and they see traders in real time. Their surveillance software is vigilant. It does not sleep. The exchanges share information with regulators both in the U.S. and in other trading centers around the world.

Traders would be wise to seek guidance from advisers who understand how regulators and law enforcement agencies investigate, make decisions and conduct litigation; advisers who listen carefully, look for solutions and who are well-prepared to litigate if that truly is the best course of action.

We now have Judge Leinenweber's ruling in the Coscia case, the CFTC guidance, the CME guidance and the ICE Futures guidance. The exchanges, federal regulators and criminal authorities are sensitive to trading practices that may disrupt the futures and securities markets. They are communicating with one another, and appear to believe that through their written guidance they have communicated their expectations to market participants.

It is fair to say that today, and going forward, the standard setters and rule enforcers will expect traders to be aware of concerns around spoofing, and will expect firms to take steps to detect and prevent spoofing in their own operations. There is now a regulatory dragnet set for spoofers. But if trading strategies are carefully conceived, properly vetted, well-documented and faithfully monitored, traders may be able to avoid unwarranted investigations, alleviate regulatory concerns that may arise, and should be able to fully and confidently participate in the financial markets.

—By Clifford C. Histed, K&L Gates LLP

Cliff Histed is a partner in K&L Gates LLP's government enforcement practice. Prior to joining the firm, he was a prosecutor in the U.S. Attorney's Office, Northern District of Illinois, where he was a deputy chief in its Securities and Commodities Fraud Section, and supervised that office's investigation and indictment of Michael Coscia. Previously, Histed was a supervisory enforcement attorney with the CFTC, in-house counsel for a global energy trading company, a state prosecutor and a criminal investigator.

[1] U.S. v. Michael Coscia, Case No. 14 CR 551 (N.D. Ill.), Dkt. 36.

[2] Id., Dkt. No. 36 at 3.

[3] Id. at 4.

[4] Id. at 10.

[5] Id. at 5-6.

[6] Id. at 9.

[7] Id.

[8] Id. at 10.

[9] Id. at 11.

[10] Id. at 12.

[11] Id. at 16-17.

[12] Id. at 14-15.

[13] Id. at 15.

[14] Rule 11(a)(2) of the Federal Rules of Criminal Procedure.

[15] Found at http://www.cmegroup.com/tools-information/lookups/advisories/market-regulation/CME_CBOT_NYMEX_COMEX_RA1405-5.html.

[16] Id. at 2.

[17] Id. at 5.

[18] Id. at 7 citing Drexel Burhnam Lambert, Inc. v. CFTC, 850 F.2d 742, 748 (D.C. Cir. 1988).

[19] CFTC Division of Market Oversight, Rule Enforcement Review of the Chicago Mercantile Exchange and the Chicago Board of Trade, July 26, 2103, at 18. Found at http://www.cftc.gov/ucm/groups/public/@iodcms/documents/file/rercmecbot072613.pdf

[20] Id.

[21] Id. at 6-7.

[22] Letter dated January 3, 2011 from then CME Group CEO Craig Donahue to the CFTC concerning its Nov. 2, 2010, ANPR, page 10, found at http://comments.cftc.gov/PublicComments/ViewComment.aspx?id=27270&SearchText=.

[23] Found at https://www.theice.com/publicdocs/futures_us/exchange_notices/IFUS_Disruptive_Practices_Notice.pdf.

[24] CME Market Regulation Advisory Notice, Aug. 29, 2014, at 5.

[25] See, for example, Futures Industry Association Principal Traders Group, Recommendations for Risk Controls in Trading Firms, November 2010, found at https://secure.fia.org/downloads/Trading_Best_Pratices.pdf.

[26] See, for example, CFTC Technology Advisory Committee, Recommendations on Pre-Trade Practices for Trading Firms, Clearing Firms, and Exchanges Involved in Direct Market Access, March 1, 2011, found at http://www.cftc.gov/ucm/groups/public/@swaps/documents/dfsubmission/tacpresentation030111_ptfs2.pdf; and FINRA, Equity Trading Initiatives: Supervision and Control Practices for Algorithmic Trading Strategies, March 2015, found at https://www.finra.org/sites/default/files/notice_doc_file_ref/Notice_Regulatory_15-09.pdf.

[27] CME Rulebook, § 408.D.

[28] See, for example, the CFTC's press release concerning an enforcement action taken against a trading company and its employees who were accused of engaging in the disruptive trading practice called "marking the close." Found at http://www.cftc.gov/PressRoom/PressReleases/pr5521-08.

[29] The government made extensive use of exchange-recorded telephone calls from the Chicago Board of Trade trading floor in the 2010 criminal trial of former floor trader David Sklena. U.S. v. David G. Sklena, 09 CR 302, (N.D. Ill.). The government also made extensive use of internally recorded telephone calls of corporate bond trader and cash manager Sentinel Management Group Inc. in the 2014 criminal trial of its CEO, Eric Bloom. U.S. v. Eric A. Bloom, 12 CR 409 (N.D. Ill.).