Spoofing the Order Book: UK and U.S. regulators take aim
by William Yonge (Morgan Lewis) and Seonaid Mackenzie (Sturgeon)

What Is Spoofing?

"Spoofing" is a form of market manipulation in which the trader layers the order book by submitting multiple orders on one side of an exchange's order book at prices away from the touch in order to move the price but with no intention to execute. The trader then executes an order on the other side of the order book to take advantage of the price movement, following up with a rapid cancellation of the orders submitted initially. In short, the market has been "spoofed" and the trader has thereby profited at the expense of other investors and the market's integrity.

The UK's civil market abuse regime was first introduced in 2001 and amended in 2005 to implement the EU Market Abuse Directive, under which manipulative transactions constitute a type of market abuse. Manipulative transactions include those that are likely to give a false or misleading impression as to the supply of, price of, or demand for, one or more qualifying investments and are executed without legitimate reason.

In August 2009, the FSA (the FCA's predecessor) publicised concerns about such order book conduct and behaviour at regulated firms offering their clients direct market access ("DMA"), believing the practice could constitute market abuse. The regulator has since taken enforcement actions against perpetrators. Similarly, around this time, the London Stock Exchange ("LSE") addressed this topic for its member firms, reminding them of their obligations under LSE rules to ensure they exercise adequate control over activity on its DMA platforms.

In 2010, the U.S. Commodity Exchange Act ("CEA") was amended to prohibit any person from engaging in any trading, practice, or conduct on or subject to the rules of a futures or swap exchange (or other "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)." To clarify the type of conduct that is prohibited, the U.S. CFTC published guidance on spoofing and other disruptive trading practices. Among other things, the CFTC noted that a spoofing violation requires a market participant to act with some degree of intent beyond recklessness to violate the statute. Moreover, when distinguishing between legitimate trading and spoofing, the CFTC explained that it intends to evaluate the market context, the person's pattern of trading activity (including fill characteristics), and other relevant circumstances.

Enforcement Actions By the UK and U.S. Regulators

Under the UK market abuse regime, both the FCA and the courts may impose an unlimited fine for spoofing. In the FCA's words: "Abusive strategies that act to the detriment of consumers or market integrity will not be tolerated." By way of example, in the Summer of 2011, the FSA obtained a court injunction against an English fund management company operating from a Swiss branch called Da Vinci Invest Limited, a related Singapore company, and a Seychelles company—along with three individuals resident in Switzerland and/or Hungary trading on behalf of those companies—to prevent manipulative activities concerning UK-listed shares.

These defendants traded on a UK-based multi-lateral trading facility offering DMA, which reported its suspicions to the FSA. The FSA proceeded to bring a claim in the High Court for a final injunction and fine against the defendants. The defendants' spoofing was shown to have consistently resulted in them buying shares at lower prices and selling shares at higher prices than would have been the case had the strategy not been employed. On 12 August 2015, the court imposed fines against the defendants totalling £7,570,000.

In May 2011, the FSA imposed a fine of £8 million on Swift Trade for market abuse arising from spoofing. Curiously, the individual traders implicated in the Da Vinci case had previously traded on behalf of Swift Trade but were not defendants in the FSA's action against Swift Trade.

The CFTC recently has used its new statutory authority to enforce a prohibition against spoofing and the DOJ recently brought criminal charges for commodities fraud against an individual for spoofing. Under the CEA, spoofing is punishable by a maximum sentence of 10 years' imprisonment and a fine of $1 million. A count of commodities fraud is punishable by a maximum sentence of 25 years' imprisonment and a $250,000 fine.

On October 1, 2014, Michael Coscia, founder of Panther Energy Trading LLC, was indicted in the U.S. on six counts of commodities fraud and six counts of spoofing in the first criminal spoofing case. The indictment alleges that Coscia and Panther engaged in spoofing by using a sophisticated computer trading algorithm to place trades and promptly cancel trades before execution to create the illusion of market interest, artificially moving prices in Coscia's favour. After the market reacted to the non-bona fide trades, Coscia placed and filled real trades, realizing $1.5 million in profits.

Interestingly, the FCA had earlier investigated and taken action against Coscia, its inaugural enforcement action against a high frequency trader. In July 2013, the FCA fined Coscia $903,178 for market manipulation of commodities futures on the UK's ICE Futures Europe Exchange using an algorithmic programme he had designed to engage in layering. Notably, Coscia and Panther's trading activity originated from the U.S. but involved the submission of orders to a UK-regulated market.

More recently, in an example of its global reach, the CFTC filed a civil complaint against Navinder Singh Sarao, a London-based high-frequency trader, and his firm. The CFTC alleges that Sarao manipulated CME's E-mini S&P 500 futures contract by placing—and then promptly cancelling or modifying just before execution—hundreds or thousands of "exceptionally large" trades. Sarao's actions enabled him to prime the market, artificially moving contract prices in his favour just before placing and filling real trades, in order to net millions of dollars in profits. The CFTC also alleges that Sarao's spoofing contributed to an extreme order book imbalance in the E-mini S&P market during the Flash Crash on May 6, 2010.

Compliance Considerations

Spoofing presents unique compliance challenges because the nature and scope of the offence remain ill-defined. Yet, spoofing is a priority among prosecutors and regulators, and brokers and exchanges are monitoring market participants for potential spoofing activities. Firms should assume that information they provide to brokers about their trading activities will be shared with regulatory authorities and law enforcement. Consequently, firms may wish to review their trading with the recent regulatory guidance and cases in mind. Such a review

should focus on trading strategies that deploy algorithms, involve a high volume of market activity, or have lower fill rates.

Firms also may consider instituting procedures for designing, testing, and introducing new trading technologies, algorithms or other system features or capabilities, and identify the types of changes that must be reviewed by appropriate compliance, risk, and operations representatives before implementation. Moreover, firms should identify specific trading trends, strategies, behaviours or positions that trigger mandatory business or compliance reviews. For example, unusual quoting activity—such as unusual volumes of quotes, modifications or cancelations or quotes submitted without a resulting transaction—or breaches of, or frequent changes to, risk limits could become subject to business and compliance reviews.

William Yonge is a solicitor and partner at Morgan, Lewis & Bockius UK LLP
+44 (0) 20 3201 5646
wyonge@morganlewis.com
Condor House
5-10 St. Paul's Churchyard
London EC4M 8AL