"Spoofing": US Law and Enforcement

PRACTICAL LAW FINANCE AND AARON STEPHENS, ZACH FARDON, KATHERINE KIRKPATRICK, MICHAEL WATLING, MATTHEW WISSA, AND MARGARET NETTESHEIM, KING & SPALDING LLP

A Practice Note providing an overview of the US legal and regulatory framework relating to spoofing, a market manipulation offense, including relevant criminal prosecutions and civil enforcement cases.

Spoofing is a form of market manipulation in which a trader submits and then cancels offers or bids in a security or commodity on an exchange or other trading platform with the co-existent intent to cancel the bid or offer before it can be executed.

Spoofing may take various forms, but it often involves the placing of non-bona-fide, large or small volume orders on one side of the order book and then canceling those orders either immediately or within a short period of time after placement. A spoofer's intent may be to alter the appearance of supply or demand to artificially move the price and therefore mislead – or spoof – other traders in the relevant security or commodity, benefitting his or her own trading position(s). Spoofing is also referred to as "layering" the order book, which involves the trader placing multiple, non-bona-fide orders on one side of the order book to manipulate the price and thus benefit their position(s) on the other side of the order book.

Spoofing often uses algorithmic and high frequency trading technology, which allows trading decisions to be generated quickly and transactions to be completed in fractions of a second. In general, algorithmic and high frequency trading are legitimate trading methods. However, regulators have scrutinized algorithmic trading methods and consider some to be improper market manipulation.

In the US, spoofing in commodities trading is a specified criminal and civil offense. The securities laws while not specific to spoofing may also be used to prosecute spoofing-like behavior. When prosecuting spoofing, the trader's intent is pivotal; the government or regulator must prove that the trader intended to cancel the order at the time it was placed.

This Note summarizes US law on spoofing and how spoofing is prosecuted in the US. This Note also provides examples of the types of trading practices that may constitute spoofing.

US SPOOFING LAW AND ENFORCEMENT: AT A GLANCE

Enforcement authorities	■ CFTC (civil). ■ Securities and Exchange Commission (SEC) (civil). ■ Financial Industry Regulatory Authority (FINRA) (civil). ■ Department of Justice (DOJ) (criminal).
Current Law	■ Dodd-Frank Act, Section 747. ■ Commodity Exchange Act (CEA), Section 4c(a)(5)(C). ■ Securities Exchange Act of 1934, as Amended (Exchange Act), Sections 10(b) and 9(a)(2). ■ Securities Act of 1933, as Amended (Securities Act), Section 17(a). ■ SEC Rule 10b-5. ■ FINRA Rule 2020. ■ FINRA Rule 5210.
Key Points	■ US law includes specific civil and criminal anti-spoofing provisions. ■ Intent: In all cases, requires proof of the individual's intent to cancel the bid or offer before execution. ■ In civil cases brought by the CFTC, individuals must be found to have acted "with some degree of intent, or scienter, beyond recklessness." (78 Fed. Reg. at 31896.) The standard of proof for civil cases is proof by a preponderance of the evidence. ■ In criminal cases brought by the DOJ, the prosecutor must prove the individual "knowingly" engaged in spoofing. The DOJ can prosecute spoofing under the CEA, or instead, under the mail, wire, and commodities fraud statutes. (7 U.S.C. § 13(a)(2); CEA § 9(a)(2); 18 U.S.C. §§ 1341, 1343, and 1348.) The standard of proof in criminal cases is proof beyond a reasonable doubt.

LEGAL TRADING STRATEGIES AND SPOOFING

As noted, to prove spoofing under the CEA, the government or regulator must show that the trader intended to cancel his or her bid or order before execution. However, there are a number of legitimate, legal trading strategies in which bids or orders are canceled before execution. Additionally, most orders in the securities and commodities markets go unfilled. The CFTC has delineated under the CEA which trading strategies are legal and which trading cancelation strategies are illegal. As such, prosecutors and regulators must distinguish between legitimate and illegitimate trading activities in which traders cancel their bids or offers to determine whether the canceled trade is spoofing.

The following sections set out non-exclusive lists of different types of trading practices, legal and illegal, that use cancelation methods. The legal practices are common on US exchanges.

LEGAL ORDER CANCELATIONS

The following are examples of legitimate (and legal) market-based order cancelations:

- **Fill or kill (FoK) order.** This is an order that demands immediate execution or cancelation, typically involving a designation added to an order instructing the broker to offer or bid (as the case may be) one time only; if the order is not filled immediately it is then automatically canceled.
- **Stop-loss (or stop-limit) order.** This is an order that goes into force as soon as there is a trade at the specified price. The order can only be filled at the stop price or higher.
- **All or none (AON) order.** This is an order to buy or sell a stock that must be executed in its entirety or not executed at all. However, unlike the FoK orders, AON orders that cannot be executed immediately remain active until they are executed or canceled.
- **Iceberg order (hidden quantity order).** This is an order placed on an electronic trading system whereby only a portion of the order is visible to other market participants. As the displayed part of the order is filled, additional portions of the order become visible.
- **Passive order.** This is an offer to sell at a price that is higher than the price at which other traders are currently willing to buy. Passive orders rest for at least some amount of time after being placed and are not guaranteed to execute.

ILLEGAL ORDER CANCELATIONS

The following are examples of illegal order cancelations, in which attempted market manipulation is the impetus for the order:

- **Spoofing.** As noted above, spoofing means placing non-bona-fide orders with the intention of affecting the market price of a security or commodity without intending to execute the trades.
- **Layering.** This is another form of spoofing, involving placing multiple non-bona-fide orders that favorably modify the price, and are followed by an executed trade on the opposite side of the market that takes advantage of the temporarily manipulated price.
- **Wash trading.** This involves entering into, or purporting to enter into, transactions that give the appearance that purchases and sales have been made without incurring market risk or changing the trader's market position.

OFFENSES AND US ENFORCEMENT FRAMEWORK

REGULATOR/AUTHORITY: CFTC AND DOJ

The CFTC enforces the civil provisions of the CEA, including the anti-spoofing provisions. In a civil action, the relevant authority depends on the underlying contract being traded. If the trader is trading in commodities or derivatives, the CFTC has jurisdiction; if it is securities, the SEC has jurisdiction.

The DOJ has the authority to criminally prosecute spoofing violations of the CEA, as well as the federal mail, wire, and commodities fraud statutes.

The CFTC provides further details on this in its interpretative guidance and policy statement on disruptive practices (CFTC Guidance) (see Legal Update, CFTC Proposes Guidance on Prohibition of Disruptive Swap Trading Practices under Dodd-Frank (8-504-9766)).

In addition to the CFTC Guidance, certain US exchanges have also published rules and guidance on what constitutes spoofing. For example:

- The Chicago Mercantile Exchange (CME) has published a market regulation advisory notice (CME Group RA1807-5).
- Intercontinental Exchange (ICE) Futures US has published a set of FAQs on disruptive trading practices.

SPOOFING OFFENSES UNDER THE CEA AND CFTC REGULATIONS

In 2010, the Dodd-Frank Act amended the CEA to include spoofing as a disruptive practice. The anti-spoofing provision, CEA Section 4c(a)(5)(C), makes it unlawful for any person to engage in spoofing, which is formally defined as "bidding or offering with the intent to cancel the bid or offer before execution" (7 U.S.C. § 6c(a)(5)).

The CFTC Guidance suggests four non-exclusive examples of situations that may constitute spoofing:

- Submitting or canceling bids or offers to overload the quotation system of a CFTC-registered entity.
- Submitting or canceling bids or offers to delay another person's execution of trades.
- Submitting or canceling multiple bids or offers to create an appearance of false market depth.
- Submitting or canceling bids or offers with intent to create artificial price movements upwards or downwards.

To constitute spoofing, the trader must act with the specific (or at least "beyond reckless") intent to cancel the bid or offer prior to execution.

In civil cases, it is somewhat ambiguous as to whether this means "specific intent" (as understood under US law to be the subjective desire or knowledge that the prohibited result will occur (see *People v. Owens*, 131 Mich. App. 76, 345 N.W.2d 904 (1983)) or some other standard of intent.

The CFTC Guidance states that:

> The Commission interprets that a CEA section 4c(a)(5)(C) violation requires a market participant to act with **some degree of intent, or scienter, beyond recklessness** to

engage in the "spoofing" trading practices prohibited by CEA section 4c(a)(5)(C). Because CEA section 4c(a)(5)(C) requires that a person intend to cancel a bid or offer before execution, the Commission believes that **reckless trading, practices, or conduct will not constitute a "spoofing" violation**." (Our emphasis added.)

In a criminal case, the DOJ must go one step further and establish that the market participant knowingly acted with specific intent at the time the order was placed. This means that the individual realized what he or she was doing and was aware of the nature of his or her conduct, and did not act through ignorance, mistake, or accident. *See* Pattern Criminal Jury Instructions of the Seventh Circuit (2012 Ed.), Instruction 4.10 defining "knowingly."

In any event, statistical data by itself is not enough for enforcers to demonstrate intent since it is common practice for traders to cancel orders and bids after they are placed for a variety of legitimate purposes. Further, a pattern of trading is not necessary for a violation to occur; in theory at least, a trader could spoof the market with a single order.

Under CFTC Regulation 166.3, an entity may be charged with a failure to supervise if its traders engage in spoofing. CFTC Regulation 166.3 requires each CFTC registrant to diligently supervise the handling by its partners, officers, employees and agents of all commodity interest accounts and activities relating to its business as a registrant. Regulation 166.3 does not require proof of an underlying violation. Therefore, a firm can be found to have violated Regulation 166.3 even if there was ultimately no spoofing violation.

PENALTIES UNDER THE CEA AND CFTC REGULATIONS FOR SPOOFING VIOLATIONS

- Spoofing under the CEA is a felony punishable by up to $1 million in penalties and up to ten years in prison for each spoofing count (7 U.S.C. § 13(a)(2)).
- Civil penalties or administrative sanctions may include orders imposing civil monetary penalties; suspending, denying, revoking, or restricting registration and exchange-trading privileges, orders of restitution, appointment of a receiver, freezing of assets, and disgorgement of unlawfully acquired benefits. CFTC Enforcement Manual https://www.cftc.gov/LawRegulation/Enforcement/OfficeofDirectorEnforcement.html
- The CEA also provides that the CFTC may obtain certain temporary relief on an *ex parte* basis. When those enjoined violate court orders, the CFTC's Division of Enforcement may seek to have the offenders held in contempt.
- Violation of CFTC Regulation 166.3 may result in a $25 million monetary civil penalty (17 C.F.R. § 166.3).

Note that certain individuals have entered into non-prosecution agreements (NPA) (see, for example, this June 2017 CFTC press release).

DEFENSES TO SPOOFING CHARGES UNDER THE CEA

As noted, reckless trading practices do not violate CEA Section 4c(a)(5)(C) (see Offenses). Orders, modifications, and cancelations are not considered spoofing if they are submitted as part of a legitimate, good faith attempt to consummate trading (for example, partially filled orders or properly placed stop-loss orders).

CME Group provides examples of reckless trading behavior. For example:

- A market participant enters orders into the market with reckless disregard for the adverse impact on orderly trading. This can be done by sending a broker a large customer order in a product that is illiquid; where, given the depth of the order book, filling the order at the market would trade through several price levels and cause significant price movement.
- A market participant designs an algorithm to be used in a very liquid market but subsequently uses the algorithm in a very illiquid market without making amendments to the algorithm. The algorithm gets stuck in a looping pattern in responding to itself and causes pricing aberrations.

REGULATOR/AUTHORITY: SEC AND DOJ; FINRA

The SEC can bring a civil enforcement action for spoofing under the general anti-manipulation and anti-fraud provisions of the Exchange Act and the Securities Act. The DOJ can prosecute criminally. In addition, FINRA member firms and associated individuals could face enforcement activity in relation to any breach of FINRA's rules.

SPOOFING OFFENSES UNDER THE US SECURITIES LAWS

Section 17(a) of the Securities Act prohibits the fraudulent sales of securities and makes it unlawful for any person in the offer or sale of any security or any security-based swap (SBS) agreement, by the use of any means or instruments of transportation or communication in interstate commerce or by the use of the US mails, directly or indirectly, to do any of the following:

- Employ any device, scheme, or artifice to defraud.
- Obtain money or property by means of any untrue statement of a material fact or any omission to state a material fact necessary to make the statements made, in light of the circumstances under which they were made, not misleading.
- Engage in any transaction, practice, or course of business that operates or would operate as a fraud or deceit upon the purchaser (15 U.S.C. § 77q(a)).

Section 9(a)(2) of the Exchange Act prohibits manipulation of securities prices and makes it unlawful to effect, alone or with one or more other persons, a series of transactions in any security creating actual or apparent active trading in such security, or raising or depressing the price of such security, for the purpose of inducing the purchase or sale of such security by others (15 U.S.C. § 78i).

Section 10(b) of the Exchange Act prohibits fraud in connection with the purchase or sale of any security and makes it unlawful for any person, directly or indirectly, by the use of any means or instrumentality of interstate commerce or of the mails, or of any facility of any national securities exchange, to use or employ a manipulative or deceptive device or contrivance in contravention of such rules and regulations as the SEC may prescribe (15 U.S.C. § 78j(b)).

Rule 10b-5 prohibits fraud, misrepresentation, and deceit in connection with the purchase or sale of any security and makes

it unlawful for any person, directly or indirectly, by the use of any means or instrumentality of interstate commerce or of the mails or of any facility of any national securities exchange, to use any device, scheme, or artifice to defraud (17 C.F.R. § 240.10b-5).

FINRA Rule 2020 prohibits securities brokers and dealers from effecting any transaction in, or inducing the purchase or sale of, any security by means of any manipulative, deceptive, or other fraudulent device or contrivance.

Additionally, FINRA Rule 5210, together with Supplementary Material .02 to Rule 5210, requires firms to adopt policies and procedures addressing "self-trades," which are defined as "transactions in a security resulting from the unintentional interaction of orders originating from the same firm that involve no change in the beneficial ownership of the security." Under Rule 5210 and Supplementary Material .02, firms must have policies and procedures in place that are reasonably designed to review their trading activity for, and prevent, a pattern or practice of self-trades resulting from orders originating from a single algorithm or trading desk or from related algorithms or trading desks. Self-trades resulting from orders that originate from unrelated algorithms or separate and distinct trading strategies within the same firm are generally considered to be bona-fide transactions.

PENALTIES FOR SPOOFING UNDER US SECURITIES LAWS AND FINRA RULES

Willful violations of the Securities Act or the Exchange Act are punishable by disgorgement of profits and a civil fine of up to $5 million or imprisonment of not more than 20 years.

For member firms, violations of FINRA Rule 2020 are punishable by censure, fine, suspension from securities activities in full or limited capacity for up to two years, or, in egregious cases, expulsion of the firm from FINRA membership. For associated individuals, such violations are punishable by censure, fine, suspension for up to two years, or permanent bar from FINRA membership. Intentional or reckless violations of FINRA Rule 5210 may result in similar sanctions.

UNITED STATES V. VORLEY AND CHANU: DOJ CHARGES SPOOFERS UNDER WIRE FRAUD STATUTE, NOT CEA

In July 2018, the DOJ indicted James Vorley and Cedric Chanu, two traders who worked at a global investment bank. The indictment alleged that the defendants engaged in an illegal, years-long spoofing scheme that involved tricking other traders into buying or selling futures contracts (which fall under the CEA's jurisdiction) at prices they otherwise would not have. However, instead of charging under the CEA, which explicitly prohibits spoofing, the government charged wire fraud affecting a financial institution and conspiracy to commit wire fraud affecting a financial institution (Conspiracy to Commit Wire Fraud Affecting a Financial Institution in violation of 18 U.S.C. § 1349; and Wire Fraud Affecting a Financial Institution in violation of 18 U.S.C. § 1343).

The federal wire fraud statute includes a longer statute of limitations when the offense affects a financial institution – ten years – as opposed to five under the CEA, and greater penalties than the CEA. The government has argued that this was warranted due to the allegations the defendants engaged "in spoofing with fraudulent intent and in order to obtain money or property from someone else."

The government also argued that a trader's order includes an "implicit representation" that the trader intends for the order to be filled, even where the trader is not in a fiduciary relationship with any actual or potential counterparty.

The Northern District of Illinois has yet to rule on the matter, but defendants have filed a motion to dismiss the charges. Several financial industry advocacy groups (including the US Chamber of Commerce, the Bank Policy Institute, the Futures Industry Association (FIA), and the Securities Industry and Financial Markets Association (SIFMA)) have filed amicus briefs supporting defendants' position. Among other things, the amicus briefs argue that, in the CEA, Congress and the CFTC have established a comprehensive statutory and regulatory regime to govern the futures markets and that the application of the wire fraud statute to open orders in those markets may adversely affect the proper and efficient functioning of the markets.

For information on mail and wire fraud, see Practice Note, Mail and Wire Fraud under 18 U.S.C. §§ 1341, 1343, and 1346 (W-017-5124).

ENFORCEMENT OF SPOOFING LAWS BY US AUTHORITIES

CFTC V. NAVINDER SINGH SARAO

In November 2016, in *CFTC v. Navinder Singh Sarao*, point-and-click trader Navinder Singh Sarao was ordered to pay $38.6 million in penalties and disgorgement after pleading guilty to one count of wire fraud and one count of spoofing on the CME from 2010 to 2014. Sarao is a UK national who the UK courts allowed US authorities to extradite. During the relevant time period, Sarao traded tens of thousands of E-mini futures contracts in calculated, short time intervals. The CFTC found that Sarao, "utilized a combination of automated and manual trading systems to place, modify, and cancel orders, resulting in a high number of orders, modifications, cancelations, and transactions, especially compared to other E-mini S&P market participants."

Specifically, Sarao placed orders on May 6, 2010 that were modified more than 81,000 times, with only 81 lots resulting in executed trades. Sarao's manipulative trading method was alleged to have contributed to the 2010 "flash crash," in which the Dow Jones Industrial Average index dropped 1,000 points but quickly recovered in 20 minutes. Sarao admitted that he made a profit of $12.8 million as a result of this scheme. To prove his intent, the government presented evidence of emails between Sarao and a trading platform programmer, discussing the inclusion of the following functions: a "cancel if close function," the ability to "alternate the closeness (that is, one price away or three prices away)," and "a facility to be able to enter multiple orders at different prices using one click."

For more information on this case, see this CFTC press release.

UNITED STATES V. JITESH THAKKAR

In March 2019, more than a year after Sarao pleaded guilty (see *CFTC v. Navinder Singh Sarao*), the trial of Jitesh Thakkar began. Thakkar was the software engineer who created the program that enabled Sarao's trading and allegedly contributed to the 2010 flash crash.

In January 2018, Thakkar, the owner of Edge Financial Technologies Inc., became the first fintech software engineer to be charged, in *CFTC v. Jitesh Thakkar and Edge Financial Technologies Inc.*, as a co-conspirator for use of one's proprietary trading technology by another party. There was speculation that, if the government succeeded in convicting Thakkar, it would open the door to future prosecutions against programmers and specific targeting of the use of "smart contracts" that can be written by programmers directly into the code of a trading program.

However, the judge dismissed the conspiracy charges mid-trial, allowing the case to continue solely on the spoofing charges. The jury ultimately deadlocked on the charges and the judge declared a mistrial. The government decided not to pursue a retrial. This setback for the DOJ may reverberate beyond *Thakkar*, as it could temper the DOJ's more creative attempts to expand the scope of spoofing liability.

UNITED STATES V. COSCIA

In August 2017, in *United States v. Coscia*, the Seventh Circuit upheld the conviction of trader Michael Coscia for spoofing, holding that:

> "The [CEA's] anti-spoofing provision provides clear notice and does not allow for arbitrary enforcement. Consequently, it is not unconstitutionally vague."

(866 F.3d 782 at 785 (7th Cir. 2017).

The underlying CEA spoofing charges were based on Coscia's calculated trading method in which he used pre-programed algorithms to execute trades of commodities (gold, soybean oil, and high-grade copper) in 2011. To carry out this scheme, Coscia created artificial market movement by placing small orders of commodities futures at a price higher than the then-current sell-side market price. He later placed large orders on the buy side in increasing price increments to create the illusion that there was price movement. Once the market price met Coscia's buy position, he would cancel the large buy-side orders.

Coscia executed these trading strategies thousands of times, profiting in the amount of $1.4 million. The Seventh Circuit distinguished legal trading practices involving canceled orders from spoofing activities also involving canceled orders by clarifying that spoofing requires the intent to cancel the order *at the time it was placed*.

Conversely, the execution of legal trading practices such as FoK orders and stop-loss orders relies on the occurrence of certain subsequent events (see Legal Order Cancellations). The government proved Coscia's intent to cancel using testimony from trading program designers who stated that he asked that the programs act:

> "[l]ike a decoy," which would be "[u]sed to pump [the] market" and that "large-volume orders were designed specifically to avoid being filled and accordingly would be canceled in three particular circumstances: (1) based on the passage of time (usually measured in milliseconds); (2) the partial filling of the large orders; and (3) complete filling of the small orders."

Based on this evidence, the Seventh Circuit affirmed that a rational jury could have found that Coscia intended to cancel the orders before they were executed, violating the anti-spoofing provision of the CEA.

For further information on the Coscia case, see:

Article, Spoofing, Regulation AT, and Algorithmic Trading: The Coscia Case (W-000-8918).

Legal Update, CFTC Chairman Announces Upcoming Rules, Warns on Enforcement: Warning on Spoofing and Market Manipulation (W-000-7400).

FCA: Final Notice to Michael Coscia

Coscia had also previously settled charges in the UK. In July 2013, the FCA issued a final notice to Coscia, fining him £597,993 for layering thousands of futures orders on ICE Futures Europe (ICE) in violation of section 118(5) of FSMA. Specifically, the FCA found that over a period of six weeks and using high frequency trading, Coscia placed large orders in the order book for less than one second, after which the orders (small or large) were canceled immediately and simultaneously if not previously executed. The FCA concluded that Coscia's trading activity created a misleading impression on the market as his large canceled orders created false impressions of liquidity and caused at least one significant market participant to withdraw from ICE.

For more information, see Legal update, FCA fines US based high frequency trader for deliberate manipulation of commodities markets (7-535-2786).

UNITED STATES V. FLOTRON

In April 2018, in *United States v. Flotron*, a jury in the US District Court for the District of Connecticut acquitted Andre Flotron, a Swiss national and former precious metals trader at a global investment bank, of conspiracy to commit wire fraud, commodities fraud, and spoofing. Prosecutors charged Flotron on the basis of his pattern of order and trade activity.

Specifically, his trading pattern entailed placing small trades which were capable of execution (primary orders) on one side of the market close to the prevailing price. Then, either before or after placement of the primary order, Flotron placed a larger order on the opposite side of the market from the primary order (opposite order) that was at least ten times as large as the size of the primary order and close to the prevailing price. When at least one of the primary orders was filled, Flotron would immediately cancel his opposite order within five seconds of placing the opposite order and before the opposite order could be executed.

The government presented evidence of trading data and testimony from Flotron's two former colleagues, who claimed that he taught them how to spoof and that it was commonplace in the industry. The defense argued that the data alone did not prove intent because it did not show the trades were inappropriate, particularly since trades are often canceled.

For information on conspiracy charges, see Practice Note, Conspiracy Charges: Overview (W-009-8988).

UNITED STATES V. GANDHI AND *UNITED STATES V. MOHAN*

In November 2018, two commodities traders pled guilty to conspiracy to engage in wire fraud, commodities fraud, and spoofing, in *United States v. Gandhi* and *United States v. Mohan*.

Gandhi and Mohan admitted that, from March 2012 to March 2014, they conspired with fellow trader Yuchun "Bruce" Mao and others at their trading firm to mislead the markets for E-Mini S&P 500 and E-Mini NASDAQ 100 futures contracts traded on CME, as well as E-Mini Dow futures contracts traded on the Chicago Board of Trade (CBOT). In addition, the ex-traders admitted they and their co-conspirators placed thousands of orders that they did not intend to execute in order to obtain executions of other orders at better prices, quantities, and times. The scheme resulted in market losses of more than $60 million.

Further, Gandhi admitted that, from May 2014 to October 2014, while employed at a different trading firm, he conspired with others to mislead the markets for E-Mini S&P 500 futures contracts traded on the CME by agreeing to place, and placing, hundreds of spoof orders for E-Mini S&P 500 futures contracts, to create the false and misleading appearance of increased supply or demand. The scheme resulted in market losses of more than $1.3 million. Both Gandhi and Mohan are awaiting sentencing.

For more information on these cases, see this DOJ press release.

Gandhi and Mohan separately settled civil charges with the CFTC, admitting engaging in manipulative and deceptive schemes that involved thousands of acts of spoofing. For further information, see this CFTC press release and this CFTC press release.

CFTC "FAILURE TO SUPERVISE" ACTION

In January 2017, the CFTC filed and settled its first "failure to supervise" case against a registered firm related to spoofing. Under CFTC Regulation 166.3, firms must employ diligent supervision of their employees and activities and case law has interpreted this duty of diligence broadly.

In January 2018, the CFTC filed eight anti-spoofing enforcement actions against three entities, and ultimately settled supervisory violations as part of those actions. For details, see Legal Update, DOJ, CFTC, FBI File Spoofing Charges Against Three Banks and Eight Individuals (W-013-0012), as well as this CFTC press release and this CFTC press release.

CFTC SPOOFING ORDERS

Victory Asset Inc.

In September 2018, the CFTC settled allegations against Victory Asset Inc. and its trader Michael Franko for spoofing, in violation of CEA Sections 4c(a)(5) and 6(c)(1) without admitting or denying the allegations. The CFTC alleged that Franko's cross-market spoofing sought to take advantage of the correlation between prices of copper future contracts on US and UK exchanges. Victory and Franko agreed to pay civil monetary penalties of $1.8 million and $500,000, respectively, with Franko further banned from trading in US futures markets for a period of six months.

For more information, see this CFTC press release.

Mizuho Bank Ltd

In September 2018, in *In re Mizuho Bank Ltd*, the CFTC alleged that a Singapore-based interest rates trader violated CEA Section 4c(a)(5) by placing large orders and then canceling them within seconds. However, the CFTC did not allege that any trader placed or executed a genuine order meant to benefit from the illicit order. Rather, the CFTC alleged that the trader "placed these spoof orders to test market reaction to [the trader's] trading in anticipation of having to hedge Mizuho swaps positions with futures at a later date." Mizuho agreed to pay a civil fine of $250,000 without admitting or denying the allegations.

Mizuho is the first CFTC spoofing action in which the CFTC took advantage of the court's articulation in *Coscia* (see *United States v. Coscia*) regarding the elements of CEA Section 4c(a)(5) by solely alleging a spoof order without a corresponding primary order meant to benefit from the spoof.

For additional detail, see this CFTC press release.

Bank of Nova Scotia

In October 2018, the CFTC settled with the Bank of Nova Scotia (BNS). The complaint alleged that BNS engaged in multiple acts of spoofing in gold and silver futures contracts traded on the CME. BNS agreed to pay a $800,000 civil monetary penalty without admitting or denying the allegations. BNS self-reported the conduct to the CFTC after it became aware of the misconduct and cooperated with the CFTC's investigation, which resulted in a reduced monetary penalty.

For more information, see this CFTC press release.

SPOOFING NON-PROSECUTION AGREEMENTS

In June 2017, the CFTC entered into its first NPA involving spoofing. The CFTC entered into the NPA with three former traders employed by a global investment bank after observing large "book imbalances" in their company's trades and finding that the traders had engaged in spoofing on at least 80 occasions by:

- Placing large orders on the opposite side of the market from smaller orders.
- Quickly canceling the large orders within seconds after either the smaller resting orders had been filled or the traders believed that the spoofing orders were at too great a risk of being executed.

The CFTC also fined the bank $25 million in civil penalties for failure to supervise.

For more information, see this CFTC press release.

In June 2019, a provisionally registered swap dealer and global commodities trading business entered into an NPA with the DOJ and an order with the CFTC after admitting the company was at fault for two traders who spoofed the precious metals futures market. The six-year scheme beginning in 2008 involved manipulating market prices by placing thousands of misleading orders on Commodity Exchange Inc. for delivery of precious metals in the future.

The two individual traders were indicted on conspiracy, wire fraud, commodities fraud and spoofing charges, however, the company only faced a parallel civil investigation. Following the company's cooperation, the company agreed to pay $25 million to the DOJ and $11.5 million to the CFTC.

For more information on this case, see the DOJ press release and CFTC press release.

SEC AND FINRA ENFORCEMENT ACTIONS

Lek Securities Corporation, et al.

In March 2017, the SEC and FINRA filed related enforcement actions against broker-dealer Lek Securities Corporation and Avalon FA Ltd, an unregistered Ukraine-based trading firm, accusing Avalon of manipulating the US securities markets by engaging in layering, spoofing, and cross-market manipulation through Lek Securities' direct market access platform. The SEC alleged that Avalon, through Lek Securities, generated more than $28 million in illicit profits. After filing its complaint in the US District Court for the Southern District of New York, the SEC obtained an emergency order freezing Avalon's assets held in its account at Lek Securities, as well as freezing and repatriating funds that Avalon had transferred overseas. The enforcement action, which is pending in the Southern District of New York, seeks civil penalties and disgorgement of "all ill-gotten gains as a result of [defendants'] unlawful conduct."

FINRA, through its Department of Market Regulation, brought an independent action against Lek Securities and its CEO, Samuel F. Lek, charging them with aiding and abetting Avalon's fraud and violating FINRA rules concerning market access and supervision. FINRA also filed related actions on behalf of several exchanges, including the NYSE and Nasdaq. In its pending complaint, FINRA requests that its administrative tribunal make findings that, if sustained, would result in the statutory disqualification of Lek Securities in accordance with Article III, Section 4 of the FINRA by-laws.

For more information, see this SEC press release and FINRA press release.

For more information on SEC settlement, see Practice Note, What's Market: the SEC's Settlement Process (W-009-8980).

For summaries of SEC settlements visit What's Market, SEC Settlement Agreements.

KEY POINTS ON SPOOFING ENFORCEMENT

Both manual and high frequency, algorithmic trading methods have been the subject of spoofing enforcement in the US. Although regulators more commonly focus on large spoofing orders, they have analyzed small orders as well: a single canceled order may be scrutinized and form the basis of an offense.

Based on previous cases, authorities have scrutinized the following trading activity to determine whether it constitutes market manipulation:

- The number of times orders were modified (*Sarao*).
- The percentage of canceled or filled orders relative to the total number of orders placed (*Coscia, Flotron*).
- Placement of multiple orders at different price levels, which were canceled before they were filled (*Sarao*).
- The pattern of the order and trade activity (*Flotron*).
- The passage of time before large volume orders were canceled (*Coscia*).
- Large book imbalances in a company's trades (*CFTC NPA referred to above*).

Enforcement authorities use data from an individual's trading patterns as the basis for their enforcement actions. However, trading patterns that include cancelation strategies may be entirely legitimate. When distinguishing between legitimate trading and spoofing, the government must prove that the trader had the specific intent (or at least "beyond reckless" in a civil case) to cancel the order at the time it was placed.

To prove intent in spoofing cases, the government has offered evidence of contemporaneous communication and witness testimony. Based on the enforcement actions and cases to date, the determination of whether a trading practice constitutes spoofing in the US hinges on evidence surrounding the trader's intent in addition to an analysis of relevant trading data. Corporations can also be charged with failure to supervise spoofing if one of their traders is being prosecuted for spoofing.

07-19