THE REVIEW OF
SECURITIES & COMMODITIES REGULATION
AN ANALYSIS OF CURRENT LAWS AND REGULATIONS AFFECTING THE SECURITIES AND FUTURES INDUSTRIES

Vol. 55 No. 3 February 9, 2022

THE EVOLUTION OF SPOOFING ENFORCEMENT AND . . . AVOIDANCE

In this article, the authors begin by describing spoofing prohibitions in federal law and exchange rules. They then describe how regulators differentiate between spoofing and legitimate trading activity. Next, they turn to common types of spoofing identified in the cases and regulators' tools and practices for dealing with them. They conclude with the surveillance and supervisory processes firms will need to monitor trading by internal reviews to protect against possible inferences of spoofing activity.

By James G. Lundy, Nicholas A.J. Wendland, and David Yoshimura *

In recent years, the regulatory scrutiny over the prohibited type of conduct in derivatives markets commonly known as "spoofing" has resulted in the types of activities included in this definition to be more varied, more visible, and more likely to be the target of regulatory enforcement actions that can result in significant penalties for market participants. It is therefore imperative to keep apprised of developments in this regulatory enforcement arena to fully understand what does and does not constitute spoofing, and how to attempt to avoid conduct that may be deemed to be spoofing and the potential unnecessary exposure to the risk of enforcement actions.

"Spoofing" is a term used to describe a form of market manipulation that involves the submission of orders that the trader did not intend to execute at the time of order entry. Spoofing orders often form a pattern of deceptive order activity that leads to visible increases or decreases in the volume displayed on the order book and are intended to impact how other participants behave. This behavior undermines the integrity of the market and unfairly impacts unsuspecting market participants that rely on bona fide order activity to accurately reflect current market conditions and asset prices.

Civil and criminal legal ramifications of spoofing activities can be severe. These may include imprisonment, significant fines, and loss of trading privileges, among other civil and criminal penalties. The reputational harm to a trader or firm civilly charged with, or criminally convicted of, spoofing behavior is significantly detrimental.

In the regulatory sphere, while spoofing enforcement has evolved, it is still developing. This article summarizes guidance from recent cases to identify steps that market participants can take to avoid activity that

* *JAMES G. LUNDY is a partner at Faegre Drinker Biddle & Reath LLP. NICHOLAS A.J. WENDLAND is counsel and DAVID YOSHIMURA is an associate at the firm. Their e-mail addresses are james.lundy@faegredrinker.com, nicholas.wendland@faegredrinker.com, and david.yoshimura@faegredrinker.com. Mr. Lundy, Mr. Wendland, and Mr. Yoshimura represent clients in CFTC, SEC, and self-regulatory organization enforcement investigations and litigation.*

RSCR Publications LLC Published 22 times a year by RSCR Publications LLC. Executive and Editorial Offices, 2628 Broadway, Suite 29A, New York, NY 10025-5055. Subscription rates: $1,197 per year in U.S., Canada, and Mexico; $1,262 elsewhere (air mail delivered). A 15% discount is available for qualified academic libraries and full-time teachers. For subscription information and customer service call 609-683-4450; fax 609-683-7291; write Subscriber Services, RSCR Publications, PO Box 585, Kingston NJ 08528; e-mail cri.customer.service@comcast.net; or visit our website at www.rscrpubs.com. General Editor: Michael O. Finkelstein; tel. 212-876-1715; e-mail mofinkelstein@gmail.com. Associate Editor: Sarah Strauss Himmelfarb; tel. 301-294-6233; e-mail sarah.s.himmelfarb@gmail.com. To submit a manuscript for publication contact Ms. Himmelfarb. ISSN: 0884-2426.

may constitute or appear to be spoofing behavior. It also provides guidance on what to consider when designing a supervision and compliance program, which regulators may evaluate for training, prevention, and management of market conduct at the firm level. Before trading, market participants should ensure they are aware of all current rules and regulatory guidance related to spoofing and other prohibited trade practices in the markets where they transact. Consistent with that, this article starts by discussing the basics before delving into the issues summarized above.

U.S. REGULATIONS AND EXCHANGE RULES ON SPOOFING

Spoofing is expressly prohibited by federal law and regulation, as well as by the rules of individual exchanges. Though the precise terms of the prohibitions vary slightly, they all prohibit the same types of behavior in principle.

Spoofing Prohibitions in Federal Law and Related Regulatory Guidance

The Commodity Futures Trading Commission ("CFTC") is the federal agency charged with regulating and policing the U.S. derivatives markets. Section 4c(a)(5)(C) of the U.S. Commodity Exchange Act ("CEA") prohibits a person or firm from engaging in any trading, practice, or conduct on a futures exchange that is "of the character of, or is commonly known to the trade as 'spoofing'," which is defined as "bidding or offering with the intent to cancel the bid or offer before execution."

The CFTC's published guidance provides some insight into its interpretation of section 4c(a)(5)(C) by supplying four non-exclusive examples of situations that constitute spoofing behavior.[1] The first example is submitting or cancelling bids or offers to overload the quotation system of a registered entity. The second is submitting or cancelling bids or offers to delay another person's execution of trades. The third is submitting or cancelling multiple bids or offers to create a false appearance of market depth. The final example is submitting or cancelling bids or offers with intent to create artificial price movements upwards or downwards. In these types of situations, or with other spoofing behavior, the CFTC may pursue regulatory enforcement action against the spoofer.

Even though spoofing activity is typically intended to benefit the person or firm entering the spoofing orders, the CFTC is *not* required to prove a real or intended benefit to the alleged spoofer to make out a successful enforcement claim. Nor does the CFTC have to prove a particular pattern of trading behavior. While regulators commonly seek to establish a trader's intent to cancel orders by showing a pattern of cancellations, a single instance of spoofing may be considered a violation under federal law. Accordingly, a successful spoofing action can be brought by the CFTC without any proof of intent to manipulate the price, or actual price manipulation.

The CFTC may impose monetary penalties and trading bans, in addition to other civil remedies, for violations of the spoofing laws it enforces. Furthermore, the U.S. Department of Justice may bring criminal charges for spoofing. Criminal spoofing convictions can result in imprisonment and fines.

Spoofing Prohibitions in Exchange Rules

In addition to the CEA prohibitions and the CFTC's interpretations of the prohibition on spoofing, some exchanges have introduced their own rules prohibiting spoofing. CME Group issued Rule 575, which provides, among other things, that "[n]o 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." The CME rule expressly applies to "open outcry trading as well as electronic trading," and it applies to "all market states, including the pre-opening period, the closing period, and all trading sessions." ICE U.S. Futures Trading Rule 4.02(*l*)(1)(a) includes prohibitions on, among other things, "entering an order or market message . . . with the intent to cancel the order before execution, or modify the order to avoid execution." It also prohibits "knowingly entering . . . bids or offers other than in good

[1] Antidisruptive Practices Authority, 78 Fed. Reg. 31,890, 31,896 (May 28, 2013).

faith for the purpose of executing *bona fide* transactions."

HOW REGULATORS DIFFERENTIATE BETWEEN SPOOFING AND LEGITIMATE TRADING ACTIVITIES

Regulators generally focus on a trader's intent to differentiate between illegal spoofing and legitimate trading. For example, a violation of the U.S. prohibition on spoofing in the CEA requires a market participant to act with some degree of intent, or scienter, beyond recklessness — a trader, at the time of order entry, must "*intend*[] to cancel the entire order before it is executed." If a trader enters an order and at the time of order entry does not have a legitimate, good-faith intent to execute at least part of the order, regulators may view that order as intentionally misleading and in violation of anti-spoofing rules.

In looking for direct evidence of illegal intent, regulators review a variety of sources, including e-mails, instant messages, text messages, and other electronic communications, as well as strategy code and development notes. Regulators also consider a number of indirect factors, including market exposure time, impact on the order book, and impact on market liquidity when trying to determine trader intent.

Market Exposure Time

An analysis to determine whether there was intent to execute an order at the time of entry requires the evaluation of many facts and circumstances, including the amount of time the order was exposed to the market. A pattern of cancelling orders almost immediately after entry may be indicative of non-*bona fide*, spoofing orders. Orders that rest on the book for a material time but are behind a significant number of orders with queue priority and are repeatedly cancelled before they can be executed against may also be indicative of spoofing orders.

When analyzing suspicious-exposure time behavior, it is not sufficient proof that the order was intended to be executed just because a market participant enters a large order, improves the book, and lets it rest for a material time. Depending on market conditions, for example, if the bid-ask spread is wide, simply tightening the spread may not necessarily subject the order to execution risk.

On the other hand, rapidly entering and cancelling multiple orders may not be indicative of spoofing. In volatile markets, a participant's order activity may simply reflect its attempt to adjust orders to reflect the multiple price changes. The key is that market exposure time — like all the factors listed here — is not a static factor, but relies heavily on the specifics of each market.

Impact on Order Book

All visible orders impact the market to some extent, which may necessarily cause other market participants to adjust their trading and order activity. This is a normal result of open and visible markets; however, traders seeking to engage in spoofing utilize an order's market impact to induce market participants into particular reactions.

In seeking to establish a market participant's intention, regulators regularly analyze the impact of their orders on the market. For example, entering an order that massively increases the visible resting liquidity on one side of the market or entering multiple smaller orders that incrementally tighten the spread can be indications — when paired with other factors or absent apparent economic rationale — of a market participant's intent to affect the market.

As with other factors outlined here, this analysis is a fact-specific review. An order with significant market impact is not on its own considered spoofing, but if such an order is cancelled quickly after beneficial executions on the opposite side of the market, or if such orders are consistently paired with opposite-side orders with much more minimal market impact, regulators may view this as spoofing activity.

Impact on Market Liquidity

Trading activity that occurs in illiquid markets or during low liquidity time periods may be subject to additional scrutiny. Regulators may consider it easier to manipulate a market when there is less liquidity, either because of the nature of the marketplace, or because the activity occurs during off-peak hours when fewer market participants are interacting.

Permissible Trading Activity

Cases filed have distinguished between illegal spoofing behavior and legitimate trading activity.[2] Legitimate trading activities include: accidental orders or cancellations; good-faith cancellations of unfilled or partially filled orders; and non-executable market communications, such as requests for quotes, indications

[2] *See, e.g.*, *United States v. Coscia*, 100 F. Supp. 3d 653, 658 (N.D. Ill. 2015).

of interest, and other authorized pre-trade communications.

In addition, guidance from U.S. exchanges has highlighted certain trading activities that will not be considered a violation of their anti-disruptive trading rules.[3] These include: "fat finger" errors, or orders entered unintentionally; orders layered throughout the book for the purpose of gaining queue priority; and modifying orders that were entered with an intent to trade due to a perceived change in circumstances.

Furthermore, there are many legitimate types of orders that are not intended to be executed or may be executed only under certain conditions. Though these types of orders are not unconditionally intended to be executed, they should not be considered spoofing. For example, "fill-or-kill" ("FOK") orders are entered to be immediately executed, and if they are *not* immediately executed, they will be cancelled. While FOK orders are *intended* to be cancelled if not filled, they are still entered with the intent to be executed. They are only cancelled *if* execution does not occur. A second example of a permissible trade is a "stop-loss" or "stop-limit" order. These are frequently used to limit losses, or lock in profits, on an existing position. The order is executed only if the specified price is hit. A final example of a permissible trade is an "all-or-none" ("AON") order. AON orders are orders where the specified number of contracts must be fully executed and cannot be partially filled. Unlike FOK orders, these orders remain in the order book until they are filled or cancelled. Because all of these types of orders are entered with an intent to trade, even if they may conditionally be cancelled, courts have recognized them as legitimate trading strategies.[4]

MOST COMMON TYPES OF SPOOFING

To date, cases brought by regulators concerning spoofing behavior or similar conduct have generally been characterized by market behavior that "creates an appearance of false market depth," behavior that "creates artificial price movements upwards or downwards," or sometimes both. Spoofing schemes can take varied forms, each of which uses a combination of spoofing orders and *bona fide* orders. Regulators continue to review emerging types of trading activity for possible violations. The following are several types of spoofing schemes identified in the cases.

Layering

Layering is a type of manipulative behavior that refers to placing both (1) multiple non-*bona fide* spoofing orders that are designed *not* to trade on one side of the order book and (2) one or more *bona fide* orders on the other side of the order book. The spoofer's hope is that the spoof orders may entice other market participants to place similarly priced orders on that side of the market, creating a false appearance of market depth, which will match against the spoofer's *bona fide* order. The spoof orders are generally larger than the *bona fide* order and are cancelled before they can be executed.

In one such case, the CFTC settled with a registrant for layering activity by its traders in the CME Treasury complex.[5] The strategy involved placing small *bona fide* orders on one side of the market, followed by large similarly priced spoof orders for 1,000 lots or more on the other side of the market. The large spoof orders were intended to create the impression of greater buying/selling interest than actually existed. The false market depth impression created by the spoof orders was intended to induce other market participants to fill the resting small *bona fide* order on the opposite side of the market. Once the *bona fide* order had been filled, the traders cancelled the resting spoof orders. The CFTC investigated trading activity over a period of 18 months and cited 2,500 potential spoof orders. The firm was fined $25 million and required to institute a new surveillance system designed to detect spoofing in addition to enhancing its training program.

Flipping

Flipping behavior consists of placing large, visible spoofing orders at or near the top of the market and then "flipping" the trading bias from one side of the market to the other by simultaneously canceling the spoofing orders and entering *bona fide* orders on the other side of the market at the same or a better price. By creating artificial price movements upwards or downwards, the spoof orders are intended to induce other market

[3] *See, e.g.*, Market Regulation Advisory Notice, Disruptive Practices Prohibited, Advisory No. CME Group RA 1405-5, at 4 (Aug. 29, 2014).

[4] *See, e.g.*, *CFTC v. Oystacher*, 203 F. Supp. 3d 934, 946 (N.D. Ill. 2016).

[5] *In re Citigroup Global Markets Inc.*, CFTC No. 17-06 (Jan. 19, 2017). The *Citigroup* case also offers many useful insights into the reach of the CFTC's jurisdiction. The CFTC was able to review trading activity in both *foreign and domestic exchanges* to build a single spoofing case. This demonstrates that investigations into spoofing may involve trading internationally and across exchanges.

participants to place orders on the same side of the market at similar price levels as the spoofing orders, which will after the "flip" match against the spoofer's *bona fide* order.

A variation on the execution of flipping behavior involves the use of exchange-provided "self-match prevention" technology to facilitate the simultaneous cancellation of the spoof orders and the entry of the *bona fide* orders. When this self-match prevention functionality is used, the entry of the *bona fide* order will immediately cause the cancellation of the resting spoof orders before they "self-match," which allows the *bona fide* order to execute against the orders of other market participants that had been enticed to join the market at similar price levels as the spoofing orders.

In one case of a flipping scheme, a trading firm allegedly annually placed spoof orders on one side of the market at or near the market price.[6] The spoof orders at least *doubled* the number of contracts offered or bid at those price levels or better. The spoof orders created the false impression of market depth and induced other market participants into placing orders on the same side of the market and at similar price levels as the spoof orders. Then, making use of self-match prevention functionality, the firm cancelled or attempted to cancel all of the spoof orders before they were executed and — virtually simultaneously — "flipped" their position in the order book from buy to sell (or vice versa) by placing at least one order on the other side of the market at the same or better price, hoping to match against the orders of market participants who had been induced to enter the market by the alleged spoof orders the firm had just canceled.

The firm's use of exchange-provided self-match prevention functionality not only prevented the *bona fide* flip orders from matching with the spoof orders, but it also allowed the firm to cancel the pending spoof orders and place *bona fide* orders on the other side of the market at the same or better prices before other market participants could assess and react to the disappearance of the false market depth the spoof orders had created. The firm was fined $2.5 million and subject to a three-year monitoring period as a result.

Vacuuming

Vacuuming behavior attempts to create a false impression of a sudden and significant decline in buying or selling interest, indicating an imminent price decrease or increase. One or more large, visible spoofing orders on the bid (offer) are entered to create or exacerbate a market imbalance. One or more smaller *bona fide* orders are entered on the same side of the market as the spoof orders. The spoof orders are then all cancelled simultaneously resulting in a significant amount of volume disappearing from the order book. This vacuuming behavior is intended to induce other market participants to react by aggressively executing against the remaining *bona fide* orders.

In one such case, the CFTC settled with a trader and his firm for spoofing activity in the CME E-mini market involving this "vacuuming" strategy.[7] The trader placed a significant number of spoof orders on one side of the market, which constituted a substantial percentage of the best bid or offer. The trader also placed *bona fide* orders on the same side of the market as the spoof orders. The trader then cancelled all the spoof orders nearly simultaneously, creating the false impression of a sudden and significant decline in the displayed buying or selling interest. This behavior was intended to induce other market participants to react to the removal of significant interest from one side of the market by moving the prices of their resting orders or entering new orders to lock in current prices before the market moved. This resulted in these orders executing against the remaining *bona fide* orders. The trader paid a $750,000 monetary penalty and was banned from trading futures for nine months. The firm paid a $1,750,000 monetary penalty as a result of the trader's conduct.

REGULATORS' INVESTIGATORY TOOLS AND PRACTICES

Regulators use a variety of software and other analytical tools to detect and prosecute spoofing activity. Regulators typically review detailed order and trade data to determine a pattern that evidences a trader's intent at the time of order entry; electronic communications to determine a trader's intent or the specific purpose of a trading strategy; and when algorithmic or automated trading is involved, the strategy's computer code and communications regarding the software development, all to determine the trader's intent. Some other circumstances regulators will evaluate are order splitters, iceberg orders, and order-to-trade ratio.

[6] *CFTC v. Oystacher*, No. 15-cv-09196 (N.D. Ill. Dec. 20, 2016).

[7] *In re Hard Eight Futures LLC*, CFTC No. 19-30 (Sept. 30, 2019); *In re Chernomzav*, CFTC No. 19-31 (Sept. 30, 2019).

Order Splitters

Automated order splitters are commonly and legitimately used to parse large orders into smaller pieces for various reasons, including to hide the actual order quantity or to prevent market disruption. The CFTC has indicated in certain enforcement actions, however, that the use of order splitters may also be an indication of manipulative intent.[8] For example, by using an order splitter that takes one large order and splits it into many smaller orders of random lot size, it may disguise this market participant's intent and lead other market participants to believe the imbalance in the book is coming from multiple market participants.

Iceberg Orders

As with order splitting, iceberg orders are commonly used for legitimate trading purposes — e.g., to limit the impact on or disruption to a market from a trader's orders while also obscuring the trading strategy from other market participants. The key concern with the use of iceberg orders in relation to spoofing activity is when they are used asymmetrically, i.e., only on one component of the trade. In actions brought by regulators that reference the use of iceberg orders, the *bona fide* orders were icebergs, displaying small order quantities to the marketplace, while the concurrent spoofing orders were not iceberg orders, and displayed significantly larger quantities. While there are legitimate trading reasons for using asymmetrical iceberg orders, such as risk/inventory management, this type of trading behavior is monitored closely for potential spoofing purposes.

In one case concerning iceberg orders, a manual, non-algorithmic trader placed one or more large spoofing orders or a series of layered spoofing orders (i.e., orders with gradually increasing or decreasing prices) totaling 60 or more lots on one side of the market. The trader then placed one or more smaller *bona fide* iceberg orders (1–10 lots) on the opposite side of the market. Once the iceberg orders were partially or completely filled, the trader cancelled the large or layered spoofing orders before they could be filled. The trader was fined $635,000 and permanently banned from trading on U.S.-regulated markets.[9]

Order-to-Trade Ratio/Cancellation Rate

Regulators may also compare: (1) the rate of execution and the rate of cancellation of *bona fide* orders versus (2) the rate of execution and the rate of cancellation of spoof orders looking for disparities. For example, in one case, a trader placed 24,814 large orders in a three-month period, and only 0.5% of them were executed. During the same period, he placed 6,782 small orders, and 52% of those orders were executed. The trader's order-to-trade ratio was 1600%, whereas the order-to-trade ratio for other exchange traders averaged between 91% and 264%. The trading data showed the trader's small orders were 100 times more likely to be filled than the large-volume orders. Most market participants consistently place orders of the same size with the same cancellation rate. Prosecutors utilized the discrepancy between large and small orders by this trader to obtain a criminal conviction.[10]

CONSIDERATIONS TO AVOID SPOOFING

Armed with this understanding of how regulators are evaluating trading activity for potentially manipulative behavior, it is important that market participants establish processes to monitor for this type of activity. Whether there is one trader, or dozens of traders, the goal is the same — to ensure that every order placed has a legitimate purpose. Regardless of whether a trade is manually entered or generated through an automated trading system, a trader should be able to explain the reasoning behind each order that is placed.

Traders

Spoofing regulations carry considerable punishments for individuals found to have violated them, including fines, revocation of trading privileges, and imprisonment.[11] Additionally, regulators may rely heavily on "circumstantial" evidence to prove their case, including statistics detailing a trader's cancellation rate, order-to-trade ratios, usage of various order types, and other data points.

To help protect against possible inferences of spoofing activity, the first and most important line of defense is trader education. Compliance training is key to ensure traders are knowledgeable regarding the types of activities regulators are pursuing under the various anti-manipulation regulations. Additionally, sophisticated surveillance software tailored to a firm's trading activity can help traders ensure their strategies

[8] *In re Tower Research Capital LLC*, CFTC No. 20-06 (Nov. 6, 2019).

[9] *In re Posen*, CFTC No. 17-20 (July 26, 2017).

[10] *United States v. Coscia*, No. 16-3017 (7th Cir. 2017), No. 14-cr-00551 (N.D. Ill. 2015).

[11] *See, e.g.*, *Coscia*, No. 14-cr-00551 (N.D. Ill. 2015) (sentencing the trader to three years' incarceration).

are not inadvertently engaged in behavior that could appear suspect.

Supervisors

Personnel who supervise traders face liability from spoofing activity. CFTC Rule 166.3 requires a firm registered with the CFTC to employ diligent supervision of its employees and activities.

A supervisory violation is an independent violation for which no underlying violation is necessary. Supervisory violations are demonstrated by showing either that: (1) the registrant's supervisory system was generally inadequate or (2) the registrant failed to perform its supervisory duties diligently. Evidence of violations that should have been detected by a diligent system of supervision — either because of the nature of the violations or because the violations have occurred repeatedly — is probative of a failure to supervise.

Firms

In recent years, the CFTC has been using other regulations to charge firms under a theory that the firm is liable for the acts of its agents: the traders. The applicable statutes provide that the act, omission, or failure of any official, agent, or other person acting for a firm within the scope of his employment or office shall be deemed the act, omission, or failure of such firm.[12] Pursuant to these regulations, strict liability is essentially imposed on principals for the actions of their agents.

Furthermore, the CFTC has started to charge firms with violations based on failures to file suspicious activity reports ("SARs"), pursuant to the obligations of certain firms under the Bank Secrecy Act. The CFTC enforces a regulation that, in relevant part, requires every futures commission merchant ("FCM") to comply with the applicable provisions of the Bank Secrecy Act.[13] As a result, FCMs must file a report of any suspicious transaction if the transaction: (1) is conducted (or attempted) through the FCM; (2) involves funds of at least $5,000; and (3) the FCM knows, suspects, or has reason to suspect that the transaction — among other things — (i) involves funds derived from illegal activity or is intended or conducted to hide or disguise funds or assets derived from illegal activity to violate or evade any federal law; (ii) is designed, whether through structuring or other means, to evade any requirements under the Bank Secrecy Act; (iii) has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the FCM knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction; or (iv) involves use of the FCM to facilitate criminal activity.

Thus, whether a firm is large or small, or whether the trading is automated or manual, there are some standard review practices firms are required to implement. In the case of a small firm, it may be more difficult to separate the trading function from the compliance and risk management functions. Nevertheless, the size of a firm does not impact the importance of conducting trading reviews and documenting such reviews. If the trading and compliance functions cannot be separated, then thorough documentation summarizing the review should be carefully maintained. Smaller firms or sole proprietors can look to outside counsel and independent compliance consultants for aid in their analysis.

All firms should consider these practices for internal reviews. Trading should be monitored across products, markets, and jurisdictions. Traders should be evaluated individually, as a part of a team or trading desk, and as a part of the overall firm. Be aware that even one order can be considered spoofing if it was intended to be cancelled before executed and especially if it impacts the market. It is important to remember when looking for evidence of spoofing that the *bona fide* order may be in a product other than the spoofed contract. It is also extremely important to consider the market and product that is being traded, as different factors dictate what is large, what is normal, and what is likely to have an impact on the product or related product's order book. Consider whether the orders are disproportionately large given either the market or the trading strategy. Finally, it is essential to consider the market and products traded, as requirements around supervision and reporting vary by jurisdiction. Since all jurisdictions have prohibitions on spoofing and like conduct, monitoring and diligent supervision across markets can be critically important.

In addition, specifically for larger firms, or where trading is more complex, the following should be considered when developing surveillance and supervisory processes for manipulative trading behaviors such as spoofing. First, a formal training process is essential. Second, a surveillance software system may be the only way to adequately supervise complex or volume intensive activity. If a surveillance system is used, the implementation and monitoring of the system should be customized to reflect the type of trading conducted by the firm. If the system generates an alert

[12] CEA § 2(a)(1)(B).

[13] 31 C.F.R. § 1026.320(a)(2).

or identifies spoofing behavior, the surveillance reporting needs to follow a defined review process. Legal or compliance advisers should be consulted on how to approach documentation and resolution of potential violations. Third, if surveillance is not conducted within the compliance department but within another group — for example, with a market surveillance group in the risk department — then the two groups need to regularly communicate and collaborate with each other and document their coordinated efforts. Fourth, if there is overlap in surveillance duties, individual responsibilities and lines of reporting must be clearly defined. Fifth, if concerning patterns are detected — by a trader, trading desk, strategy, product, etc., — appropriate personnel need to review these patterns and investigate any potential concerns. Sixth, the firm should consider and discuss with their legal advisors whether a SAR or other self-reporting of any potential misconduct to the appropriate regulator is required.

CONCLUSION

With the increasing attention to manipulative conduct in financial markets over the years, the CFTC's regulatory interest in investigating and prosecuting spoofing behavior will continue expanding. In this environment, it is paramount that traders, supervisors, and firms of all sizes keep themselves apprised of developments in manipulative spoofing behavior schemes and take proactive measures to detect and attempt to prevent any such activity within its sphere of regulatory responsibility.

Furthermore, if a firm receives requests for information or documents from any regulator, it should quickly address the requests and internally investigate its own exposure to enforcement actions and penalties. When faced with answering for potential spoofing behavior, firms should engage legal counsel with experience in such internal investigations and with advocating before the CFTC Enforcement Division and other regulatory bodies. Such experience may be paramount in achieving a favorable negotiated outcome and avoiding harsh regulatory, civil, or even criminal penalties.

Finally, if a negotiated resolution is not possible or appropriate, it is important to have counsel that understands the highly complex legal backdrop of prohibited spoofing behaviors to successfully litigate and zealously defend against CFTC enforcement actions. ■