NSCP NATIONAL SOCIETY OF COMPLIANCE PROFESSIONALS Currents May 2018

Spoofing, Surveillance, & Supervision

By James G. Lundy, Nicholas A.J. Wendland and Jay A. Biondo

The U.S. Commodity Futures Trading Commission ("CFTC") and futures self-regulatory organizations continue to aggressively pursue "spoofing" cases against traders. When evidence of criminal willful intent exists, they refer certain matters to the Department of Justice ("DOJ") for criminal prosecution. The CFTC settled its first spoofing case in late December 2016.[1] In early November that same year, the DOJ obtained its first criminal conviction for spoofing.[2] Since that time, the CFTC has expanded its efforts in this area to target firms for failing to supervise traders accused of spoofing activity. In this article we analyze the messages sent by the CFTC with its regulation by enforcement efforts, and the interplay of spoofing, surveillance, and supervision.

A Review of the Regulations and the CFTC's Expanding Efforts

We begin with a summary of applicable spoofing and supervisory laws and then analyze the pertinent CFTC enforcement cases. Section 4c(a)(5)(C) of the Commodity Exchange Act ("CEA") makes it unlawful for "[a]ny person to engage in any trading, practice, or conduct on or subject to the rules of a 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)."

The CFTC's "Failure to Supervise" law is Regulation 166.3 and it requires a firm to employ diligent supervision of its employees and activities:

Each Commission registrant, except an associated person who has no supervisory duties, must diligently supervise the handling by its partners, officers, employees and agents (or persons occupying a similar status or performing a similar function) of all commodity interest accounts carried, operated, advised or introduced by the registrant and all other activities of its partners, officers, employees and agents (or persons occupying a similar status or performing a similar function) relating to its business as a Commission registrant.

On January 19, 2017, the CFTC filed its first settled failure to supervise case against a registered firm for supervision failures related to spoofing and ordered the firm to pay a $25 million monetary penalty.

Case law has interpreted this duty of diligence broadly and an underlying violation is not required.[3] A violation under Regulation 166.3 is an independent violation for which no underlying violation is necessary.[4] A violation of Regulation 166.3 is 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.[5] Evidence of violations that "should be 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.[6]

About the Authors
James G. Lundy is a Partner with Drinker Biddle & Readh LLP. He can be reached at James.Lundy@dbr.com.
Nicholas A.J. Wendland is Counsel with Drinker Biddle & Reath LLP. He can be reached at Nicholas.Wendland@dbr.com.
Jay A. Biondo is Manager, Trading Technologies. He can be reached at jay.biondo@tradingtechnologies.com.

1. *See CFTC v. Oystacher and 3 Red trading LLC*, Case No. 15-cv-09196 (N.D. Ill.).
2. On August 7, 2017, the U.S. Court of Appeals for the Seventh Circuit affirmed this conviction. *See United States v. Coscia*, No. 16-3017, 2017 WL 3381433 at *1. The U.S. Supreme Court denied defendant's petition for review on May 14, 2018.
3. The U.S. Securities and Exchange Commission requires an underlying substantive violation in order to establish a failure to supervise charge, but the CFTC has no such prerequisite. See Section 15(b)(4)(E) of the Securities Exchange Act of 1934.
4. *See In re Collins*, [1996-1998 Transfer Binder] Comm. Fut. L. Rep. (CCH) ii 27,194 at 45,744 (CFTC Dec. 10, 1997).
5. *See In re Forex Capital Markets LLC*, [2012-2013 Transfer Binder] Comm. Fut. L. Rep. (CCH) ii 32,658, at 73,166 (Oct. 3, 2011) (*citing In re Murlas Commodities*, [1994-1996 Transfer Binder] Comm. Fut. L Rep. (CCH) ii 26,485 at 43,161 (CFTC Sept. I, 1995)); *see also In re GNP Commodities, Inc.*, [1990-1992 Transfer Binder] Comm. Fut. L. Rep. (CCH) ii 25,360 at 39,219 (CFTC Aug. 11, 1992) (providing that, even if an adequate supervisory system is in place, Regulation 166.3 can still be violated if the supervisory system is not diligently administered); *Samson Refining Co. v. Drexel Burnham Lambert, Inc.*, [1987-1990 Transfer Binder] Comm. Fut. L. Rep. (CCH) ii 24,596 at 36,566 (CFTC Feb. 16, 1990) (noting that, under Regulation 166.3, an FCM has a "duty to develop procedures for the detection and deterrence of possible wrongdoing by its agents") (internal quotation omitted).
6. *See In re Paragon Futures Assoc.*, [1990¬ 1992 Transfer Binder] Comm. Fut. L. Rep. (CCH) ii 25,266 at 38,850 (Apr. 1, 1992); *see CFTC v. Sidoti*, 178 F.3d 1132, 113 7 (11th Cir. 1999) (holding defendant liable for failure to supervise because he "knew of specific instances of misconduct, yet failed to take reasonable steps to correct the problems").

On January 19, 2017, the CFTC filed its first settled failure to supervise case against a registered firm for supervision failures related to spoofing and ordered the firm to pay a $25 million civil monetary penalty.[7] The order instituting the proceeding ("OIP") found that:

Between July 16, 2011 and December 31, 2012, the firm by and through five of its traders engaged in spoofing in U.S. Treasury futures markets more than 2,500 times and that the firm failed to diligently supervise said traders. Specifically, the CFTC found that the firm's supervisory system was in inadequate in two respects. First, it did not sufficiently train the traders about spoofing. Second, it did not have in place systems and controls designed to prevent and detect spoofing. The OIP listed a series of required undertakings for the firm as part of the resolution with the CFTC. Two undertakings specifically related to the firm's training and surveillance inadequacies:

> **Procedures and Controls to Detect Spoofing Activity:** [Respondent] shall maintain systems and controls reasonably designed to detect spoofing activity by its traders, such as the systems and controls Citigroup developed and implemented in response to the Traders' spoofing activity. These systems and controls shall, at a minimum, be designed to detect and generate a report regarding patterns of trading that might constitute spoofing activity (e.g., the placement and rapid cancellation of large-lot futures orders). Citigroup personnel shall promptly review such reports and follow up as necessary to determine whether spoofing activity has occurred.
>
> **Training:** [Respondent] shall provide annual training addressing the legal requirements of the Act with regard to spoofing, to be given to Citigroup employees who submit any orders on U.S. futures markets and their supervisors.[8]

In a bizarre twist – the CFTC charged the firm and fined it $25 million – but allowed three of the traders who engaged in spoofing to walk away with non-prosecution agreements.

Notably, on June 29, 2017, the CFTC announced and touted its first "non-prosecution agreements" with three former traders from this firm.[9] The CFTC's release emphasized the traders "material assistance provided to the CFTC's investigation." In a bizarre twist – the CFTC charged the firm and fined it $25 million – but allowed three of the traders who engaged in spoofing to walk away with non-prosecution agreements. The message sent appears to perhaps incentivize traders being investigated for spoofing to point at their firms for failing to train and supervise them regarding spoofing.[10]

On September 29, 2017, the CFTC charged another firm with a stand-alone failure to supervise case involving spoofing in crude oil futures.[11] This OIP found that the trader was given inadequate training, direction, and supervision, which resulted in him repeatedly engaging in spoofing (i.e., bidding or offering with the intent to cancel his bid or offer before execution).[12] Notably, the firm's compliance department detected the misconduct in August 2014; however, the firm failed to satisfy its obligation to supervise an appropriate investigation into the trading misconduct.

On January 29, 2018, the CFTC and the DOJ announced their most significant and aggressive actions against spoofers and the firms employing them for failing to supervise. The CFTC filed settled actions against three firms for supervisory violations, amongst other charges, and the CFTC charged six individuals with alleged commodities fraud and spoofing schemes.[13] Each of the firms settled to supervisory violations and as part of the CFTC's remedies they further agreed to: continue to maintain surveillance systems to detect spoofing; ensure personnel "promptly" review reports generated by such systems and follow up as necessary if potential manipulative trading is identified; and maintain training programs regarding spoofing, manipulation, and attempted manipulation. For one of the matters, the OIP specifically found that while the firm had a surveillance system and policies and procedures to detect and deter spoofing, the firm "did not follow up on the majority of potential instances of misconduct identified by its electronic surveillance system. [Respondent] also failed to perform its supervisory duties diligently because the surveillance systems alerts put it on notice of potential misconduct yet it failed to take adequate steps to address or remedy the issues."[14] As a result, the OIP included similar undertakings for all three firms to address the supervisory failures:

7. *See In the Matter of Citigroup Global Markets, Inc.*, CFTC Docket No: 17-06 (Jan. 19, 2017).
8. *See Id.* At 7-8.
9. *See* CFTC Release Number 7581-17, available at https://www.cftc.gov/PressRoom/PressReleases/pr7581-17.
10. On January 19, 2017, the CFTC issued "New Advisories on Cooperation." *See* CFTC Release Number 7518-17 (Jan. 19, 2017).
11. Earlier that month, on September 1, 2017, CME Group issued two Notices of Disciplinary Action against firms for failing to supervise traders engaging in spoofing. *See* NYMEX 16-0434-BC-1, *available at* http://www.cmegroup.com/notices/disciplinary/2017/08/NYMEX-16-0434-BC-1-JAYPEE-SINGAPORE-PTE-LTD.html#pageNumber=1. *See also* COMEX 15-0261-BC-1, available at http://www.cmegroup.com/notices/disciplinary/2017/08/COMEX-15-0261-BC-1-SKEET-COMMODITIES-DMCC.html#pageNumber=1.
12. *See In the Matter of Logista Advisors LLC*, CFTC Docket No. 17-29 (Sept. 29, 2017).
13. *See* CFTC Release Number 7681-18, available at https://www.cftc.gov/PressRoom/PressReleases/pr7681-18. In the parallel criminal actions, the DOJ announced criminal charges against eight individuals (the six charged by the CFTC plus two others).
14. *See In the Matter of Deutsche Bank AG and Deutsche Bank Securities, Inc.*, CFTC Docket No. 18-06 at 7 (Jan. 29, 2018).

> **Procedures and Controls to Detect Spoofing Activity**: Respondents shall maintain systems and controls reasonably designed to detect spoofing activity by its traders, such as the systems and controls Respondents developed and implemented in response to the Traders' spoofing activity. These systems and controls shall, at a minimum, be designed to detect and generate a report regarding patterns of trading that might constitute spoofing activity. Respondents' personnel shall promptly review such reports and follow up as necessary to determine whether spoofing activity has occurred.
>
> **Training**: Respondents shall maintain their training program that provides training, at least annually, addressing the legal requirements of the Act with regard to spoofing, manipulation and attempted manipulation, to be given to all employees trading on behalf of Respondents or other affiliated entities who submit any orders on futures markets, and their supervisors.[15]

More recently, on May 15, 2018, and confirming the messages sent by the above cases, CFTC Commissioner Rostin Benham admonished:

As our developing spoofing case law demonstrates, this duty to supervise includes ensuring that employees receive sufficient training and that their activities are monitored through adequate systems and controls to detect spoofing.[16]

The CFTC sends a loud and clear message that firms need to have a robust surveillance and supervisory systems and processes.

The CFTC's aggressive focus on firms and their supervision of traders – and their activities regarding spoofing and manipulative trading – sends a loud and clear message that firms need to have robust surveillance and supervisory systems and processes to avoid suffering the same fate as the firms discussed above.

21st Century Surveillance

The CFTC's enforcement efforts make it clear that in order to satisfy their duty of diligent supervision firms are required to maintain systems and controls reasonably designed to detect spoofing activity by their traders, and these systems and controls shall, at a minimum, be designed to detect and generate a report regarding patterns of trading that might constitute spoofing activity. As a result, identifying compliance surveillance systems that promote the rapid and accurate detection of spoofing activity has become of paramount importance to firms operating in the commodities markets that want to avoid suffering large monetary fines and reputational damage.

There are generally two types of trade surveillance that firms can employ in order to detect and prevent spoofing activity. The first type is referred to as pre-trade surveillance. Pre-trade surveillance programs have traditionally been used to validate trade instructions, ensure trading thresholds are not breached, and prevent trades being conducted on restricted instruments.

The second type of trade surveillance available to firms is referred to as post-trade surveillance. Post-trade surveillance systems historically have involved rule based parameter models that are selected by compliance officers to generate "alerts" that may (after further investigation) reveal an instance of potential spoofing activity. For example, a rule based parameter model may be centered around large cancels that occur within a certain period of time after small fills are received on orders on the opposite side of the market.

Firms that are looking to implement a surveillance system to detect and prevent spoofing activity will likely encounter significant challenges with both categories. First, pre-trade surveillance has not historically been used for the detection of manipulative activity like spoofing. Effective spoofing surveillance typically requires an analysis of a pattern of activity that developed over time in order to attempt to determine a trader's intent. Trying to prevent such a trading pattern from emerging in the first place with hard-coded trading thresholds or restricted instruments lists can be extraordinarily difficult to accomplish. Pre-trade surveillance and protections, rather, are more commonly used in relation to risk controls, capital sufficiency controls, and other related matters.

Post-trade surveillance programs typically have limitations as well. For example, the variety of spoofing patterns that are currently drawing regulatory attention can create major challenges for compliance departments who are tasked with choosing the parameter thresholds for dozens of surveillance metrics across multiple exchanges and numerous products. For example, what constitutes a "large" order? Or, what constitutes a "small" fill? In what time frame do these events have to occur? Parameters for these reports must be calibrated correctly and reviewed regularly to prevent the system from generating reports with no alerts, or reports with so many alerts that the output is rendered meaningless.

15. *See Id*. At 14.
16. Remarks of Commissioner Rostin Behnam before Energy Risk USA, Houston, Texas: *Delivering a Message on Relationship Patterns* (May 15, 2018), available at https://www.cftc.gov/PressRoom/SpeechesTestimony/opabehnam6.

Fortunately, with advancing technologies, new surveillance tools have emerged that appear to be a positive development for firms in the commodities markets. These new surveillance systems leverage artificial intelligence, machine learning, and behavioral analytics to help compliance professionals more accurately and rapidly detect patterns of trading that might constitute spoofing activity. In turn, these advanced surveillance systems should allow compliance professionals to more efficiently and thoroughly conduct follow-up investigations into certain activity, and more broadly help regulators fulfill their mandate of ensuring that markets are fair and efficient for all participants as well.

Supervision

A surveillance system needs to tie into a firm's overall supervisory system. Consistent with this principle, firms need to have written policies, procedures, and processes regarding how they detect and deter disruptive trading and these policies, procedures, and processes need to be periodically assessed. Specifically, the surveillance system needs to be tailored to a firm's particular trading activities, and it needs to be regularly tested, revised, and updated. In the January 29, 2018 press release announcing the enforcement actions against the three banks and eight individuals discussed above, the CFTC specifically stated that technological enhancements have created new opportunities in today's markets, for both legitimate trading and bad actors.[17] Thus, a surveillance system designed for reviewing manual trading may not be deemed sufficient by regulators when used to review algorithmic trading. In other words, it's difficult to catch a car thief on horseback.

A firm's supervisory efforts regarding the implementation and monitoring of its surveillance system needs to be documented. Also, the surveillance reporting needs to follow a diligent process and also be well documented. When the system generates alerts, appropriate inquiries need to be made tailored to the nature of the alert and documented. If patterns are detected – by trader, trading desk, strategy, product, etc. – appropriate supervisory individuals should track these patterns for trends.

If surveillance staff is not housed within the compliance department, but in another part of the firm such as the risk department with a market surveillance group, then such a group needs to closely and regularly communicate and collaborate with the compliance department and document these coordinated efforts. In instances where there is overlap in surveillance duties, individual responsibility must be made clear to each individual, with clearly defined lines of reporting as well.

Training, training, training – in addition to a robust surveillance system and strong supervisory policies, procedures, and processes – firms absolutely must regularly and formally train traders. This training cannot be "check the box" training. The programs need to be strong and periodically assessed and updated as this area of the industry evolves. All of the traders should also certify that they received copies of the applicable policies and procedures. The formal training needs to have a sign in and traders "blowing this off" cannot be tolerated and must be met with appropriate discipline supported by senior management.

In January 2018, the CFTC charged a software development company and its president with aiding and abetting spoofing and manipulative trading activity..

For some firms and organizations, training only traders may not be enough. In January 2018, the CFTC charged a software development company and its president with aiding and abetting spoofing and manipulative trading activity.[18] According the CFTC, this software company worked closely with a trader to meet the trader's desired manipulative specifications. The CFTC further alleged that the software company and its president knew that the trader would use the manipulative software applications to engage in spoofing and inject false information into the market. In its release, the CFTC specifically admonished that "the CFTC will work vigorously to hold accountable not only the individuals who engage in the spoofing, but also those who produce and sell the tools designed to spoof."[19] Thus, firms developing and implementing their own software need to extend the supervision requirements to developers of such software.

Lastly, a firm's escalation policies, procedures, practices, and training need to instruct personnel on how to deal with and escalate internally and externally (if needed and required), red flags of possible spoofing and other types of manipulative trading. Written policies and procedures and strong surveillance tools are useless if they are not utilized or reasonably and appropriately followed. In the CFTC's first failure to supervise case for spoofing discussed above, the CFTC specifically found that the supervisor was alerted to the spoofing activity, yet the supervisor failed

17. *See supra* note 13.
18. *CFTC v. Jitesh Thakkar and Edge Financial Technologies, Inc.*, Case No. 18-cv-00619 (N.D. Ill.).
19. *See* CFTC Release Number 7689-18, *available at* https://www.cftc.gov/PressRoom/PressReleases/pr7689-18.

to comply with the firm's existing policies and procedures because he did not alert compliance or escalate to senior management.[20]

Takeaways / Strategic Recommendations

In considering the CFTC's aggressive efforts when it comes to spoofing, surveillance, and supervision – several strategic lessons and recommendations serve as takeaways.

First, the CFTC will continue to investigate firms for failing to supervise traders being investigated for spoofing and manipulative trading – this is now standard CFTC enforcement practice.

Second, firms need to have in place a sophisticated and robust surveillance system appropriately tailored to the firm's and traders' trading activities.

Finally – for spoofing, surveillance, and supervision – appropriate and strategic documentation is key.

Third, the firm's supervision and compliance processes, policies, and procedures must include: appropriate and periodic training; documented processes for managing the surveillance system and alerts generated; and appropriate escalation procedures for alerts that result in possible violative trading activity.

Finally – for spoofing, surveillance, and supervision – appropriate and strategic documentation is key. The work related to the surveillance system implementation, alerts generated, and any corresponding investigative efforts needs to be logged and documented. To avoid documentation regarding investigative efforts being discoverable by third parties, we recommend that firms consult with in-house counsel (or outside counsel) at an appropriate point in the investigative effort so that the attorney-client privilege and attorney work product doctrine can be applied. Bear in mind that most courts do not extend these privileges to lawyers serving as compliance officers, because they view compliance as an operational function of the business. If the circumstances arise that the firm may need to strategically waive these privileges and share records with the CFTC (or otherwise), then it is the firm's right to waive these privileges should they deem it strategically appropriate to do so.

Conclusion

The CFTC's enforcement efforts regarding spoofing and supervision are only a few years old. But these areas have quickly become the primary enforcement priorities of the CFTC. As discussed above, the CFTC quickly accelerated its programmatic efforts from focusing on just the trader's activities – to the firm's supervision of these activities. Armed with a thorough understanding of the guidance discussed above and these takeaways, firms can apply appropriate strategies to attempt to extricate themselves from a spoofing supervisory investigation as quickly as possible or ideally avoid being subjected to any supervisory exposure in the first place.

20. *See* supra 7.