REPORT

Futures & Derivatives Law

The Journal on the Law of Investment & Risk Management Products

January 2019 ▪ Volume 39 ▪ Issue 1

TO SPOOF OR NOT TO SPOOF? THE DOJ ANSWERS THE QUESTION

By William J. Stellmach, Sohair Aguirre, and Paul J. Pantano, Jr.

William Stellmach is a partner in Willkie Farr & Gallagher's Litigation Department and Co-Chair of the White Collar Defense Practice Group; Sohair Aguirre is an associate and Paul Pantano is a partner in the firm's CFTC and FERC Enforcement Defense Practice.

DOJ'S INCREASED FOCUS ON SPOOFING

Federal prosecutors are focusing increased attention on alleged violations of the Commodity Exchange Act's prohibition against spoofing. On November 6, 2018, for example, the U.S. Department of Justice announced that it had secured a guilty plea from John Edmonds, a former JPMorgan metals trader, for engaging in spoofing for the purpose of manipulating precious metals futures prices. According to the DOJ press release:

> For years, John Edmonds engaged in a sophisticated scheme to manipulate the market for precious metals futures contracts for his own gain *by placing orders that were never intended to be executed.* . . . The Criminal Division is committed to prosecuting those who undermine the investing public's trust in the integrity of our commodities markets through spoofing or any other illegal conduct. . . . In pleading guilty, Edmonds admitted that he learned this deceptive trading strategy from more senior traders at the Bank, and *he personally deployed this strategy hundreds of times with the knowledge and consent of his immediate supervisors.*
>
> This case is the result of an *ongoing investigation* by the FBI's New York Field Office.[1]

The references to the facts that Mr. Edmonds' guilty plea arose from "an ongoing investigation" and that he engaged in spoofing "with the knowledge and consent of his immediate supervisors" suggest that more spoofing-related indictments are likely to follow.

The Edmonds guilty plea is just the most recent public indication of the DOJ's allocation of significant resources to pursuing alleged spoofing violations. In the Fraud Section Year in Review 2018, the DOJ touted the Securities & Fraud Section Unit's initiative to investigate and prosecute spoofing in commodity futures markets. According to the DOJ, as part of this initiative, "the Fraud Section has charged over a dozen individuals with spoofing-related crimes, and has obtained convictions of several traders affiliated with both large financial institutions and medium-sized proprietary trading companies."[2]

The Commodity Futures Trading Commission and the futures exchanges also have substantially increased the number of enforcement actions that they are filing

against traders for spoofing. The CFTC's Enforcement Division has set up a Spoofing Task Force "to preserve the integrity of [the listed derivatives] markets."[3] According to the CFTC's Enforcement Director:

> The advent of the electronic order book brought with it significant benefits to our markets—it increased information available, reduced friction in trading, and significantly enhanced the price discovery process. But at the same time, this technological development has presented new opportunities for bad actors. Just as the electronic order book increases information available to traders, it creates the possibility that false information injected into the order book could trick them into trading to benefit a bad actor.[4]

Mr. McDonald has described spoofing as "a particularly pernicious example of bad actors seeking to manipulate the market through the abuse of technology."[5] The harms attributed to spoofing by Mr. McDonald include hindering competition, undermining market integrity, and driving traders away from the markets, which reduces the liquidity that markets need to flourish.[6]

During the fiscal year ending September 30, 2018, the CFTC initiated 15 enforcement actions for alleged spoofing violations.[7] So far, the CME has brought spoofing charges against 44 market participants in 2018.[8] During the same period, ICE has filed seven spoofing charges.[9]

As we discuss below, the increased focus on spoofing by the criminal and civil enforcement authorities is being driven by a number of factors. Electronic trading and the wide-spread use of sophisticated algorithms appear to have increased the appetite of traders to test their ability to influence the trading activity of other market participants and thereby impact futures contract prices. At the same time, the addition to the CEA and exchange rules of spoofing as a type of disruptive trading practice has provided criminal, civil, and exchange enforcement authorities with powerful new tools for prosecuting spoofing. Moreover, even though spoofing has been expressly prohibited by the CEA for eight years and exchange rules for approximately four years, a number of market participants still seem to be unaware that it is illegal.

CEA PROHIBITION AGAINST SPOOFING

Section 747 of the Dodd-Frank Wall Street Reform and Consumer Protection Act amended the CEA to expressly prohibit certain disruptive trading practices, including spoofing.[10] Section 4c(a)(5)(C) of the CEA makes it "unlawful for any person to engage in any trading, practice, or conduct on or subject the rules of a registered entity that . . . [i]s, 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)."[11]

In its interpretive guidance, the CFTC has explained that spoofing includes:

- Submitting or cancelling bids or offers to overload the quotations system of a registered entity;
- Submitting or cancelling bids or offers to delay another person's execution of trades;
- Submitting or cancelling multiple bids or offers to create an appearance of false market depth; and
- Submitting or canceling bids or offers with intent to create artificial price movements upwards or downwards.[12]

The CFTC also noted that a spoofing violation requires that the "market participant act with some degree of intent, or scienter, beyond recklessness."[13]

Following the Dodd-Frank Act amendments to the CEA, both the CME Group Inc. and ICE Futures U.S. adopted rules prohibiting disruptive trading practices, including a prohibition against spoofing. CME Rule 575.A provides 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 avoid execution."[14] ICE Rule 4.02(l)(A) states that "[i]t is a violation to enter an order or market message, or cause an order or market message to be entered, *with the intent to cancel* the order before execution, or modify the order to avoid execution."[15] Like the CEA, a spoofing violation under the CME and ICE rules requires a showing of intent, at the time of placing an order, to cancel it before it is hit or lifted by another market participant.

Section 9(a)(2) of the CEA makes it a felony, punishable by a fine of not more than $1,000,000 or imprisonment of not more than 10 years, for any person "knowingly to violate" the CEA spoofing prohibition.[16] For criminal spoofing violations, DOJ has been charging commodities fraud under 18 U.S.C.A. 1348, which requires proof that the defendant: (1) in connection with the purchase or sale of any commodity futures contract or futures option contract; (2) knowingly engaged in a scheme or artifice to defraud; and (3) through false or fraudulent pretenses, representations, or promises obtained money or property. While the burden of proof in a criminal spoofing case is beyond a reasonable double, in a CFTC enforcement case, the CFTC must prove its claim by a preponderance of the evidence.

THE DOJ'S TRACK RECORD IN SPOOFING CASES

This DOJ's more aggressive approach to charging criminal cases has resulted in a marked increase in the number of spoofing prosecutions and a dramatic shift in the evidentiary threshold behind the charges. The numbers speak for themselves, with a pipeline going forward provided by the CFTC's Spoofing Task Force.[17] A noteworthy development lies in the quantum of evidence that DOJ now finds sufficient to charge a criminal case. Previously, DOJ had brought criminal spoofing cases backed with direct evidence of a defendant's express intent to spoof by canceling orders, such as testimony from the software programmer designing the trading algorithm.[18] By contrast, this past year has seen DOJ charge two cases notable for relying far more heavily on circumstantial evidence. One of those cases, *U.S. v. Flotron*, involved a primarily manual trader—the first criminal spoofing case of its kind—and, while it resulted in acquittal at trial, it nevertheless signaled a more aggressive posture from DOJ.[19] Similarly, the other case, *U.S. v. Zhao*, appears to rely entirely on circumstantial trading patterns, without any direct evidence of intent from emails or other witnesses.[20]

Following the acquittal in Flotron, it remains to be seen whether DOJ will reconsider its embrace of what Flotron's defense lawyer lambasted as "prosecution by statistics."[21] Notably, the defendant in Zhao, who had been arrested in Australia on the U.S. charges, waived extradition following Flotron's acquittal, and, following Zhao's initial appearance in this country, DOJ sought an extension of time within which to indict him.[22] Whether DOJ is negotiating a disposition with defense counsel or buying time to bolster its proof remains to be seen.

Notwithstanding the setback in the Flotron trial, DOJ's spoofing crackdown has already yielded multiple guilty pleas in several cases.[23] In light of that successful prosecutorial track record, DOJ's appetite for spoofing cases likely will remain strong, even if it reverts to the more successful prosecution blueprint from *Coscia*. Going forward, anyone dealing with a CFTC or exchange spoofing investigation should be sensitive to the heightened risk of a parallel criminal investigation.

THE IMPACT OF CRIMINAL CASES ON CFTC AND EXCHANGE INVESTIGATIONS AND PROCEEDINGS

Persons subject to the jurisdiction of designated contract markets have an affirmative obligation to cooperate with exchange investigations.[24] Failure to respond to questions during an exchange investigation is a general offense under exchange disciplinary rules.[25] The CFTC, like the exchanges, expects witnesses, especially those who work for registrants, to cooperate with its investigations. If a trader asserts their Fifth Amendment right against self-incrimination in a CFTC investigation, a court can draw an adverse inference against the trader. The adverse inference, when combined with other evidence, may be sufficient to prove a violation by a preponderance of the evidence.[26]

Because spoofing is both a criminal and civil offense, defense lawyers have a hard choice to make when deciding whether to advise clients to exercise their right against self-incrimination in exchange and CFTC investigations of potential spoofing activity. In the criminal case against Coscia, the DOJ used Coscia's investigative testimony taken by the CFTC against him.[27] The exchanges, at least, are starting to make some accommodations in light of the potential criminal exposure that traders face in spoofing investigations. Although they still treat a failure to respond to their questions as a rule violation, they may treat a parallel criminal investigation as a mitigating factor when assessing a penalty for failing to cooperate with an exchange investigation.

PROTECTING THE FIRM AGAINST CRIMINAL AND CIVIL SPOOFING LIABILITY

There are a number of steps that firms should consider taking to minimize their exposure to criminal or civil spoofing liability. First, firms should have policies and procedures that prohibit all forms of disruptive trading, including spoofing. The policies and procedures should address trading practices and conduct on any CFTC-registered entity, including the use of electronic trading systems, algorithms, and order routing systems. The policies and procedures should provide traders with practical guidance about what types of trading are permitted and what types are prohibited.

Firms should reinforce their policies and procedures by providing targeted training on the spoofing prohibition. The training should cover the elements of a violation and examples of prohibited trading taken from criminal, CFTC, and exchange cases. Exchange market risk advisories include many examples of prohibited spoofing activity that can be incorporated into a firm's training program.[28] The training should be interactive so traders will retain important guidance. In addition, the training should help

traders identify situations that should prompt them to ask questions of compliance and legal personnel before executing a particular trading strategy.

Firms should put in place active programs for monitoring trading for potential spoofing activity. An effective spoofing surveillance program should focus on and analyze a number of key factors, including: trader/desk/firm order messaging; new orders, modifications and cancellations; market dynamics; the depth and balance of the firm's and the exchange's order book; the characteristics of the particular market; the matching algorithm; the average order size; the average order duration; and the average cancellation rate.

Firms should investigate all incidences of potential spoofing. Those incidents could be identified by a number of sources, including traders and the firm's monitoring program. The effectiveness of a firm's compliance and monitoring program will be judged, in part, by whether the firm investigates all potential spoofing activity identified by the compliance and monitoring program. Firms with strong compliance cultures should not have to investigate very many potential spoofing incidents. The firm should document its conclusions even when it determines that no spoofing occurred so it is prepared to respond to questions if the activity is investigated by criminal, civil, or exchange authorities.

If a firm concludes as a result of an internal investigation that one or more of its traders has engaged in spoofing, the firm should consider voluntary disclosure of the spoofing activity to the DOJ, the CFTC, and / or the relevant exchange, as appropriate. Because there is a high likelihood that an exchange will identify the spoofing activity, a firm should decide quickly whether to make a voluntary disclosure. Cooperation credit depends, in large part, on disclosing problematic activity before it is identified by the authorities.

The decision to self-disclose potential misconduct to the Government is a highly fact-specific calculus with varying risks. As a threshold matter, DOJ only awards credit for "voluntary" self-disclosures, meaning that prosecutors may challenge the threshold determination of eligibility if they conclude that whistleblowers or press coverage prompted the disclosure. Under certain circumstances, DOJ may conclude that those background facts negate the voluntariness requirement, thereby disqualifying an applicant for credit as a self-discloser.

Moreover, even a voluntary self-disclosure inevitably invites some degree of investigation by the Government, which will attempt to pressure test for itself the internal investigation that the self-disclosing entity or individual conducted to ensure that it was sufficiently robust in identifying the extent of any misconduct and the wrongdoers. In terms of outcomes, the benefits likewise are uncertain: neither DOJ nor the CFTC guarantees a declination for self-disclosure. At most, DOJ offers a presumption in favor of a declination, absent "aggravating circumstances," for voluntary self-disclosures. More tangibly, DOJ commits that, in the event of a penalty, it will be discounted by half from the minimum penalty of what otherwise would have been assessed absent the self-disclosure.[29] Finally, to garner full credit for cooperation (and earn the maximum discount in the penalty or the declination), the self-disclosing entity must identify all individuals "substantially involved or responsible for the misconduct."[30]

Importantly, DOJ does not afford self-disclosure confidentiality, meaning that prosecutors could notify the CFTC or other regulatory stakeholders, such as exchanges or overseas authorities, regarding the self-disclosure. Making a self-disclosure therefore likely means approaching other authorities simultaneously, which carries obvious risks depending on the jurisdiction and particular regulatory mandates. In sum, approaching the Government requires a holistic risk assessment weighing all costs and benefits.

CONCLUSION

There is every reason to believe that the DOJ, the CFTC, and the exchanges will continue to focus considerable attention on spoofing. The electronic trading environment seems destined to continue to temp traders to test their ability to induce others to trade in a way that will benefit the execution of their orders. Furthermore, it is much easier for the authorities to prove a spoofing violation than a manipulation violation. Firms should take the necessary steps to manage their risk of exposure to spoofing by their employees and agents. Benjamin Franklin's centuries-old axiom remains sound advice even in today's electronic world: "An ounce of prevention is worth a pound of cure."

ENDNOTES:

[1]Press Release, DOJ, Former Precious Metals Trader Pleads Guilty to Commodities Fraud and Spoofing Conspiracy, https://www.justice.gov/opa/pr/former-precious-metals-trader-pleads-guilty-commodities-fraud-and-spoofing-conspiracy (Nov. 6, 2018) (emphasis added).

[2] https://www.justice.gov/criminal-fraud/file/1123566/download at 17; *see U.S. v. Edmonds*, 3:18-cr-00239 (D. Conn. filed Oct. 9, 2018); *U.S. v. Mao*, 4:18-cr-00606 (S.D. Tex. filed Oct. 10, 2010); *U.S. v. Gandhi*, 4:18-cr-00609 (S.D. Tex. filed Oct. 11, 2018); *U.S. v. Mohan*, 4:18-cr-00610; 4:18-cr-00080 (S.D. Tex. filed Oct. 11, 2018); *U.S. v. Bases and Pacilio* (N.D. Ill. filed July 18, 2018); *U.S. v. Vorley and Chanu*, 1:18-cr-00035 (N.D. Ill. filed July 24, 2018); *U.S. v. Zhao*, 1:18-cr-00024 (N.D. Ill. filed Jan. 11, 2018); *U.S. v. Thakkar*, 1:18-cr-00036 (N.D. Ill. filed Jan. 19, 2018); and *U.S. v. Flotron*, 3:17-cr-00220 (D. Conn. filed Jan. 30, 2018).

[3]James M. McDonald, *Speech of CFTC Enforcement Director James M. McDonald Regarding Enforcement trends at the CFTC, NYU School of Law: Program on Corporate Compliance & Enforcement*, CFTC, Nov. 14, 2018.

[4]*Id.*; see also James McDonald, *Statement of CFTC Director of Enforcement James McDonald*, CFTC, January 29, 2018.

[5]*Id.*

[6]*Id.*

[7]See Consent Orders: *In re Gandhi,* CFTC No. 19-0, 2018 WL 5084650 (Oct. 11, 2018); *In re The Bank of Nova Scotia*, CFTC No. 18-50, 2018 WL 4828376 (Sept. 28, 2018); *In re Mizuho Bank, Ltd., CFTC No. 18-38*, 2018 WL 4628253 (Sept. 21, 2018); *In re Geneva Trading USA, LLC*, CFTC No. 18-37, 2018 WL 4628252 (Sept. 20, 2018); *In re Victory Asset, Inc.*, CFTC No. 18-36, 2018 WL 4563040 (Sept. 19, 2018); *In re Franko*, CFTC No. 18-35, 2018 WL 4563039 (Sept. 19, 2018); *In re Singhal*, CFTC No. 18-11, 2018 WL 1782904 (Apr. 9, 2018); *In re HSBC Secs. (USA) Inc.*, CFTC No. 18-08, 2018 WL 684635 (Jan. 29, 2018); *In re UBS AG*, CFTC No. 18-07, 2018 WL 684636 (Jan. 29, 2018); and *In re Deutsche Bank AG*, CFTC No. 18-06, 2018 WL 684634 (Jan. 29, 2018). Litigated Cases: *CFTC v. Thakkar*, No. 1:18-cv-00619 (N.D. Ill. filed Jan. 28, 2018); *CFTC v. Zhao*, No. 1:18-cv-00620 (N.D. Ill. filed Jan. 28, 2018); *CFTC v. Mohan*, No. 4:18-cv-00260 (S.D. Tex. filed Jan. 28, 2018); *CFTC v. Vorley*, No. 1:18-cv-00603 (N.D. Ill. filed Jan. 26, 2018); and *CFTC v. Flotron*, No. 3:18-cv-00158 (D. Conn. filed Jan. 26, 2018).

[8]CME Group, Notices (December 20, 2018), https://www.cmegroup.com/tools-information/advisorySearch.html#cat=advisorynotices%3AAdvisory+Notices%2FMarket+Regulation+Advisories&pageNumber=1&subcat=advisorynotices%3AAdvisory+Notices%2FMarket+Regulation+Advisories%2FBusiness-Conduct-Committee&searchLocations=%2Fcontent%2Fcmegroup%2F

[9]Classic spoofing: ICE Futures U.S., *CASE NO. 2016-077: SETTLEMENT OF CHARGES AGAINST STUART SATULLO* (2018), https://www.theice.com/publicdocs/futures_us/disciplinary_notices/ICE_Futures_US_Stuart_Satullo_20180214..pdf; ICE Futures U.S., *CASE NO. 2017-030: SETTLEMENT OF CHARGES AGAINST SHAY CAHERLY* (2018), https://www.theice.com/publicdocs/futures_us/disciplinary_notices/ICE_Futures_US_Shay_Caherly_20180918.pdf; ICE Futures U.S., CASE NO. 2017-030: *SETTLEMENT OF CHARGES AGAINST TRADITUM GROUP LLC* (2018), https://www.theice.com/publicdocs/futures_us/disciplinary_notices/ICE_Futures_US_Traditum_Group_LLC_20180918.pdf; ICE Futures U.S., *CASE NO. 2017-001: SETTLEMENT OF CHARGES AGAINST BRIAN SOLDANO* (2018), https://www.theice.com/publicdocs/futures_us/disciplinary_notices/ICE_Futures_US_Brian_Soldano_20181205.pdf; ICE Futures U.S., *NOTICE OF SUMMARY ACCESS DENIAL* (2018), https://www.theice.com/publicdocs/futures_us/disciplinary_notices/ICE_Futures_US_Cowell_20180806.pdf; Entering orders without intent to trade: ICE Futures U.S., *CASE NO. 2017-049: SETTLEMENT OF CHARGES AGAINST STEP CONSULTING LLC* (2018), https://www.theice.com/publicdocs/futures_us/disciplinary_notices/ICE_Futures_US_Step_Consulting_LLC_20180917.pdf; ICE Futures U.S., *CASE NO. 2017-047: SETTLEMENT OF CHARGES AGAINST UNCIA ENERGY LP - SERIES I (2018),* https://www.theice.com/publicdocs/futures_us/disciplinary_notices/ICE_Futures_Uncia_Energy_LP_Series_I_201801204.pdf.

[10] Dodd-Frank Wall Street Reform and Consumer Protection Act, Public Law 111-203, 124 Stat. 1376, 1739, Sec. 747 (2010).

[11]Commodity Exchange Act, 7 U.S.C.A. § 4c(a)(5)(C) (1936).

[12]CFTC, Antidisruptive Practices Authority, Interpretive Guidance and Policy Statement, 78 Fed. Reg. 31890, 31896 (May 28, 2013).

[13]*Id.*

[14]CME Rule 575, Disruptive Practices Prohibited, *available at* https://www.cmegroup.com/content/dam/cmegroup/rulebook/CME/I/5/5.pdf. (Emphasis added). Similarly, CME Rule 575.B provides that "[n]o person shall enter or cause to be entered an actionable or non-actionable message or messages with intent to mislead other market participants." *See also* CME Group Market Regulation Advisory Notice, CME Group RA1807-5 (July 11, 2018), *available at* https://www.cmegroup.com/rulebook/files/cme-group-Rule-575.pdf.

[15]ICE Rule 4.02(l), Trade Practice Violations, *available at* https://www.theice.com/publicdocs/rulebooks/futures_us/4_Trading.pdf. (Emphasis added). ICE Rule 4.02(I)(C) provides that "[i]t is a violation to enter an order or market message, or cause an order or market message to be entered, with the intent to . . . mislead other market participants." *See also* ICE Futures U.S. Disruptive Trading Practices FAQs (August 2017), *available at* https://www.theice.com/publicdocs/futures_us/Futures_US_Disruptive_Practice_FAQ.pdf.

[16]7 U.S.C.A. § 13(a)(2).

[17]Press Release, CFTC, *Statement of CFTC Director of Enforcement James McDonald*, https://www.cftc.gov/PressRoom/SpeechesTestimony/mcdonaldstatement012918 (January 29, 2018).

[18]*See, e.g., United States v. Coscia*, 866 F.3d 782, 789, Comm. Fut. L. Rep. (CCH) P 34,84 (7th Cir. 2017), cert. denied, 138 S. Ct. 1989, 201 L. Ed. 2d 249 (2018) (programmer testified that the trading program was designed to "pump [the] market"); *United States v. Sarao*, No. 15-cr-75, Dkt. 24 (N.D. Ill. Sept. 2, 2015) (emails between the defendant and programmer expressly referenced spoofing).

[19]*See United States v. Flotron*, 2018 WL 1401986 (D. Conn. 2018). Flotron was a trader at

a global commodities firm, who was indicted for trades he placed for precious metal futures contracts from 2008 to 2013. In addition to trading analysis, the Government alleged that one of Flotron's subordinates witnessed Flotron place orders on the market that he intended to cancel. At trial, the Government's case relied primarily on trade data and testimony from two former subordinates, but lacked the algorithms and incriminating communications that characterized the proof in prior criminal spoofing cases.

[20]*United States v. Zhao,* No. 18-cr-24, Dkt. No. 1 (N.D. Ill. Jan. 11, 2018). Zhao was a trader at a proprietary trading firm in Australia, and was charged for alleged spoofing trades in the CME E-mini futures contracts market from 2012 to 2016. The criminal complaint cites extensively to a trading analysis by the FBI, coupled with an expert's opinion, to allege the requisite intent. According to that analysis, the alleged spoof orders were significantly larger, traded less frequently, and were exposed to the market for much shorter periods than Zhao's legitimate trades.

[21]Cristie Smythe, *Ex-UBS Metals Trader Beats Spoofing Conspiracy Charge,* Bloomberg (April 25, 2018), https://www.bloomberg.com/news/articles/2018-04-25/ex-ubs-metals-trader-flotron-beats-spoofing-conspiracy-charge.

[22]Maria Nikolova, *US Govt seeks more time to file info or indictment against Australian trader accused of spoofing, Financefeeds* (December 7, 2018), https://financefeeds.com/us-govt-seeks-time-file-info-indictment-australian-trader-accused-spoofing/.

[23]*See U.S. v. Thakkar, 1:18-cr-00036* (N.D. Ill. filed Jan. 19, 2018), *Complaint at 4* (noting cooperation by another trader and various inculpatory emails with the defendant regarding the cancellation of orders) and *U.S. v. John Edmonds*, 18-cr-239, Dkt. 1 (D. Conn. Oct. 9, 2018) (JP Morgan precious metals trader pleads guilty to six-year spoofing scheme; Press Release, DOJ, Three Traders Charged, and Two Agree to Plead Guilty, in Connection with over $60 Million Commodities Fraud and Spoofing Conspiracy, https://www.justice.gov/opa/pr/three-traders-charged-and-two-agree-plead-guilty-connection-over-60-million-commodities-fraud (Oct. 12, 2018).

[24]*See, e.g.*, Rule 21.01 of the ICE Futures U.S. Rulebook ("The Compliance Department shall have the authority to initiate and conduct investigations and to prosecute Rule violations committed by Members and by non-member market participants."). On August 3, 2012, ICE adopted Rule 4.00, which subjects any person initiating or executing a trade on ICE (directly or through an intermediary) to the jurisdiction of the exchange. The CME has adopted similar rules subjecting all exchange market participants to the jurisdiction of the exchange. *See* CME Rule 418 ("Any Person initiating or executing a transaction on or subject to the Rules of the Exchange directly or through an intermediary, and any Person for whose benefit such a transaction has been initiated or executed, expressly consents to the jurisdiction of the Exchange and agrees to be bound by and comply with the Rules of the Exchange in relation to such transactions, including, but not limited to, rules requiring cooperation and participation in investigatory and disciplinary processes.").

[25]*See* CME Rule 432.L.; ICE Rule 4.00(b).

[26]*See United States Securities and Exchange Commission v. Cook*, 2010 WL 11537512 (D. Minn. 2010); *U.S. Commodity Futures Trading Commission v. Gramalegui*, Comm. Fut. L. Rep. (CCH) P 34360, 2018 WL 4610953 (D. Colo. 2018).

[27]*See United States v. Coscia*, 866 F.3d 782, 790, Comm. Fut. L. Rep. (CCH) P 34,84 (7th Cir. 2017), cert. denied, 138 S. Ct. 1989, 201 L. Ed. 2d 249 (2018).

[28]*See* CME Group Market Regulation Advisory Notice, CME Group RA1807-5 (July 11, 2018), available at https://www.cmegroup.com/rulebook/files/cme-group-Rule-575.pdf; ICE Futures U.S., Disruptive Trading Practices FAQs (August 2017), available at https://www.theice.com/publicdocs/futures_us/Futures_US_Disruptive_Practice_FAQ.pdf.

[29]*See* United States Attorneys' Manual § 9-47.120, *FCPA Corporate Enforcement Policy*, https://www.justice.gov/criminal-fraud/file/838416/download. The policy, which was

originally limited **to** FCPA cases, was subsequently extended as non-binding guidance to other DOJ cases. *See* Remarks of Rod Rosenstein, Deputy Attorney General, DOJ, at the 32nd Annual ABA National Institute on White Collar Crime, https://www.justice.gov/opa/speech/deputy-attorney-general-rosenstein-delivers-remarks-32nd-annual-aba-national-institute (March 2, 2018).

[30]Rod J. Rosenstein, Deputy Attorney General, DOJ, Remarks at the 34th International Conference on the Foreign Corrupt Practices Act, https://www.justice.gov/opa/speech/deputy-attorney-general-rosenstein-delivers-remarks-34th-international-conference-foreign (Nov. 29 2017).