



2020 Year in Review

Spoofing and Market Manipulation

United States | United Kingdom | European Union

RAHMAN RAVELLI



Spoofing and Market Manipulation 2020 Year in Review

Among the many changes in 2020, at least one thing remained constant: US law enforcement's focus on "spoofing" and similar variations of market manipulation. The CFTC, SEC, and DOJ all notched important wins despite defendants' continued efforts to chip away at regulators' evolving theories of liability.

Across the Atlantic, the attention of British and European authorities was largely elsewhere this year. Yet with their US counterpart continuing to rack up huge spoofing penalties, UK/EU governments seeking to replenish their money-starved national treasuries will no doubt attempt to replicate the Americans' success in due course.

To get ready for what's to come in 2021, this review discusses and analyzes the key spoofing developments to date.

London, November 4, 2020

Table of Contents

KEY TAKEAWAYS	3	Status of Criminal Spoofing Cases Brought to Date	18
UNITED STATES	4	UNITED KINGDOM	19
Introduction	4	Introduction	19
A Continued Focus on Spoofing at the CFTC.....	4	The FCA and Ofgem Take Action Against Market Manipulation	20
No New CFTC "Vacuuming" Cases.....	11	EUROPEAN UNION	21
The SEC Continues its Ride on the Spoofing Bandwagon	11	Introduction	21
DOJ Moves on from its Trial Loss in Flotron.....	13	European Regulators Target Spoofing in the Energy Markets	22
DOJ Eeks out a Shaky Trial Win in Vorley.....	15	Impact of Brexit	23
The Defense Successfully Winnows Down DOJ's Case in Pacilio	16	CONTACTS	24
Is Spoofing an "Organized Crime"?.....	17	ENDNOTES	25

KEY TAKEAWAYS

- The COVID-19 outbreak did little to slow down the CFTC's regulatory actions against spoofing in 2020, with the agency recording its largest civil penalty in its history—a \$920 million fine against JP Morgan—for purported spoofing. Yet nearly all of the CFTC's 2020 spoofing actions were uncontested, and it remains to be seen whether the CFTC can successfully prove spoofing at trial.
- Spoofing actions filed by US regulators continue to disproportionately target traders located overseas, with defendants based in London, Ukraine, Bratislava, Hong Kong, China, Australia, South Korea, and the U.A.E.
- There were no new cases targeting so-called “vacuuming,” a variety of spoofing involving “fake” orders placed on the same side of the market as “real” ones.
- The SEC continues to target spoofing in the equities markets. In addition to securing a final judgment in its case against Lek Securities, the SEC settled two other spoofing actions and pressed ahead with its market manipulation case filed in Boston against dozens of Chinese nationals.
- The DOJ netted over \$981 million in monetary penalties from corporate defendants for spoofing-related misconduct (by far its largest annual haul for such crimes ever).
- The DOJ secured a mixed verdict against two former Deutsche Bank precious metals traders following a trial in Chicago. The trial judge suggested this result was susceptible to challenge, and defense motions for an acquittal and a new trial remain pending.
- Despite nine criminal spoofing convictions since 2015 (mainly through cooperation agreements), no US court has imposed a prison sentence for spoofing since Michael Coscia's 36-month sentence in 2015.
- Mirroring enforcement tactics used in the US, UK regulators are using large-volume data analytics to investigate spoofing. The FCA announced a number of open spoofing investigations and brought their latest enforcement action targetting the practice this year against a London-based trader.
- Regulators at the EU's ACER issued new guidance on market manipulation and appear to have taken a keen interest in manipulative trading on energy markets.

UNITED STATES

INTRODUCTION

The rules and regulations relating to spoofing and manipulation in the US financial markets are primarily enforced by three federal agencies: the Commodity Futures Exchange Commission (CFTC), the Securities and Exchange Commission (SEC), and the Department of Justice (DOJ).

CFTC: The CFTC is responsible for overseeing derivatives, such as futures, options, and swaps. These derivatives are generally tied to underlying assets like agricultural commodities (wheat, corn, cotton), energy (oil, gasoline), precious metals (copper, gold, silver) and financial instruments (interest rates, stock indexes, foreign currency). The CFTC's enforcement jurisdiction is limited to bringing civil and administrative actions against violators of the Commodities Exchange Act (CEA) (7 U.S.C. §§ 1-26) and its attendant regulations (17 C.F.R. pts. 1-190). The CEA specifically prohibits spoofing under § 4c(a)(5)(C) (7 U.S.C. § 6c(a)(5)(C)). Spoofing can also be targeted under the CEA's general anti-manipulation provisions contained in § 9(a) (7 U.S.C. § 13(a)).

SEC: The primary function of the SEC is to ensure compliance with two Depression-era federal laws—the 1933 Securities Act and the 1934 Exchange Act—that govern the issuance and exchange of stocks, bonds, and other securities. Unlike the CEA, neither the Securities Act nor the Exchange Act contain a provision that explicitly bans spoofing. Nevertheless, the SEC has brought enforcement actions against spoofing-like behavior under these laws' provisions prohibiting fraudulent behavior. Typically, these are Exchange Act § 9 (15 U.S.C. § 78i), Exchange Act § 10b (15 U.S.C. § 78j) and the accompanying Rule 10b-5, and Securities Act § 17(a)(3) (15 U.S.C. § 77q)).

DOJ: Willful violations of the CEA, Securities Act, and Exchange Act can be criminally prosecuted as felonies. In addition to these laws, DOJ can (and does) prosecute spoofing under the wire fraud (18 U.S.C. § 1343), commodities fraud (18 U.S.C. § 1348), and even racketeering (18 U.S.C. § 1963) statutes. The DOJ has the authority to prosecute any individual or company that violates these laws, and it often does so in parallel with civil actions brought by either the CFTC or SEC. When this occurs, the civil action is typically stayed until the criminal case is resolved. Spoofing cases have been primarily brought by the DOJ's Fraud Section, headquartered in Washington, DC. In 2019 in fact, the Fraud Section was reorganized to create a Market Integrity and Major Fraud Unit that contained a subsection specifically dedicated to pursuing CEA violations. While the Fraud Section can indict cases in any of the country's 94 judicial districts, most spoofing cases are brought in the Northern District of Illinois, home to the Chicago Mercantile Exchange and Chicago Board of Trade.

As detailed below, all of these regulators continued to actively pursue spoofing cases throughout 2020. These cases are underpinned by the government's increasingly sophisticated analytics capabilities that allow law enforcement to identify suspicious market activity within the enormous amount of trade data generated daily on US exchanges. With a variety of legal theories for prosecutors to choose from, and a statute of limitations that can stretch to ten years or more, spoofing regulation will remain a key concern for anyone with exposure to US markets in 2021 and years to come.

A CONTINUED FOCUS ON SPOOFING AT THE CFTC

On July 8, 2020, the CFTC finalized its 2020-2024 Strategic Plan.¹ This document describes one of the agencies "Strategic Goals" as focusing on "detecting, investigating, and prosecuting misconduct that could potentially undermine

market integrity,” including “fraud, manipulation, spoofing, and disruptive trading.”² To that end, an increasing share of the CFTC’s enforcement resources have gone towards enforcing the CEA’s anti-spoofing provision (ASP) in recent years.³

As the CFTC’s Chairman stated after the \$920 million spoofing penalty against JPMorgan in

September, “Spoofing is illegal — pure and simple. This record-setting enforcement action demonstrates the CFTC’s commitment to being tough on those who intentionally break our [spoofing] rules.”

Reflecting this perspective, the CFTC brought over a dozen spoofing enforcement actions this year (nearly breaking its annual record). Each of these cases is summarized below.

In re. Mirae Asset Daewoo Co., Ltd., CFTC Docket No. 20-11 (Jan. 13, 2020)

Trader Location:	Seoul, South Korea
Relevant Time Period:	December 2014 to April 2016
Futures Contract Affected:	S&P 500 Index (E-Mini)
Exchange Affected:	Chicago Mercantile Exchange
Alleged Conduct:	Disproportionally large orders that were intended to be cancelled were placed on one side of the market. These orders created a “misleading impression of market depth” and thereby induced other traders to place orders in the same direction. Small orders were then entered on the opposite side of the market which were subsequently filled. Within seconds of the fill, the large orders were cancelled.
Loss Amount:	Not specified
Resolution:	\$700,000 (Civil Penalty)
Cooperation Credit:	Yes
Parallel DOJ Action:	No

In re. Propex Derivatives Pty Ltd, CFTC Docket No. 20-12 (Jan. 21, 2020)

Trader Location:	Sydney, Australia
Relevant Time Period:	July 2012 to March 2017
Futures Contract Affected:	S&P 500 Index (E-Mini)
Exchange Affected:	Chicago Mercantile Exchange
Alleged Conduct:	On thousands of occasions, orders were placed with the intent to cancel them. Orders that were intended to execute were then placed on the opposite side. The alleged “spoofer” orders were generally five times as large as the corresponding “real” orders. The “spoofer” orders were cancelled shortly after the “real” orders were filled.
Loss Amount:	\$464,300
Resolution:	\$464,300 (Restitution) \$462,271 (Civil Penalty) \$73,429 (Disgorgement)
Cooperation Credit:	Yes
Parallel DOJ Action:	Yes (<i>United States v. Propex Derivatives Pty Ltd</i> , 20-cr-0039 (N.D. Ill.))

In re. Deutsche Bank Securities Inc., CFTC Docket No. 20-17 (June 18, 2020)

Trader Location:	Tokyo, Japan
Relevant Time Period:	January 2013 to December 2013
Futures Contract Affected:	Treasury, Eurodollar
Exchange Affected:	Chicago Mercantile Exchange
Alleged Conduct:	The alleged trading activity followed the typical “spoofing” pattern: large orders were placed on one side of the market to induce others to fill smaller orders placed on the other side; the larger orders were then cancelled. The “spoof” orders were generally 20 times larger than the smaller orders left open at the same time. Evidence suggested that this strategy was used primarily during New York overnight hours, when trading volume was substantially decreased, so as to have a larger market impact. There was also evidence that spoof orders were placed in the market for one futures contracts in order to influence trading in a separate, but related, contract.
Loss Amount:	Not specified
Resolution:	\$1,250,000 (Civil Penalty)
Cooperation Credit:	Yes
Parallel DOJ Action:	No

In re. The Bank of Nova Scotia (BNS), CFTC Docket No. 20-27 (Aug. 19, 2020)

Trader Location:	New York, London, Hong Kong
Relevant Time Period:	January 2008 to July 2016
Futures Contract Affected:	Gold, Silver
Exchange Affected:	Commodity Exchange, Inc.
Alleged Conduct:	<p>On thousands of occasions, large orders (or multiple small orders) were placed with the intent to cancel them. Orders that were intended to execute were then placed on the opposite side. The alleged “spoof” orders were generally five times as large as the corresponding “real” orders. The “spoof” orders were cancelled shortly after the “real” orders were filled. This practice allowed BNS traders to execute trades at their desired price, allegedly causing harm to other market participants.</p> <p>Evidence showed that BNS’s compliance staff were aware of the conduct but did nothing to stop it. For example, one of the principal traders responsible for much of the spoofing activity contacted BNS compliance to request clarification on whether his trading strategies were compliant with CFTC guidance. Although the request was elevated to senior compliance officers, no action was taken. In an email explaining this decision, a compliance officer wrote: “[W]hat is being seen may look like potential layering or spoofing, but based on the fact [that] we are talking [about] 1 lot, we believe he is just adjusting his exposure to the marketplace.” This assessment was determined to be wrong by the CFTC and BNS was punished for failing to adequately supervise its traders.</p>
Loss Amount:	\$6,622,190
Resolution:	\$6,622,190 (Restitution) \$42,000,000 (Civil Penalty) \$11,828,912 (Disgorgement)
Cooperation Credit:	Yes
Parallel DOJ Action:	Yes (<i>United States v. Bank of Nova Scotia</i> , 20-cr-00707 (D.N.J.); <i>United States v. Flaum</i> , 19-cr-00338 (E.D.N.Y.))

CFTC v. Edge Financial Technologies, Inc., 18-cv-00619, Docket No. 65-1 (N.D. Ill. Aug. 13, 2020)

Trader Location:	London
Relevant Time Period:	January 2013 to October 2013
Futures Contract Affected:	S&P 500 (E-mini)
Exchange Affected:	Chicago Mercantile Exchange
Alleged Conduct:	Edge Financial was not alleged to have engaged in any manipulative market behavior itself. Rather, the company was accused of creating a trading program that allowed a London-based trader (Navinder Sarao) engage in a spoofing scheme. The program's key component was a "Back-of-Book" function that kept Sarao's "spoofer" orders behind other orders at a particular price level to minimize the chances they would be filled. In the event any portion of these orders were filled, the program immediately and automatically cancelled the balance. The CFTC contended that these program functions were intentionally designed to help Sarao place orders that he did not intend to fill for the purpose of influencing the trading decisions of other market participants.
Loss Amount:	Not specified
Resolution:	\$24,200 (Disgorgement) \$48,400 (Civil Penalty)
Cooperation Credit:	Yes
Parallel DOJ Action:	Yes (<i>United States v. Sarao</i> , 15-cr-00075 (N.D. Ill.); <i>United States v. Thakkar</i> , 18-cr-00036 (N.D. Ill.))

In re. Thomas Donino, CFTC Docket No. 20-68 (Sept. 28, 2020)

Trader Location:	Jupiter, Florida
Relevant Time Period:	January 2013 to January 2016
Futures Contract Affected:	Soybean, Gold, Crude Oil
Exchange Affected:	Chicago Board of Trade, Commodity Exchange, Inc., New York Mercantile Exchange
Alleged Conduct:	Donino was a trader at a proprietary trading firm (FNY Partners Fund LP) who was alleged to have entered large orders he did not intend to execute in a variety of commodities markets. These "spoofer" orders were generally five times as large as orders he simultaneously placed on the other side of the market that he wanted to be filled. After the smaller orders were filled, Donino quickly cancelled the large orders.
Loss Amount:	Not specified
Resolution:	\$135,000 (Civil Penalty)
Cooperation Credit:	No
Parallel DOJ Action:	No

In re. FNY Partners Fund LP, CFTC Docket No. 20-67 (Sept. 28, 2020)

Trader Location:	Jupiter, Florida
Relevant Time Period:	January 2013 to January 2016
Futures Contract Affected:	Soybean, Gold, Crude Oil
Exchange Affected:	Chicago Board of Trade, Commodity Exchange, Inc., New York Mercantile Exchange
Alleged Conduct:	FNY Partners was held liable for failing to prevent the spoofing of one of its traders (Thomas Donino).
Loss Amount:	Not specified
Resolution:	\$450,000 (Civil Penalty)
Cooperation Credit:	Yes
Parallel DOJ Action:	No

In re. JP Morgan Chase & Co., et al., CFTC Docket No. 20-69 (Sept. 29, 2020)

Trader Location:	New York, Singapore, London
Relevant Time Period:	At least 2008 through 2016
Futures Contract Affected:	Precious Metals, Treasuries, Treasury Bonds
Exchange Affected:	Commodity Exchange, Inc., New York Mercantile Exchange, Chicago Board of Trade
Alleged Conduct:	<p>The JPM Precious Metals Desk and Treasuries Desk's spoofing conduct followed the classic pattern. First, a trader would place a relatively small order (sometimes an iceberg order) that he desired to execute ("Genuine Order"). Before or after entering a Genuine Order, the trader would, on the opposite side of the market, place a non-iceberg, relatively large resting order that he intended to cancel before execution ("Spoof Order"), or alternatively would rapidly place a series of non-iceberg resting orders that he intended to cancel before execution ("Layered Spoof Orders"). The trader's Spoof Order or total Layered Spoof Orders would be for a greater number of lots than the visible quantity of his Genuine Order on the opposite side of the market. Finally, traders would typically cancel their Spoof Orders shortly after placing them, and would typically cancel the highest bids or lowest offers placed in a given series of Layered Spoof Orders shortly after placing them.</p> <p>A Precious Metals Desk or Treasuries Desk trader's goal in spoofing through this pattern of trading was to manipulate market prices so that all or part of his Genuine Order would be filled at an artificial price. In placing Spoof Orders and Layered Spoof Orders, JP Morgan traders falsely represented to market participants that they actually wanted to buy or sell the number of lots in their orders when, in reality, they did not want to do so.</p>
Loss Amount:	\$311,737,008
Resolution:	\$311,737,008 (Restitution) \$436,431,811 (Civil Penalty) \$120,332,430 (Disgorgement)
Cooperation Credit:	Yes
Parallel DOJ Action:	Yes (<i>United States v. JPMorgan Chase & Co.</i> , 20-cr-00175 (D. Conn.); <i>United States v. Edmonds</i> , 18-cr-00239 (D. Conn.); <i>United States v. Trunz</i> , 19-cr-00375 (E.D.N.Y.); <i>United States v. Smith, et al.</i> , 19-cr-00669 (N.D. Ill.))

CFTC v. Roman Banoczay, Jr., et al., 20-cv-05777, Docket No. 1 (N.D. Ill. Sept. 29, 2020)

Trader Location:	Bratislava, Slovakia
Relevant Time Period:	January 16, 2018 to February 12, 2018
Futures Contract Affected:	Crude Oil
Exchange Affected:	New York Mercantile Exchange
Alleged Conduct:	Banoczay, Jr. and his father were principals of a trading firm that actively traded in the crude oil futures markets. After suffering substantial losses in 2018, the CFTC alleges that they began to engage in a spoofing scheme that involved placing “spoofer” orders up to 700 times per day. This strategy allowed them to earn over \$332,000 in profits in just eight days.
Loss Amount:	\$332,000
Resolution:	Pending
Cooperation Credit:	N/A
Parallel DOJ Action:	No

In re. Brandan Delovitch, CFTC Docket No. 20-71 (Sept. 30, 2020)

In re. Wesley Johnson, CFTC Docket No. 20-72 (Sept. 30, 2020)

In re. Rajeev Kansal, CFTC Docket No. 20-73 (Sept. 30, 2020)

Trader Location:	Ontario, Canada; India
Relevant Time Period:	March 2017 to June 2020
Futures Contract Affected:	Lean Hogs, Live Cattle, Silver, Copper, Soybean, Cotton, Canola, Sugar
Exchange Affected:	Chicago Mercantile Exchange, Commodity Exchange, Inc., Chicago Board of Trade, ICE Futures US
Alleged Conduct:	The traders charged in these related cases worked for ARB Trading Group LP, a proprietary trading firm. The CFTC alleged that they each engaged in a spoofing strategy involving the entry of large orders they did not intend to execute in a variety of commodities markets. These “spoofer” orders were generally five times as large as orders simultaneously placed on the other side of the market that they wanted to be filled. After the smaller orders were filled, the larger orders were quickly cancelled.
Loss Amount:	Not specified
Resolution:	\$100,000 each (Civil Penalty)
Cooperation Credit:	No
Parallel DOJ Action:	No

In re. ARB Trading Group LP, CFTC Docket No. 20-74 (Sept. 30, 2020)

Trader Location:	Ontario, Canada; India
Relevant Time Period:	March 2017 to June 2020
Futures Contract Affected:	Lean Hogs, Live Cattle, Silver, Copper, Soybean, Cotton, Canola, Sugar
Exchange Affected:	Chicago Mercantile Exchange, Commodity Exchange, Inc., Chicago Board of Trade, ICE Futures US
Alleged Conduct:	ARB Trading was held liable for alleged spoofing activity of five of its traders. The trading data showed that each trader engaged in essentially the same strategy: placement of an order that they wanted to get filled ("Genuine Order"), on one side of the market, typically consisting of a passive order for ten or fewer contracts; and on the opposite side of the market, placement of one or more orders that they intended to cancel before execution ("Spoof Order"), typically consisting of one or more passive orders for, collectively, five times as many contracts as the Genuine Order. Once the Genuine Orders were filled, the Spoof Orders were then quickly cancelled.
Loss Amount:	Not specified
Resolution:	\$445,000 (Civil Penalty)
Cooperation Credit:	Yes
Parallel DOJ Action:	No

In re. Sunoco LP, CFTC Docket No. 20-75 (Sept. 30, 2020)

Trader Location:	Dallas, Texas
Relevant Time Period:	February 2014 to January 2015
Commodity Affected:	Crude Oil, Heating Oil, RBOB (Gasoline)
Exchange Affected:	New York Mercantile Exchange
Alleged Conduct:	A Sunoco trader placed small iceberg orders on one side of the market that he wanted to get filled. He then placed on the opposite side of the market one or more larger orders, often for 50 or 100 lots, that he intend to cancel before execution. If his small orders were filled, he would then generally cancel his larger orders quickly thereafter.
Loss Amount:	Not specified
Resolution:	\$450,000 (Civil Penalty)
Cooperation Credit:	Yes
Parallel DOJ Action:	No

NO NEW CFTC “VACUUMING” CASES

Since the CEA’s anti-spoofing provision sprung into existence with the passage of the 2010 Dodd-Frank Wall Street Reform and Consumer Protection Act, virtually every CFTC enforcement action has targeted market activity following the same pattern: (1) “real” orders that a trader wants to be executed are placed on one side of the market (usually as an iceberg⁴); (2) larger “spoofer” orders are placed on the opposite side; (3) if and when the “real” orders are filled, the “spoofer” orders are quickly cancelled. The government’s overarching theory in these cases is that the spoofs are intended to induce other traders into placing their own orders in front of the spoofs, and thereby fill the real orders lying in wait on the other side.

In September 2019, the CFTC brought attention to a new form of spoofing-like manipulative behavior—“vacuuming”—that diverged from the classic spoofing model. In an administrative action against Hard Eight Futures, LLC, the CFTC alleged that one of its traders spoofed the E-mini S&P 500 futures market by placing orders he intended to cancel on the same side of the market as orders he wanted to execute. According to the CFTC:

“Trader A canceled his Spoof Orders in a manner designed to create what is sometimes referred to as a ‘vacuum’—that is, by canceling his Spoof Orders virtually simultaneously to create the false impression of a sudden and significant decline in buying or selling interest, [Trader A] indicated an imminent price decrease or increase. Trader A intended

for other traders to react to this ‘vacuum’ by placing aggressive orders that crossed the bid-ask spread, to fill Genuine Orders Trader A left resting on the same side of the market as the ‘vacuum’ he had created. This often resulted in Trader A successfully moving the market an entire price level.”¹⁵

For this conduct as well as classic spoofing, Hard Eight agreed to pay a civil penalty of \$1,750,000 and the firm’s founder, Igor Chernomzaz, agreed to pay a separate penalty of \$750,000.

Because neither Hard Eight nor Chernomzaz contested the CFTC’s allegations, there is little publicly disclosed information about the specifics of the alleged “vacuuming” technique. And since there have been no further regulatory actions targeting vacuuming to date, whether this theory will be upheld in court or form the basis of additional civil or criminal cases remains to be seen. In any event, it is likely that regulators will continue to analyze trade data for signs of vacuuming and, at the very least, investigate those that may be responsible for engaging in the practice.

THE SEC CONTINUES ITS RIDE ON THE SPOOFING BANDWAGON

Perhaps because Congress only inserted an anti-spoofing provision into the CEA (and not the Securities or Exchange Acts), the SEC lagged behind the CFTC in terms of its efforts against spoofing. Yet in the last several years, the SEC has started to shift its focus towards spoofing activity on the US securities markets that are within its remit.

- **SEC v. Lek Securities Corp., et al., 17-cv-01789 (S.D.N.Y.)**

In November 2019, the SEC notched an important trial win against two individuals, Nathan Fayer and Sergey Pustelnik, and

their firm, Avalon FA Ltd., headquartered in Kiev, Ukraine. In its 2017 complaint, the SEC alleged that a US broker-dealer, Lek Securities Corporation, and its CEO, Samuel Lek, assisted Avalon carry out a manipulative trading scheme involving “layered” orders in US equity markets. While not labelled as “spoofing,” the conduct was essentially identical. Avalon purportedly placed “non-bona fide orders”—orders that it did not intend to execute and that had no legitimate economic purpose—to buy or sell stock. Avalon’s alleged purpose in entering these orders was to obtain more favorable prices on its other orders. Between December 2010 through September 2016, trade data showed that Avalon used this technique hundreds of thousands of times and made millions in profits.

The SEC also alleged that Avalon engaged in a separate “cross-market manipulation” scheme that involved intentionally trading stocks at a loss for the purpose of artificially moving the prices of corresponding options (which Avalon would then trade at a profit). This strategy was employed hundreds of times between August 2012 and December 2015 for a significant profit. Together, the layering and cross-market manipulation schemes purportedly netted Avalon more than \$28 million.

Sam Lek and his company eventually settled the claims against them—Lek agreed to pay a \$420,000 penalty, and Lek Securities agreed to retain a monitor for three years, disgorge \$525,892, and pay a \$1 million penalty.

Following a nearly two week-long trial against the remaining defendants, the jury returned a unanimous verdict for the SEC on November 12, 2019. On March 20, 2020, the court issued its final judgment: joint and several disgorgement of \$4,495,564, and a separate civil penalty of \$5,000,000 each against Avalon, Fayer, and Pustelnik. This ruling is currently being appealed.

- **In re. Nicholas Mejia Scrivener, SEC Docket No. 3-19908 (Aug. 10, 2020)**

On August 10, 2020, the SEC settled an administrative proceeding against Nicholas Mejia Scrivener, an independent day trader based in California. According to the SEC’s order, between February 2015 and September 2016, Scrivener used multiple brokerage accounts to place non-bona fide orders for stocks to induce other traders to fill his other orders placed on the opposite side of the market. For example, after establishing a long position in a stock, Scrivener would place multiple orders to buy that stock, at multiple price levels, without an intent to execute those orders. These orders were designed to push up the market price, after which Scrivener would then sell his shares at an inflated value. The buy orders would then be cancelled. Through this practice, Scrivener allegedly earned at least \$140,250 in illicit profits. The SEC claimed that Scrivener’s conduct violated § 9(a)(2) of the Exchange Act (15 U.S.C. § 78i(a)(2)) and ordered him to disgorge \$140,250 and pay a civil penalty of \$50,000.

- **In re. J.P. Morgan Securities LLC, SEC Docket No. 3-20094 (Sept. 29, 2020)**

On September 29, 2020, the SEC settled an administrative proceeding against J.P. Morgan Securities LLC. That case, brought in conjunction with related actions by the

CFTC and DOJ, alleged that JP Morgan traders engaged in manipulative trading of U.S. Treasuries between April 2015 and January 2016. As in other spoofing schemes, non-bona fide orders were entered on one side of the market that were intended to create a false impression of trading interest and drive prices up or down. As a result, orders placed on the opposite side of the market were able to be executed at more favorable prices than otherwise would have been possible. The SEC claimed that this conduct violated § 17(a)(3) of the Securities Act, which prohibits any person from engaging in any transaction or course of business which operates as a fraud or deceit upon the purchaser. To resolve these charges, J.P. Morgan agreed to disgorge \$10,000,000 and pay a \$25,000,000 civil penalty.

- **SEC v. Chen, et al., 19-cv-012127 (D. Mass.)**

The SEC's 2019 spoofing action against dozens of China-based traders continues to develop. In an amended complaint filed last December, the SEC alleged that starting in August 2013, the defendants engaged in a coordinated market manipulation scheme using numerous accounts at several different brokerage firms to artificially influence the prices of various publicly traded securities in the US. The intent of this purported "scheme was to create the false appearance of trading interest and activity in particular stocks, thereby enabling [Defendants] to reap illicit profits by artificially boosting or depressing stock prices." To avoid detection, the Defendants allegedly used nominee accounts held in the names of others and/or

misrepresented the nature of their trading to brokerage firms. The SEC alleges that this conduct violated §§ 9(a)(2) and 10(b) of the Exchange Act, Rule 10b-5, and §§ 17(a)(1) and (3) of the Securities Act, and generated \$31 million in illegal gains.⁶ A number of the defendants failed to answer the SEC's complaint and default judgments were subsequently entered against them earlier this year. Litigation with the non-defaulting defendants appears to be continuing, but no trial date has yet been set.

DOJ MOVES ON FROM ITS TRIAL LOSS IN FLOTRON

While the DOJ has successfully extracted a number of guilty pleas and DPAs from individual traders and their firms since 2015⁷, it began 2020 with a mixed record in contested spoofing cases. After winning its first ever spoofing trial in *United States v. Coscia*, 14-cr-00551 (N.D. Ill.), DOJ lost its second, *United States v. Flotron*, 17-cr-00220 (D. Conn.).

The third criminal spoofing trial took place in April 2019. Unlike *Coscia* and *Flotron*, that case was not against a trader, but rather a software programmer. The defendant, Jittesh Thakkar, was accused of aiding and abetting an alleged spoofing scheme orchestrated by Navinder Sarao, a London-based trader accused of causing the 2010 "flash crash."⁸ Even after securing Sarao's testimony against Thakkar (following a guilty plea in a separate case against him), the jury was unable to reach a verdict and the court declared a mistrial. The DOJ declined to retry Thakkar and the criminal charges against him were dismissed.

Despite DOJ's seeming difficulties in securing spoofing convictions at trial, prosecutors continued to file new cases and resolve old ones this year. In fact, the DOJ secured three major Deferred Prosecution Agreements

(DPA) this year, netting over \$981,000,000 in monetary penalties from corporate defendants for spoofing-related conduct (by far its largest annual spoofing haul ever):

- January 21, 2020: **Propex Derivatives Pty Ltd.** entered into a DPA requiring it to pay \$1 million in penalties, disgorgement, and restitution.
- August 19, 2020: **The Bank of Nova Scotia** entered into a DPA requiring it to pay \$60,451,102 in penalties, disgorgement, and restitution.
- September 29, 2020: **JPMorgan Chase & Co.** entered into a DPA requiring it to pay \$920 million in penalties, disgorgement, and restitution.⁹

With respect to individuals, as of January 1, 2020 DOJ had six open criminal spoofing cases that had already resulted in publicly disclosed guilty pleas:

- **United States v. Sarao, 15-cr-00075 (N.D. Ill.)**
Navinder Sarao was a London-based day trader who was charged in November 2016 with placing false buy and sell orders on the S&P Mini 500 to fake an impression of supply and demand that allowed him to execute genuine trades at prices more favorable to him. After spending four months in a London prison, Sarao was extradited to the U.S. and pled guilty to wire fraud and spoofing in his initial court appearance. Following his guilty plea, Sarao cooperated with the government and testified against Jitesh Thakkar, the programmer who built Sarao's trading programs. In light of Sarao's severe autism and a
- **United States v. Zhao, 18-cr-00024 (N.D. Ill.)**
Jiongsheng Zhao was a proprietary trader based in Sydney, Australia who was charged in a one count information on December 18, 2017. DOJ alleged that from 2012 to 2016, Zhao placed thousands of spoof orders for E-mini S&P 500 futures contracts on the Chicago Mercantile Exchange (CME). On January 29, 2018, Zhao was arrested by the Australian Federal Police and remanded into custody pending extradition to the US. He was extradited later that year and eventually pled guilty pursuant to a cooperation agreement in December 2018. Zhao's cooperation led to the DOJ's subsequent DPA with his former employer, Propex, in January 2020. At his sentencing hearing on February 4, 2020, Zhao was sentenced to time served.
- **United States v. Flaum, 19-cr-00338 (E.D.N.Y.)**
Corey Flaum is a former precious metals trader at Scotia Capital and Bear Stearns who pleaded guilty to a one count information on July 25, 2019. He was accused of placing thousands of "spoof" orders over a nine-year period beginning in June 2007. Flaum continues to cooperate in ongoing spoofing investigations in the precious metals markets, and his sentencing is currently scheduled for January 27, 2021.
- **United States v. Edmonds, 18-cr-00239 (D. Conn.)**
John Edmonds is a former precious metals trader at J.P. Morgan who pleaded guilty to

a two count information on October 9, 2018. Edmonds was originally scheduled to be sentenced in December 2018, but in light of his cooperation with the DOJ, his sentencing has been rescheduled a number of times. As of this writing, no new sentencing date appears on the docket.

- ***United States v. Trunz, 19-cr-00375 (E.D.N.Y.)***

Christian Trunz was a precious metals trader for J.P. Morgan at its London, Singapore, and New York offices. In August 2019, he pleaded guilty to two counts of conspiracy to commit wire fraud. Trunz admitted to conspiring with other traders to enter spoof orders to buy and sell precious metals futures contracts in order to induce other market participants to fill certain orders. Like Edmonds, Trunz is cooperating with the DOJ and is scheduled to be sentenced on January 28, 2021.

- ***United States v. Liew, 17-cr-00001 (N.D. Ill.)***

David Liew was a precious metals trader for Deutsche Bank based in Singapore. On May 24, 2017, Liew was charged with conspiring to commit securities fraud and spoofing by placing numerous spoof orders between 2009 and 2012. In June 2017, Liew voluntarily surrendered to U.S. authorities and pleaded guilty to the information pursuant to a plea agreement. Liew cooperated with prosecutors and testified against his former colleagues, James Vorley and Cedric Chanu, at their trial in September. In a filing on October 7, 2020, the DOJ requested that Liew's sentencing be postponed until after Vorley and Chanu's sentencing in January 2021.

DOJ EEKS OUT A SHAKY TRIAL WIN IN VORLEY

The Vorley case is notably for its novel charging theory. Although the underlying conduct was for all intents and purposes classic spoofing, the DOJ did not allege a violation of the CEA's anti-spoofing provision. Rather, DOJ charged the defendants, both former precious metals traders at Deutsche Bank, with conspiracy to commit wire fraud affecting a financial institution in violation of 18 U.S.C. § 1349. By charging the case as wire fraud, DOJ was able to take advantage of a longer, ten-year statute of limitations and reach conduct that would have otherwise been time-barred.

At the same time, framing the case as a fraud opened up the indictment to an attack by the defendants. In their motion to dismiss the original indictment, defendants argued that prosecutors' failed to state a wire fraud offense because they did not allege any actual false statements. Specifically, they contended that because the indictment alleged "real, at-risk offers that [they] were obligated to, and did, fill if they were accepted before the defendants could withdraw them, their conduct in placing those orders could not have violated the wire fraud statute."¹⁰ But Judge Tharp was unpersuaded. In denying the motion to dismiss, he held that a wire fraud conviction does not require proof of a false statement. Rather, defendants can engage in a "scheme to defraud" through "implied misrepresentations" only. And further, Judge Tharp ruled that whether the orders at issue actually constituted an implied misrepresentation was a central fact question to be decided by the jury.¹¹

Following this ruling, prosecutors filed a superseding indictment on November 26, 2019 that included a number of additional counts and alleged spoofing instances. Defendants moved to dismiss this new indictment based on purportedly improper pre- and post-indictment delay in violation of the Speedy Trial Act.¹² After this motion too was denied, the parties proceeded to trial in September.

After a week-long, socially distanced trial in which no affirmative defense case was presented, jurors deliberated for nearly three days (after at least twice indicating they were deadlocked and drawing an Allen¹³ charge from Judge Tharp). On September 25, 2020, the jury returned a mixed verdict that found Vorley guilty of three of the nine counts against him and his co-defendant, Cedric Chanu, guilty of seven of the eleven counts against him.

Following the verdict, the defendants indicated they will seek an acquittal under Federal Rule of Criminal Procedure 29 and, in the alternative, a new trial under Federal Rule of Criminal Procedure 33. Potentially signaling that the DOJ's conviction was susceptible to these challenges, Judge Tharp denied prosecutors' request for remand pending sentencing and stated: "[T]here are any number of issues here that are going to be further litigated in this court and then I'm sure litigated in the Seventh Circuit. . . . I'm sure [defendants] have every reason to . . . harbor some significant hope, and not just hope but reasonable expectation that, you know, this verdict may not stand."¹⁴

While these issues are hashed out, sentencing is tentatively set for January 21, 2021.

THE DEFENSE SUCCESSFULLY WINNOWS DOWN DOJ'S CASE IN PACILIO

John Pacilio is a former precious metals trader who in early 2018 was charged, along with his former colleague Edward Bases, with wire fraud affecting a financial institution (18 U.S.C. § 1343), commodities fraud (18 U.S.C. § 1348), and conspiracy to commit commodities fraud (18 U.S.C. § 1349). Pacilio was separately charged with a single count of violating the anti-spoofing provision of the CEA.¹⁵

In November 2018, both defendants moved to dismiss the common counts against them. The crux of their argument was that the bids and offers at issue could not, as a matter of law, serve as a basis for a wire or commodities fraud conviction. In the defendants' view, all of their orders accurately stated the terms of a proposed transaction which could have been accepted by any counterparty that decided to accept them.¹⁶ But District Court Judge Lee rejected this argument in a May 2020 decision: "[Defendants'] theory ignores the indictment's allegations . . . that Defendants never intended to fill the bids and orders in question and placed them solely for the purpose of creating a misleading picture of market conditions that they used to their benefit."¹⁷

While unsuccessful in dismissing the fraud counts, Pacilio fared better in a separate motion that sought to toss out the spoofing charge on three grounds: duplicity, lack of specificity, and the statute of limitations.¹⁸ On October 16, 2020, Judge Lee concluded that the spoofing count was indeed improperly duplicitous¹⁹ and he ordered its dismissal without addressing the alternative arguments.

The count at issue charged Pacilio with a single spoofing violation but was based on factual allegations that spanned numerous different

trades occurring across several years. The government argued that spoofing was a “scheme” offense that allowed prosecutors to charge multiple instances of criminal behavior under a single count. Noting that the anti-spoofing provision does not use the word “scheme” (in contrast to the wire and commodities fraud statutes), Judge Lee concluded that spoofing was not a scheme offense. In other words, he held that spoofing must be charged as a single course of conduct during a discrete time period. Because the indictment against Pacilio failed to do so, Judge Lee granted Pacilio’s motion to dismiss the spoofing count.

Pacilio and Bases’ trial on the remaining counts is scheduled to begin in Chicago on July 21, 2021.

IS SPOOFING AN “ORGANIZED CRIME”?

Just before JP Morgan reached its nearly \$1 billion DPA in September 2019, the DOJ unsealed an indictment against three of its former precious metals traders: Michael Nowak, Gregg Smith, and Christopher Jordan.²⁰ Like previous spoofing cases, this case involved substantive wire fraud, commodities fraud, and spoofing charges. But in an unprecedented move, the defendants were also charged with a racketeering conspiracy in violation of the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. §§ 1961-1968 (“RICO”). The RICO statute was passed in the early 1970s and was specifically designed to give prosecutors a mechanism to target top organized crime bosses. Since that time, it has repeatedly done just that, with it famously being used to bring down numerous members of the five New York mafia families (among many others).

As applied to precious metals trading, the DOJ’s theory is that the JP Morgan precious metals desk effectively acted as a long-running criminal enterprise. According to the indictment, the defendants conspired to “conduct and participate, directly and indirectly, in the conduct of the enterprises’ affairs through a pattern of racketeering activity . . . consisting of multiple acts” of wire fraud affecting a financial institution and bank fraud. These alleged frauds involved traditional spoofing as well as a separate scheme to defraud counterparties in “barrier options” transactions.

On February 28, 2020, defendants filed a motion to dismiss the RICO conspiracy count and each of the other substantive counts related to spoofing.²¹ In summary, the defendants argue:

- The indictment failed to allege a scheme or artifice to defraud because: (1) “open-market orders that are alleged to carry a genuine risk of execution cannot, by themselves, constitute a scheme or artifice to defraud”; and (2) there are no alleged misrepresentations or omissions.
- The indictment failed to allege specific intent to defraud a financial institution (a requisite element of the relevant offense);
- The spoofing-based fraud allegations are unconstitutionally vague; and
- The conduct alleged in the indictment is not racketeering activity for purposes of the RICO statute.

The motion additionally seeks to dismiss certain charges based on lack of specificity, duplicity, and the statute of limitations.

No ruling has yet been issued on this motion. In the event it’s denied, trial is scheduled to commence in September 2021.

STATUS OF CRIMINAL SPOOFING CASES BROUGHT TO DATE

CORPORATES

Defendant	Result	Year	Penalty
Merrill Lynch Commodities, Inc.	NPA	2019	\$25 million
Tower Research Capital LLC	DPA	2019	\$67.4 million
Propex Derivatives Pty Ltd.	DPA	2020	\$1 million
Bank of Nova Scotia	DPA	2020	\$60.4 million
JP Morgan Chase & Co.	DPA	2020	\$920 million

INDIVIDUALS

Defendant	Result	Year	Sentence
Michael Coscia	Guilty following trial	2015	36 months
Navinder Sarao	Guilty plea with cooperation	2017	1 year home confinement; \$12.8 million forfeiture
David Liew	Guilty plea with cooperation	2017	Pending
Jiongsheng Zhao	Guilty plea with cooperation	2018	Time served
Andre Flotron	Not guilty following trial	2018	--
John Edmonds	Guilty plea with cooperation	2018	Pending
Kamaldeep Gandhi	Guilty plea with cooperation	2018	Pending
Krishna Mohan	Guilty plea with cooperation	2018	Pending
Edward Bases	Trial scheduled for July 2021	2018	--
John Pacilio	Trial scheduled for July 2021	2018	--
Jitesh Thakkar	Not guilty following trial	2019	--
Corey Flaum	Guilty plea with cooperation	2019	Pending
Christian Trunz	Guilty plea with cooperation	2019	Pending
Xiasong Wang	Pending (No trial date set)	2019	--
Jiali Wang	Pending (No trial date set)	2019	--
Gregg Smith	Trial scheduled for October 2021	2019	--
Michael Nowak	Trial scheduled for October 2021	2019	--
Christopher Jordan	Trial scheduled for October 2021	2019	--
Jeffrey Ruffo	Trial scheduled for October 2021	2019	--
James Vorley	Guilty following trial (appeal pending)	2020	Pending
Cedric Charu	Guilty following trial (appeal pending)	2020	Pending

UNITED KINGDOM

INTRODUCTION

Unlike the US, the UK does not have any statutes that expressly prohibit spoofing. Nevertheless, as the DOJ and SEC showed in the cases discussed above, a specially designed anti-spoofing provision is not a prerequisite for regulatory action. And importantly, there are various statutes already on the books in Britain that reach spoofing-type conduct.

For example, the Financial Services Act 2012 (FSA) section 89 makes it an offense for a person to “make a statement or to conceal facts with the intention of inducing another person . . . to enter into, or to refrain from entering into, a relevant agreement.” Similarly, FSA section 90 prohibits “engag[ing] in any course of conduct which creates a false or misleading impression as to the market in or the price or value of any relevant investments” if it was intentionally or recklessly done to (1) create such an impression and (2) “induce another person to acquire, dispose of, subscribe for or underwrite” an investment.

Likewise, section 2 of the Fraud Act 2006 makes it illegal to “dishonestly make a false representation” that is intended to benefit the statement maker or another, or cause losses to the person to whom it was made. Per the UK Supreme Court’s 2017 ruling in *Ivey v Genting Casinos* [2017] UKSC 67, dishonesty is adjudged on an objective basis only—that is, an individual can be found guilty of fraud so long as the evidence proves they were dishonest by the standards of an ordinary, reasonable individual. And reflecting Judge Tharp’s conclusion in *Vorley* that US law allows

wire fraud to be proven with “implied representations” only (see above), UK courts have determined that a “representation” under the Fraud Act can be express or implied “and may be regarded as made if it is submitted in any form to any system or device.”

Finally, Article 15 of the Market Abuse Regulation (MAR) broadly prohibits market manipulation and attempted market manipulation. Under MAR Article 12, manipulative activity can include placing orders which: (1) are likely to give false or misleading signals as to the supply of, demand for, or price of a financial instrument or related spot commodity contract; and/or (2) secures the price of one of a financial instrument or related spot commodity contract at an abnormal or artificial level.

The availability of these enforcement tools, combined with the various London-based securities and commodities exchanges, suggest that the UK is primed to follow the US’ lead in aggressively targeting spoofing. And in fact, earlier this year the FCA’s executive director of enforcement and market oversight highlighted the agency’s increasing data-processing capabilities by noting that it received over 150 million order reports every trading day in 2019. As seen in the evolution of spoofing enforcement in the US, more trade data in the hands of regulators will inevitably lead to more trading activity being flagged for further investigation and possible prosecution.

THE FCA AND OFGEM TAKE ACTION AGAINST MARKET MANIPULATION

While there have not yet been any criminal spoofing cases in Britain, the Financial Conduct Authority (FCA) and Office of Gas and Electricity Markets (Ofgem)²² used their regulatory powers this year to impose stiff fines on those who undertake market manipulation practices in the UK. The FCA announced on September 16, 2020 that it imposed a £100,000 fine against Corrado Abbattista, a trader at Fenician Capital Management LLP in London.²³ According to the FCA, for several months in 2017 Abbattista “placed large orders (by reference to the average order size in those shares in the market at that time) for CFDs²⁴ . . . which he did not intend to execute (the ‘Misleading Orders’), on the opposite side of the order book to existing smaller orders which he intended to execute (the ‘Genuine Orders’).” These orders allegedly allowed Abbattista to “falsely represent to the market an intention to buy/sell when his true intention was the opposite” in violation of Article 15 of the Market Abuse Regulation. Abbattista has appealed the FCA’s determination to its Upper Tribunal.

Irrespective of the Upper Tribunal’s eventual decision, this case is notable because it shows British regulators are making spoofing investigations a priority. As it noted in its press release: “The trading undertaken by Mr Abbattista was initially identified by the FCA’s internal surveillance systems. The FCA ingests order book data from the leading UK equity trading venues and then runs surveillance algorithms, designed to identify potentially abusive behaviours, across that consolidated data set.”²⁵ So just as US law enforcement has expanded its data analytics capabilities to aggressively target spoofing, it appears that the FCA is moving in the same direction. Indeed, as

of March 2020, the FCA disclosed that it had at least 5 spoofing investigations, and 29 market manipulation cases open.²⁶

And although Abbattista was based in London, UK authorities, like their analogues in the US, have shown a willingness to go after firms and individuals who trade on UK markets from abroad. Going back to 2011, for example, the FCA’s predecessor (the FSA) obtained an injunction and £8 million fine against Swift Trade for spoofing activity by its traders based in Switzerland and Hungary. Similarly, in July 2013, the FCA fined US-based Michael Coscia \$903,178 for market manipulation of commodities futures on the UK’s ICE Futures Europe Exchange, before parallel proceedings against him were initiated in the US.

More recently, in September 2019 Ofgem fined French company Engie Global Markets €2.3 million for manipulative spoofing on the wholesale gas markets and in March of this year imposed a record £37 million fine against InterGen Group to recompense the losses suffered by the National Grid Electricity System Operator from a breach of REMIT Article 5 (see below).

Whilst UK regulators have shown notably less zeal than their US counterparts in going after spoofing, the record fine recently imposed by Ofgem against InterGen and the FCA’s declaration that it has 29 active cases open this year, sends a strong message that enforcement action will continue to be taken against such activities. At the same time, however, the recent case of *Burford Capital -v- London Stock Exchange* in the Commercial Court²⁷ reveals that it is not always possible to conclude wrongdoing has taken place. Therefore, whether any of the FCA’s pipeline cases will actually involve the enforcement of criminal powers, or the continued use of civil powers, remains to be seen.

EUROPEAN UNION

INTRODUCTION

The UK's MAR is modeled on the EU's Regulation No 596/2014 (Reg 596), which was passed on April 16, 2014. In the preamble to this legislation, the European Parliament underlined its intention to strictly regulate spot and derivative markets, with a particular focus on cross-market manipulation:

Spot markets and related derivative markets are highly interconnected and global, and market abuse may take place across markets as well as across borders which can lead to significant systemic risks. . . . [M]anipulative strategies can extend across spot and derivatives markets. Trading in financial instruments, including commodity derivatives, can be used to manipulate related spot commodity contracts and spot commodity contracts can be used to manipulate related financial instruments. The prohibition of market manipulation should capture these inter-linkages.²⁸

In Article 12(2)(c), Reg 596 specifies that conduct will be considered manipulative if it involves “the placing of orders to a trading venue, including any cancellation or modification thereof, by any available means of trading, including by electronic means, such as algorithmic and high frequency trading strategies, and which” (i) disrupts or delays “the functioning of the trading system of the trading venue,” (ii) makes it “more difficult for other persons to identify genuine orders on the trading system,” or (iii) creates “a false or misleading signal about the supply of, demand for, or price of, a financial instrument, in particular by entering orders to initiate or exacerbate a trend.”

In supplemental legislation, the EU provided additional guidance on market activity that would be considered indicative of spoofing. For example, the guidance describes spoofing/layering as follows: “Submitting multiple or large orders to trade often away from the touch on one side of the order book in order to execute a trade on the other side of the order book. Once the trade has taken place, the orders with no intention to be executed shall be removed.”²⁹

The guidance also states that manipulative behavior may be indicated by: “Entering of orders which are withdrawn before execution, thus having the effect, or which are likely to have the effect, of giving a misleading impression that there is a demand for or supply of a financial instrument [or] related spot commodity contract – usually known as ‘placing orders with no intention of executing them.’”³⁰

The guidance goes on to note that this practice “may be illustrated by the following additional indicators”:

- “Orders to trade inserted with such a price that they increase the bid or decrease the offer, and have the effect, or are likely to have the effect, of increasing or decreasing the price of a related financial instrument.”
- “Entering orders to trade or a series of orders to trade, or executing transactions or series of transactions, likely to start or exacerbate a trend and to encourage other participants to accelerate or extend the trend in order to create an opportunity to close out or open a position at a favourable price — usually known as momentum ignition. This practice may also be illustrated by the high ratio of cancelled orders (e.g. order to trade ratio) which may be combined with a ratio on volume (e.g. number of financial instruments per order).”

EUROPEAN REGULATORS TARGET SPOOFING IN ENERGY MARKETS

Regulation on Wholesale Energy Market integrity and Transparency (“REMIT”) is an EU regulation on energy market integrity and transparency.³¹ In force since 28 December 2011, it provides a consistent EU-wide regulatory framework specific to wholesale energy markets, and creates an important framework for identifying and penalising market abuse in the UK and across the rest of Europe.

REMIT is enforced by the FCA and Ofgem in the UK, and the Agency for the Co-operation of Energy Regulators (ACER) and other national regulatory authorities (NRAs) across Europe.

Article 5 of REMIT specifies that any engagement in, or attempt to engage in, market manipulation on wholesale energy markets shall be prohibited. Article 2 of REMIT defines market manipulation as:

- a) entering into any transaction or issuing any order to trade in wholesale energy products which:
 - (i) gives, or is likely to give, false or misleading signals as to the supply of, demand for, or price of wholesale energy products;
 - (ii) secures or attempts to secure, by a person, or persons acting in collaboration, the price of one or several wholesale energy products at an artificial level, unless the person who entered into the transaction or issued the order to trade establishes that his reasons for doing so are legitimate and that that transaction or

order to trade conforms to accepted market practices on the wholesale energy market concerned; or

- (iii) employs or attempts to employ a fictitious device or any other form of deception or contrivance which gives, or is likely to give, false or misleading signals regarding the supply of, demand for, or price of wholesale energy products.

In March 2019, ACER, the European Agency which oversees the REMIT, provided guidance on trading behaviours associated with layering and spoofing.³² This continues a trend of developing guidance relating to market manipulation issued by ACER.

This was ACER's third guidance note on market abuse, and provides a non-exhaustive list of indicators it will use to identify trading behaviours associated with layering and spoofing. Indicators include the size, price, duration, status, pattern and repetition of orders. It goes on to explain that mere intention of a market participant to give signals or positions that artificially affect the price is sufficient to amount to attempted market manipulation, and that the actual giving of false or misleading signals or price placing is not necessary.³³

The first fines applied for REMIT breaches in the EU were imposed in Spain. Back in December 2015, Spain's competition and market regulator (CNMC) fined Iberdrola €25 million for a breach of Article 5 of REMIT (market manipulation in the energy sector).

A more recent example of sanctioning for manipulative behaviour of the type viewed as layering/spoofing in the EU is a fine of one million euros imposed on BP Gas Marketing Limited. In its decision published on January 16, 2020³⁴, the Dispute Settlement and Sanctions Committee

(CoRDIS) of the French Energy Regulatory Commission (CRE) held that the company BP Gas Marketing Limited (BPGM) engaged in market manipulation on the French Southern virtual Gas Trading Point (PEG Sud) between October 1, 2013 and March 1, 2014. CoRDIS found that, during 56 instances spread over 37 trading days, BPGM engaged in market manipulation consisting of a combination of trading behaviours including:

- layering a minimum of three sell orders throughout the trading day while placing iceberg orders hiding important volumes on the buy side of the order book;
- back-and-forth transactions within a short period of time that did not seem to have a rational economic justification; and
- large cancellation or price lag of its sell orders (placing orders at a price far from the bid/ask spread to avoid their execution).

According to CoRDIS, BPGM's behaviour was likely to send false or misleading signals to the market as to the supply and demand, thus breaching Article 5 of REMIT which prohibits market manipulation.³⁵

This decision follows a previous CoRDIS decision from October 2018 imposing a € 5 million fine on the company VITOL S.A. for engaging in a similar type of market manipulation on the PEG Sud.

IMPACT OF BREXIT

As with anything having to do with Europe, the impact of Brexit on market manipulation regulation must be considered. On the January 31, 2020, the UK left the EU and, following ratification of the Withdrawal Agreement, a transition period came into force. During the transition period the current Great Britain wholesale general market rules and REMIT arrangements remain in force. The transition period will run until the end of 2020. In an open letter to the wholesale energy market participants in Great Britain, Northern Ireland and the EU, dated 13 October 2020,³⁶ Ofgem provided market participants with an update on the REMIT arrangements that will apply in Great Britain after the transition period comes to an end.

The key measure of this open letter was to confirm to market participants that, regardless of whether a future partnership agreement is reached between the UK and the EU, they expect the REMIT enforcement regulations, which give Ofgem the power to investigate and enforce REMIT breaches, will continue and that key REMIT definitions relating to market manipulation shall remain the same.

CONTACTS

For more information, please visit our website, www.rahmanravelli.co.uk, or contact one of the lawyers below.



Joshua Ray

London

+44 (0) 758 753 3599

joshua.ray@rahmanravelli.co.uk



Neil Williams

London

+ 44 (0) 203 910 4560

neil.williams@rahmanravelli.co.uk



Nicola Sharp

Halifax

+ 44 (0) 203 910 4567

nicola.sharp@rahmanravelli.co.uk



Josie Welland

London

+ 44 (0) 203 947 1539

josie.welland@rahmanravelli.co.uk

ENDNOTES

- ¹ CFTC Release No. 8196-20, <https://www.cftc.gov/PressRoom/PressReleases/8196-20>
- ² CFTC Strategic Plan 2020-2024, p. 8.
- ³ The ASP defines spoofing as “bidding or offering with the intent to cancel the bid or offer before execution.” 7 U.S.C. § 6c(a)(5).
- ⁴ Icebergs are permitted on most futures exchanges and allow traders to conceal the full volume of an order placed in the order book. For example, if a trader wants to buy a total of 100 lots, the trader can place a 100 lot iceberg order that reveals only one lot at a time.
- ⁵ In re. Hard Eight Futures, LLC, CFTC Docket No. 19-30 (Sept. 30, 2019).
- ⁶ DOJ brought parallel charges against two of the defendants for criminal conspiracy to commit securities fraud, which remain pending. *United States v. Wang*, 19-mj-06485 (D. Mass.).
- ⁷ See below for a full list of publicly disclosed criminal spoofing cases brought by DOJ to date.
- ⁸ *United States v. Thakkar*, 18-cr-00036 (N.D. Ill.).
- ⁹ With the JPMorgan DPA, DOJ shattered its previous monetary recovery in a spoofing case set by the \$67,400,000 DPA with Tower Research Capital LLC in 2019. *United States v. Tower Research Capital LLC*, 19-cr-00819 (S.D. Tex.).
- ¹⁰ *Vorley*, 18-cr-00035, Docket No. 119, at p. 5.
- ¹¹ *Id.*, at p. 6.
- ¹² *Id.*, Docket No. 231.
- ¹³ *Id.*, Trial Tr. (Sept. 25, 2020) at 2317-18.
- ¹⁴ *United States v. Bases and Pacilio*, 18-cr-00048 (N.D. Ill.).
- ¹⁵ *Id.*, Docket No. 301 at 1.
- ¹⁶ *Id.* at 2.
- ¹⁷ *d.*, Docket No. 366.
- ¹⁸ Under US law, an indictment can be dismissed if it joins two or more offenses in the same count. Fed. R. Crim. P. 12(b)(3)(B). Duplicity is considered a fatal defect because it creates a situation where “the jury cannot in a general verdict render its fining on each offense, making it difficult to determine whether a conviction rests on only one of the offenses or both.” *United States v. Buchmeier*, 255 F.3d 415, 425 (7th Cir. 2001).
- ¹⁹ *United States v. Smith, et al.*, 19-cr-00663 (N.D. Ill.). A fourth defendant, Jeffrey Ruffo, a former JP Morgan salesperson, was added in a superseding indictment.
- ²⁰ *Id.*, Docket No. 114.
- ²¹ Ofgem is a non-ministerial government department and independent National Regulatory Authority, recognised by EU Directives.
- ²² FCA Decision Notice (July 22, 2020), <https://www.fca.org.uk/publication/decision-notice/corrado-abbattista-2020.pdf>.
- ²³ A “CFD,” or “contract for difference,” is basically a futures contract: they are “an agreement between a customer and a financial institution where the difference in the value of a specified asset at the beginning and end of the contract is exchanged.” *Id.*
- ²⁴ www.fca.org.uk/news/press-releases/fca-publishes-decision-notice-against-corrado-abbattista-market-manipulation.
- ²⁵ www.fca.org.uk/data/enforcement-data-annual-report-2019-20.
- ²⁶ In a judgement handed down by Andrew Baker J on 15 May 2020, in which an application for an Norwich Pharmacal Order made by Burford was refused, it revealed that the FCA had found no wrongdoing following its investigation into allegations that Burford's shares had been the subject of a (lawful) short-selling attack by Muddy Waters, a US investment advisory business on 6 and 7 August 2019.
- ²⁷ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014R0596>.
- ²⁸ Annex II to Commission Delegated Regulation (EU) 2016/522 of 17 December 2015, at paragraph 5(e).
- ²⁹ *Id.* at paragraph 6(a).
- ³⁰ No 1227/2011
- ³¹ Guidance Note 1/2019 on the application of Article 5 of REMIT on the prohibition of market manipulation layering and spoofing, 1st Edition.
- ³² *Id.* at paragraph 71.
- ³³ <https://energytradingregulation.com/2020/01/20/bp-gas-marketing-ltd-fined-1m-eur-for-activity-on-french-gas-market>
- ³⁴ CoRDIS' decision is subject to an appeal under the French national law
- ³⁵ https://www.ofgem.gov.uk/system/files/docs/2020/10/e_u_exit_remit_comms_-_oct_20_update_0.pdf

RAHMAN RAVELLI

London Office

Bridge House
181 Queen Victoria St
London EC4V 4EG
+44 (0)203 947 1539

Northern Office

Roma House, 59 Pellon Lane
Halifax, West Yorkshire
HX1 5BE
+44 (0)1422 346 666

Midlands Office

3 Brindley Place
Birmingham, West Midlands
B1 2JB
+44 (0)121 231 7025

www.rahmanravelli.co.uk

