JONES DAY

FEBRUARY 2016

COMMENTARY

Spotlight on Spoofing: Looking Back at 2015 and Forward to 2016

In 2014, regulators signaled that they would focus their efforts on investigating and prosecuting individuals engaged in spoofing. True to their word, 2015 saw the nation's first criminal conviction of a trader for spoofing in the U.S., as well as an increase in civil enforcement actions against traders who allegedly engaged in spoofing. Securities and futures exchanges also ramped up their efforts to detect, deter, and punish spoofing. The expectation is that regulators and self-regulatory organizations will continue to actively monitor the markets using increasingly sophisticated technology to detect spoofing. This is likely to lead to an increase in the number of enforcement actions and prosecutions for spoofing in 2016.

What Is "Spoofing"?

Spoofing can take many different forms. Typically, spoofing involves a trader placing a large number of buy or sell orders that he never intends to complete for the purpose of artificially inflating or lowering the market price of a security, futures contract, or other financial instrument that is traded on an exchange.[1] Once the market moves, the trader immediately cancels his open orders and takes advantage of the artificially high or low price with orders on the opposite side of the market that he intends to close out.[2] While spoofing and other types of market manipulation have occurred for years, regulators and exchanges have seen an increase in spoofing during this age where trading is dominated by high frequency and algorithmic trading.[3]

Activity that regulators and self-regulatory organizations may focus on in connection with their efforts to detect spoofing include the following: (1) layered or lopsided orders, (2) "flashed" orders that appear designed to move a flat market, (3) a pattern of orders being entered and cancelled prior to execution, (4) a high ratio of cancelled orders to executed trades relative to other traders, (5) a high ratio of modified orders relative to other traders, (6) cancelled orders that are relatively large to the average order size of the security or futures contract, (7) cancelled orders that are close to the best bid/offer, (8) order cancellations that occur a short time after being entered, (9) a concentration of modified or cancelled orders during certain windows during the trading day, or (10) an atypical concentration of orders within an order book.

Regulators often use anti-fraud and anti-manipulation statutes to punish spoofing.[4] For example, the Securities and Exchange Commission ("SEC") pursues actions against alleged spoofers under the anti-fraud provisions of Section 10(b) of the Securities Exchange Act of 1934, SEC Rule 10b-5, and Section 17(a) of the Securities Act of 1933.[5] The U.S. Department of Justice ("DOJ") also can use the mail and wire fraud statutes to punish spoofers.

When Dodd-Frank was signed into law on July 21, 2010, the Commodity Futures Trading Commission ("CFTC") received a new tool explicitly addressing spoofing. Dodd-Frank amended the Commodity Exchange Act ("CEA") and expressly made spoofing in the commodity futures markets a violation of federal law.[6] Specifically, 7 U.S.C. § 6c(a)(5)(C) makes it "unlawful for any person to engage in any trading, practice, or conduct on or subject to the rules of a registered entity that…is, is of the character of, or is commonly known to the trade as, 'spoofing' (bidding or offering with the intent to cancel the bid or offer before execution)."[7] On May 28, 2013, the CFTC released interpretive guidance regarding what would be considered spoofing.[8] According to the CFTC, "a market participant must act with some degree of intent to violate the 'spoofing' provision. Reckless trading, practices, or conduct would not violate [the prohibition on 'spoofing']."[9] The CFTC went on to say that "orders, modifications, or cancellations would not be considered 'spoofing' if they were submitted as part of a legitimate, good-faith attempt to consummate a trade…[L]egitimate good-faith cancellations of partially filled orders would not violate [the] CEA."[10]

The definition of spoofing received further refinement in connection with the criminal prosecution of Michael Coscia for spoofing in the U.S. District Court for the Northern District of Illinois. In *U.S. v. Coscia*, the court had to define spoofing in its jury instructions. The court instructed the jury as follows:

> "Spoofing" is defined as "bidding or offering with the intent to cancel the bid or offer before execution." To find this element satisfied, you must find the government has proven beyond a reasonable doubt that, at the time [the trader] entered the bid or offer specified in the Count that you are considering, he intended to cancel the entire bid or offer before it was executed, and that he did not place the bid or offer as part of a legitimate, good faith attempt to execute at least part of that bid or offer. The government must prove that [the trader] had the purpose or conscious desire to cancel his bid or offer before it was executed. It is not, however, sufficient for the government to prove that [the trader] knew or should have known that the consequence – that is, cancellation of the bid or offer before execution – was substantially likely to occur.[11]

Major Spoofing-Related Events in 2015

In 2015, spoofing was a popular "buzz word" in the financial markets. It received a great deal of attention in the financial press due to a perceived increase in regulatory activity focused on spoofing. The following are highlights of the major spoofing-related events of 2015. These events demonstrate the various types of trading strategies that regulators are focused on, the range of markets that regulators are monitoring, and the multiple enforcement tools at both the state and federal level that regulators may use to investigate and police potential acts of spoofing.

The Michael Coscia Prosecution and Conviction

On November 3, 2015, after settling civil cases with the CFTC, Financial Conduct Authority ("FCA"), and Chicago Mercantile Exchange ("CME") totaling $3.1 million in fines and $2.7 million in disgorgement, Michael Coscia became the first person in the United States to be convicted for the crime of spoofing.[12] Coscia's jury trial lasted seven days. The government called several witnesses, including traders from other firms, representatives from multiple exchanges, and a programmer hired by Coscia to develop his trading algorithm.[13] After just over an hour of deliberation, the jury found Coscia guilty on six counts of spoofing under the CEA.[14] At the close of the trial several things became clear:

- To satisfy its burden of proof in a criminal case, the government must show, at a minimum, that a defendant had *intent* to engage in spoofing, not merely that he cancelled a bid or offer prior to execution. The government also must show that a defendant intended to cancel the entire bid or offer before it was executed, and that the bid or offer was not part of a good-faith attempt to execute a part of the bid or offer.[15]
- To prove the requisite intent, it is unlikely that the government can rely merely on presenting cancelled orders themselves as evidence. It is likely that the government will need additional evidence to show that a trader

intended to spoof the market. The *Coscia* prosecutors relied on the testimony of a programmer who created the algorithms at Coscia's direction. The programmer also referred to notes indicating Coscia wanted the trading algorithms to "pump the market."[16]

- The DOJ only pursued six instances of spoofing against Coscia, which resulted in an alleged profit of only $1,070.00, indicating prosecutors are more concerned about the ease with which spoofing can be repeated rather than the total gain realized from the allegedly illegal trades.[17]

Navinder Sarao

In April of 2015, the DOJ charged Navinder Singh Sarao, a London-based high frequency trader, with 21 criminal counts relating to fraud and market manipulation in connection with the so-called "Flash Crash" on May 6, 2010.[18] At the same time, the CFTC also charged Sarao with price manipulation and spoofing.[19] On May 6, 2010, nearly $1 trillion in value was erased from U.S. stocks in minutes. This event, often referred to as the Flash Crash, saw the Dow Jones Industrial Average drop 998.5 points within a few minutes.[20] The DOJ alleged that Sarao was "significantly responsible" for the Flash Crash due to his spoofing of the E-mini S&P 500 near month futures contract.[21] There are several key takeaways from the Sarao indictment:

- Sarao's activities on May 6, 2010 occurred prior to implementation of Dodd-Frank, which took effect in July 2010, yet prosecutors are vigorously pursuing criminal charges against him. The Sarao case demonstrates that while Dodd-Frank specifically addresses spoofing in the futures markets, federal prosecutors will continue to rely on pre-Dodd-Frank anti-market manipulation and anti-fraud laws to pursue spoofers when necessary.[22]
- Even with regulators and prosecutors focusing their efforts on pursuing spoofers, oftentimes it takes investigators years to gather the evidence needed to prosecute a spoofer. In this case, even though Sarao's trading activity had been flagged as suspicious in 2010, it still took prosecutors five years to bring forth any charges.[23]
- Federal prosecutors view the reach of their anti-spoofing toolkit as extending to trading occurring in U.S. markets by offshore participants.

Igor Oystacher

In November of 2015, the CFTC filed a motion in federal court to prohibit Igor Oystacher, the founder of 3Red Trading LLC, from trading futures contracts until its civil case against him was resolved.[24] Prior to this, the CFTC had accused him of spoofing on 51 days from December 2011 through January 2015.[25] In addition to the CFTC investigations, in June 2015, Intercontinental Exchange, Inc. ("ICE)" penalized Oystacher for allegedly spoofing the market for its Russell 2000 Mini Futures contract.[26] The CME also penalized Oystacher which ordered him to pay $275,000 in fines and temporarily banned him from trading.[27] Oystacher now faces a DOJ investigation as well.[28] What separates Oysatcher from Coscia and Sarao is that Oystacher appears to have made all of his own trading decisions, and he would only have orders on one side of the market at a time; never did he have simultaneous bid and offer orders outstanding.

Rather than using trading algorithms, Oystacher made all his own trades by pointing and clicking with his mouse; he did however allegedly use commercially available software that cancelled existing orders on one side of the market before he could place orders on the opposite side, allowing him to quickly flip his orders from one side to the other. The Oystacher investigations and trading activity reveal the following:

- Spoofing activity is not limited to high-frequency traders, nor trading algorithms. Traders can use commercially available technology combined with traditional methods of online trading to achieve the same effect.
- Oystacher's actions did not actually move the price of the contracts he was trading, rather Oystacher is accused of creating a "false impression of market depth and book pressure" with his initial orders, which gave him an unfair advantage when he flipped his orders "before other market participants could assess and react to the disappearance of the false market and book pressure."[29]
- Regulators are sensitive to any behavior that may manipulate the market, even if that behavior does not constitute traditional spoofing.
- It may be difficult for the government to show the requisite intent in a case like Oystacher's given the fact that

he did not move the market price and could merely have been reacting to what he perceived was a change in the market.

The Martin Act and the FX Markets

In November 2015, New York Attorney General ("NYAG") Eric Schneiderman issued subpoenas to multiple interdealer brokers.[30] These subpoenas, which the NYAG issued pursuant to the powers granted to him under the Martin Act, are part of an investigation into whether these brokers used fake bids and offers in Foreign Exchange ("FX") options to distort the market and create interest in largely illiquid emerging-market currencies.[31] This latest state investigation reveals several important points:

- Federal regulators are not the only ones focused on spoofing; state regulators are focused on spoofing as well.
- The NYAG believes his statutory powers under the Martin Act are broad enough to regulate spoofing in otherwise unregulated markets like the FX market.

DaVinci

Last year also saw a crackdown on spoofing in the United Kingdom where there were high-profile actions brought against traders engaged in "layering," which is a specific type of spoofing. In August of 2015, U.K. Regulators won a £7.6 million decision against a Swiss investment firm and three Hungarian traders engaged in layering.[32] The FCA accused DaVinci Invest Ltd. of submitting a mixture of large and small orders on one side of the order book in order to create a false impression of supply and demand of a particular security.[33] The large orders were placed at a price close enough to the best bid or offer at the time to give a false sense of supply, but far enough away to minimize the chances they were executed.[34] The smaller orders, submitted in increasing or decreasing prices, were designed to improve the bid or offer price. As the price moved, further large orders were placed.[35] Once the price moved to where the traders were satisfied, they would cancel the orders and place orders on the other side of the order book in order to take advantage of the new prices.[36] The DaVinci proceeding illustrates several important facts:

- The crackdown on spoofing is not limited to U.S. markets; foreign regulators are also using the tools at their disposal to detect and prosecute spoofing.
- Spoofing can be accomplished in a variety of ways, but all of these tactics involve the placing of orders that are not intended to execute.

SEC Enforcement Actions

On December 3, 2015, the SEC brought fraud and spoofing charges against three Chicago-based traders under Section 17(a) of the Securities Act of 1933, as well as Sections 9(a)(2) and 10(b) of the Exchange Act of 1934, and SEC Rule 10b-5.[37] The SEC alleged that brothers Behruz and Shahryar Afshar, and their friend, Richard Kenny, used spoofing techniques to take advantage of a so-called "maker-taker" program offered by an options exchange that provides rebates for orders that are sent to an exchange and trade against a subsequently received order.[38] The rebate is designed to incentivize traders to bring liquidity to the market. By sending hidden All-Or-None ("AON") options orders and placing smaller, non-bona fide orders on the opposite side of the market the three were able to induce traders to place orders at the same price as the AON orders, allowing the three traders to match those orders and receive the maker rebate.[39] At the time of the alleged spoofing, options were bid at $7 and offered at $9. The traders put in 18 AON orders to sell 10 option contracts at $8 each, and then one public order to buy at $8. That single buy order caused others to put large buy orders in at $8, which executed against the 10 AON orders, allowing the Afshars and Kenny to collect the rebate.[40] The SEC's enforcement action against the Afshar brothers and Richard Kenny demonstrates several points:

- While Dodd-Frank may be the only regulatory framework that specifically references spoofing, the SEC views the 1933 and 1934 Acts as tools that can still be used against spoofers despite no provision outlawing "spoofing" by name.
- Regulators will scrutinize spoofers even if they place relatively small orders. In the SEC's view, small orders can distort the market because of the sensitivity of trading algorithms that react to even the smallest price changes in the market.[41]

Exchange Action and Technological Advances

During 2015, securities and futures exchanges redoubled their efforts to detect and punish spoofing when it occurs, while trying not to prevent market participants from engaging in legal trading practices. For example, in January 2015, ICE Futures US issued a publication entitled: "Disruptive Trading Practices: FAQs" that provides guidance to market participants designed to delineate between legitimate market practices and misconduct such as spoofing.[42] Several months later, in May of 2015, the CFTC directed CME to beef up its enforcement staff and to "develop strategies to identify instances of spoofing, and, as appropriate, pursue actions against perpetrators."[43]

Many believe that spoofing has become more widespread because "markets today are almost entirely electronic, and algorithms aren't as savvy as their flesh-and-blood counterparts."[44] This has led exchanges to deploy advanced technology to assist with their policing efforts. For example, exchanges have begun using computer software to identify suspicious trading activity that may warrant further investigation.[45] Nasdaq uses SMARTS trade surveillance technology to root out suspicious activity in the European and U.S. exchanges.[46] Other exchanges have turned to third-party developers for monitoring software. One such developer, Vertex Analytics, has created a graphics software that is used to detect spoofing.[47] Such technology has been tested by exchanges. The software is able to graphically represent every order and transaction in a market, making review of the transactions more efficient.[48]

Understandably, many exchanges do not want to divulge to the public what technology, software, and processes they are implementing to help detect spoofing. If market participants with nefarious intentions know what technology or software an exchange is using, they can adjust their trading patterns to defeat the exchange's policing efforts. We also understand that exchanges have proprietary detection processes, and employ customized software and technology to help detect spoofing. These technological developments have the potential to change the manner in which spoofing is prosecuted.

In addition to new technology, exchanges are seeking the implementation of new rules in order to police spoofing. For example, in July of 2015 BATS Global Markets Inc. proposed what it called the BATS Client Suspension Rule.[49] Such a rule would allow an exchange operator to immediately issue a cease-and-desist order to a broker providing access to a suspected spoofer.[50] The broker would then have 15 days to appeal, and if the appeal was not successful, the broker would need to immediately deny access to the suspected spoofer or face removal from the market.[51] Such technological developments and rule proposals show:

- Exchanges recognize that they must detect and punish spoofing, but, at the same time, they must not confuse spoofing with legitimate sophisticated trading practices.
- Technology such as Smarts and Vertex Analytics graphics software could end the need to review reams of paper and trading data by hand to detect and establish that spoofing occurred. Therefore self-regulatory entities (and regulators) can act more quickly to punish spoofers.
- While these technologies do not show a traders' mental state, the data itself could be used to bolster arguments that a particular trader had no intent to execute certain orders.

2016 and Beyond

The events described above, and the rise of anti-spoofing technology, indicate that spoofing will continue to be in the headlines throughout 2016 and beyond. In fact, as we were preparing this article, the Financial Industry Regulatory Authority ("FINRA") announced it will begin grading firms based on the volume of spoofing and other manipulative trading that they allow through their systems.[52] FINRA envisions that it will provide brokers with reports showing potential spoofing, and that brokers will be expected to confirm whether wrongdoing has occurred.

It is clear that, going forward, firms must employ top-notch compliance systems and individuals who understand their firm's particular trading strategies, as well as the new regulatory regime. To keep their firms out of spoofing trouble, a compliance staff should have a detailed understanding of the instructions being given to their traders' computer programmers to ensure that algorithms under development comply with anti-spoofing laws. Instituting proactive spoofing compliance policies could help prevent spoofing from occurring. And, if the firm becomes the target of regulatory scrutiny, prophylactic compliance measures could help shape an investigation, and potentially mitigate any fine. Furthermore, legal departments and compliance staff should react promptly, and with the assistance of outside counsel, to respond to the new FINRA reports concerning spoofing and other regulatory inquiries.

Lawyer Contacts

For further information, please contact your principal Firm representative or one of the lawyers listed below. General email messages may be sent using our "Contact Us" form, which can be found at www.jonesday.com/contactus/.

Jason Jurgens
New York
+1.212.326.3771
jjurgens@jonesday.com

Stephen J. Obie
New York
+1.212.326.3773
sobie@jonesday.com

Mario J. Cacciola, an associate in the New York office, assisted in the preparation of this Commentary.

Endnotes

[1] Bradley Hope, *5 Things to Know About Spoofing in Financial Markets*, The Wall Street Journal (Feb. 22, 2015, 10:36 PM EST), http://blogs.wsj.com/briefly/2015/02/22/5-things-to-know-about-spoofing-in-financial-markets/.

[2] *Id*.

[3] Matthew Leising, *Spoofing Went Mainstream in 2015*, Bloomberg Business (Dec. 21, 2015, 7:00 PM EST), http://www.bloomberg.com/news/articles/2015-12-22/nabbing-the-rogue-algo-inside-the-year-spoofing-went-mainstream.

[4] Clifford C. Histed, *A Look At The 1st Criminal 'Spoofing' Prosecution: Part 1*, Law360 (Apr. 20, 2015, 12:01 PM ET), http://www.law360.com/articles/645167/a-look-at-the-1st-criminal-spoofing-prosecution-part-1.

[5] *Id*.

[6] *Id*.

[7] Commodity Exchange Act, 7 U.S.C. § 6c.

[8] 78 Fed. Reg. 31890, *available at* http://www.cftc.gov/idc/groups/public/@lrfederalregister/documents/file/2013-12365a.pdf.

[9] *Id*.

[10] *Id*.

[11] Jury Instructions, *USA v. Coscia*, No. 14 CR 00551, (N.D. Ill. Nov. 3, 2015).

[12] Jessica Corso, *High-Speed Trader Found Guilty In Landmark Spoofing Case*, Law360 (Nov. 3, 2015, 6:09 PM ET), http://www.law360.com/articles/722493/high-speed-trader-found-guilty-in-landmark-spoofing-case.

[13] Witness List, *USA v. Coscia*, No. 14 CR 00551 (N.D. Ill. Nov. 3, 2015).

[14] Jessica Corso, *High-Speed Trader Found Guilty In Landmark Spoofing Case*, Law360 (Nov. 3, 2015, 6:09 PM ET), http://www.law360.com/articles/722493/high-speed-trader-found-guilty-in-landmark-spoofing-case.

[15] Jury Instructions, *USA v. Coscia*, No. 14 CR 00551 (N.D. Ill. Nov. 3, 2015).

[16] Lynne Marek, *A First: Chicago Jury Convicts Trader in Widely Watched 'Spoofing' Case*, Crain's Chicago Business (Nov. 3, 2015), http://www.chicagobusiness.com/article/20151103/NEWS01/151109940/a-first-chicago-jury-convicts-trader-in-widely-watched-spoofing-case.

[17] Brian Lewis and Janan Hanna, *Swift Guilty Verdict in Spoofing Trial May Fuel New Prosecutions in U.S.*, Bloomberg Business (Nov. 3, 2015, 10:27 EST), http://www.bloomberg.com/news/articles/2015-11-03/commodities-trader-coscia-found-guilty-in-first-spoofing-trial.

[18] Everett Rosenfeld, *UK Trader Charged for Manipulation Contributing to 2010 Flash Crash*, CNBC (Apr. 21, 2015, 2:50 PM EST), http://www.cnbc.com/2015/04/21/futures-trader-charged-for-manipulating-stock-market-contributing-to-2010-flash-crash.html.

[19] *CFTC Charges U.K. Resident Navinder Singh Sarao and His Company Nav Sarao Futures Limited PLC with Price Manipulation and Spoofing*, CFTC (Apr. 21, 2015), http://www.cftc.gov/PressRoom/PressReleases/pr7156-15.

[20] Janet Whitman, *The Market's Wild Ride*, Montreal Gazette (May 5, 2010), http://www.montrealgazette.com/business/fp/markets+wild+ride/2994890/story.html.

[21] Everett Rosenfeld, *UK Trader Charged for Manipulation Contributing to 2010 Flash Crash*, CNBC (Apr. 21, 2015, 2:50 PM EST), http://www.cnbc.com/2015/04/21/futures-trader-charged-for-manipulating-stock-market-contributing-to-2010-flash-crash.html.

[22] *Id*.

[23] *Id*.

[24] Bradley Hope, *Regulators to Courts: Stop That Spoofer*, The Wall Street Journal (Nov. 10, 2015, 7:26 PM ET), http://www.wsj.com/articles/regulators-to-courts-stop-that-spoofer-1447201589.

[25] *Id*.

[26] Igor Oystacher Case Summery, National Futures Association, http://www.nfa.futures.org/basicnet/Case.aspx?entityid=0482612&case=2013-009&contrib=ICE.

[27] Matthew Leising, *The Man Accused of Spoofing Some of the World's Biggest Futures Exchanges*, Bloomberg Business (Oct. 19, 2015, 4:32 PM EDT), http://www.bloomberg.com/news/articles/2015-10-19/before-u-s-called-igor-oystacher-a-spoofer-he-was-known-as-990.

[28] *Id*.

[29] Paul Peterson, *Commodity Fraud: Who's Spoofing Who?*, AGFAX (Jan. 8, 2016), http://agfax.com/2016/01/08/commodity-fraud-whos-spoofing/.

[30] Keri Geiger, *Currency Spoofing Is Said to Be New York's Latest Target*, Bloomberg Business (Nov. 23, 2015, 10:27 AM EST), http://www.bloomberg.com/news/articles/2015-11-23/currency-spoofing-is-said-to-be-new-york-s-latest-target.

[31] *Id*.

[32] Kristin Ridley, *UK Regulator Wins £7.6 Million High Court 'Layering' Market Abuse Order*, Reuters (Aug. 12, 2015 BST), http://uk.reuters.com/article/uk-britain-financial-fca-idUKKCN0QH26C20150812.

[33] *FCA Secures High Court Judgment Awarding Injunction and over £7 Million in Penalties Against Five Defendants For Market Abuse* (Aug. 17, 2015), https://www.fca.org.uk/news/fca-secures-high-court-judgment-awarding-injunction-and-over-7-million-in-penalties.

[34] *Id*.

[35] *Id*.

[36] *Id*.

[37] SEC Press Release 2015-273, *available at* http://www.sec.gov/news/pressrelease/2015-273.html.

[38] *Id*.

[39] *Id*.

[40] Matt Levine, *Tricky Twins Spoofed Trading Computers*, Bloomberg View (Dec. 3, 2015, 6:53 PM EST), http://www.bloombergview.com/articles/2015-12-03/tricky-twins-spoofed-trading-computers.

[41] *Id*.

[42] *Available at* https://www.theice.com/publicdocs/futures_us/Futures_US_Disruptive_Practice_FAQ.pdf.

[43] Sarah N. Lynch, *CFTC Says CME Directed to Beef Up 'Spoofing Enforcement'*, Reuters (May 14, 2015, 4:22 PM EDT), http://www.reuters.com/article/us-cftc-cme-group-spoofing-idUSKBN0NZ1LW20150514.

[44] Matthew Leising, *Spoofing Went Mainstream in 2015*, Bloomberg Business (Dec. 21, 2015, 7:00 PM EST), http://www.bloomberg.com/news/articles/2015-12-22/nabbing-the-rogue-algo-inside-the-year-spoofing-went-mainstream.

[45] Edward Robinson, *Market Police Deploy New Weapons Against Spoofers*, Bloomberg Business (Dec. 28, 2015, 7:00 PM EST), http://www.bloomberg.com/news/articles/2015-12-29/in-algo-wars-market-police-deploy-new-weapons-against-spoofers.

[46] *Id*.

[47] Matthew Leising, *Spoofing Went Mainstream in 2015*, Bloomberg Business (Dec. 21, 2015, 7:00 PM EST), http://www.bloomberg.com/news/articles/2015-12-22/nabbing-the-rogue-algo-inside-the-year-spoofing-went-mainstream.

[48] *Id*.

[49] Matthew Perlman, *BATS Eyes New Rule to Fight Market Manipulators*, Law 360 (July 30, 2015, 1:45 PM ET), http://www.law360.com/articles/685221/bats-eyes-new-rule-to-fight-market-manipulators.

[50] *Id*.

[51] *Id*.

[52] Ed Beeson, *FINRA Aims to Teach a Lesson with Spoofing Report Cards*, Law360 (Jan. 5, 2016, 10:32 PM ET), http://www.law360.com/articles/742698.

Jones Day publications should not be construed as legal advice on any specific facts or circumstances. The contents are intended for general information purposes only and may not be quoted or referred to in any other publication or proceeding without the prior written consent of the Firm, to be given or withheld at our discretion. To request reprint permission for any of our publications, please use our "Contact Us" form, which can be found on our website at www.jonesday.com. The mailing of this publication is not intended to create, and receipt of it does not constitute, an attorney-client relationship. The views set forth herein are the personal views of the authors and do not necessarily reflect those of the Firm.