A Spoof of Justice: Double Jeopardy Implications for Convictions of Both Spoofing and Commodities Fraud for the Same Transaction

Abram Olychyk
American University Washington College of Law

Follow this and additional works at: https://digitalcommons.wcl.american.edu/aulr

Part of the Science and Technology Law Commons

Recommended Citation
Available at: https://digitalcommons.wcl.american.edu/aulr/vol65/iss1/5

This Comment is brought to you for free and open access by the Washington College of Law Journals & Law Reviews at Digital Commons @ American University Washington College of Law. It has been accepted for inclusion in American University Law Review by an authorized editor of Digital Commons @ American University Washington College of Law. For more information, please contact kclay@wcl.american.edu.
A Spoof of Justice: Double Jeopardy Implications for Convictions of Both Spoofing and Commodities Fraud for the Same Transaction

This comment is available in American University Law Review: https://digitalcommons.wcl.american.edu/aulr/vol65/iss1/5
A SPOOF OF JUSTICE: DOUBLE JEOPARDY IMPLICATIONS FOR CONVICTIONS OF BOTH SPOOFING AND COMMODITIES FRAUD FOR THE SAME TRANSACTION

ABRAM OLCHYK*

To the fastest go the spoils. The rise of automated algorithmic trading has transformed the American stock market into an institution prioritizing speed above all else. The relative chaos implicit in light-speed trading obscures the view of regulators, providing an enterprising new breed of traders ample opportunity to manipulate the market. The most recent scheme garnering the attention of state and federal agencies is known as spoofing, where a trader initiates a precise pattern of trades to lure in buyers or sellers—thereby raising or lowering the value of the commodity—trading on the distortion, then cancelling the baited trades before they fully execute.

In 2014, a federal grand jury indicted Michael Coscia on charges of criminal spoofing and commodities fraud. The indictment alleges Coscia spoofed several trades by entering into large buy contracts—for positions he held—to create a false sense of demand, selling off his positions at peak value, then cancelling the buy orders before they executed. Coscia's indictment focused on six transactions and contains a charge of both spoofing and commodities fraud—a more general securities fraud statute—for each. This Comment will make the novel argument that a conviction for both spoofing and commodities fraud for the same transaction could be challenged under a theory of double jeopardy as unconstitutionally duplicitous punishment. To do so, this Comment will analyze the spoofing and commodities fraud statutes

* Senior Staff Member, American University Law Review, Volume 65; J.D. Candidate, May 2016, American University, Washington College of Law; B.A. Political Science, 2012, Syracuse University. First, I would like to thank Professors Michael Carroll and Amy Tenney for their encouragement, dedication, and support in this endeavor. Additionally, I would like to thank my girlfriend Bonnie Jones for her unwavering patience and unlimited snacks. Finally, I would like to thank the American University Law Review staff for all their work in making this piece publishable.

239
to show that proof of the former will always prove the latter, and that, therefore, a defendant cannot be convicted of both for the same transaction.

TABLE OF CONTENTS

Introduction .................................................................................................................. 240
I. Background ............................................................................................................ 246
   A. Historical Overview of Spoofing Regulation .................. 246
   B. Commodities Fraud: A New Weapon From Sarbanes-Oxley .............................................. 248
   C. The Michael Coscia Indictment .................................. 249
   D. The Blockburger Test and Double Jeopardy Jurisprudence .................................................. 251
   E. Lex Generalis, Merger Doctrine, and the Rule of Lenity ................................................................. 255
II. A Criminal Indictment for Both Spoofing and Commodities Fraud for the Same Transaction Implicates Double Jeopardy ............................................ 258
   A. Spoofing and Commodities Fraud Under the Gavieres Mandate .............................................. 258
   B. A Comparison of the Spoofing and Commodities Fraud Elements Post-Gavieres Fails the Blockburger Sameness Test ....................................................... 264
   C. The Canons of Lex Specialis Derogat Lex Generalis and Merger Doctrine Show How Spoofing Operates as a Mechanical Subset of Commodities Fraud, Rather Than as a Different Act ........................................ 269

Conclusion ................................................................................................................ 272

"[T]he Constitution was designed as much to prevent the criminal from being twice punished for the same offence as from being twice tried for it."1

INTRODUCTION

In 2009, Daniel Spivey2 began laying cable.3 From Chicago, Illinois to Carteret, New Jersey in the most direct route possible, he laid the

---

2. Daniel Spivey is the founder, president, and CEO of Spread Networks ("Spread"). Dan Spivey, SPREAD NETWORKS, http://spreadnetworks.com/management/management-team/dan-spivey (last visited Oct. 26, 2015). He developed the idea of decreasing transmission time for stock and commodities orders by constructing a new, more direct
fiber optic cable aiming to provide high frequency stock traders active on both the New York and Chicago exchanges with the fastest available electronic connection between the two exchanges. If successful, the line would provide a trading speed unrivaled by those trading on traditional routes—and successful it was. The line, owned by the newly-created Spread Networks (“Spread”), trimmed 100 miles and three milliseconds—a relative eternity—off of the next fastest route. For reference, a human blink lasts roughly one tenth of a second, or 100 milliseconds. For just $300,000 per month with a few million up front, traders on Spread’s line now operate on exchanges so quickly that only a privileged few even have the technology to keep up. High-frequency trading firms now account

fiber optic cable to connect the exchanges in Carteret, New Jersey and Chicago, Illinois. Dark Fiber, SPREAD NETWORKS, http://spreadnetworks.com/products/dark-fiber (last visited Oct. 26, 2015). Spread Networks now sells access to that line. Id. 3. See Christopher Steiner, Wall Street’s Speed War, FORBES (Sept. 9, 2010, 10:00 AM), http://www.forbes.com/forbes/2010/0927/outfront-netscape-jim-barksdale-daniel-spivey-wall-street-speed-war.html (explaining how the cable’s advantage stems from its direct route from Chicago to Carteret as opposed to older cable routes that follow uneven railroad lines). 4. The New York Stock Exchange (NYSE) in its current iteration actually operates on a series of heavily guarded computer servers housed in Mahwah, New Jersey. See MICHAEL LEWIS, FLASH BOYS: A WALL STREET REVOLT 53 (2014) (tracing the disconnect between the historic image of the NYSE trading floor with how the exchange actually works). 5. See Steiner, supra note 3 (explaining that the new line’s straight trajectory between two cities allows it to transmit information much faster than older lines that paralleled indirect railroad lines). 6. Traditional fiber cable routes between Chicago and New York follow paths dictated by flat land, subject to restrictions prohibiting laying cable along interstate highways. When those routes meet the Allegheny Mountains in Pennsylvania, they begin to zigzag, increasing the line’s length and adding transmission time to trade requests. Spivey’s cable cut through the mountains to gain its sizable speed advantage. See LEWIS, supra note 4, at 10 (differentiating Spivey’s route from traditional cable routes). 7. See Steiner, supra note 3 (noting that Spread was the company that Spivey and his backers founded to operate the new line); see also Home, SPREAD NETWORKS, http://spreadnetworks.com (last visited Oct. 26, 2015) (asserting that Spread is “[t]he standard for reliable, high-bandwidth communications between New York and Chicago”). 8. See Steiner, supra note 3 (recognizing the fast speed of 13.3 milliseconds at which Spread’s line transmits from Chicago to New York, whereas the next fastest line transmits in 16.3 milliseconds and noting that in automated high frequency trading, three milliseconds, or three one-thousandths of a second, is an enormous window). 9. See Stephen Reucroft & John Swain, How Often and Why Do People’s Eyes Blink?, BOS. GLOBE (May 14, 2007), http://www.boston.com/news/science/articles/2007/05/14/how_often_and_why_do_peoples_eyes_blink. 10. See LEWIS, supra note 4, at 18 (explaining how the Spread line allowed high
for one half of all trading activity on U.S. stock exchanges. They wield advanced hardware that, when combined with powerful computer algorithms and blinding speed, allows for near-instantaneous trading free of human intervention. Effectively regulating high frequency trading presents the difficult task of managing an unfamiliar iteration of a bedrock American institution. So as Congress investigates the possibility of a comprehensive oversight structure, federal agencies are left to promulgate piecemeal and more targeted rules in the interim.

The proliferation of high frequency trading as exemplified by the success of Spread Networks gave rise to “spoofing,” the loosely frequency traders, who were already trading at an elite speed not publicly available, to operate at an even faster level).


defined practice of entering into a trade with the intent to cancel before execution. Spoofing is computer-on-computer crime: one trader programs his trading algorithm to make bids when certain market conditions present themselves, only to cancel the bids at such speed that other traders’ computers are left operating with incrementally outdated market positions. The miniscule window of time before the other computers self-correct allows the spoofer to trade on a slightly inflated (or deflated) market, creating a narrow profit margin. Spoofing regulation is still in its infancy; the Commodity Futures Trading Commission (CFTC), the regulator with jurisdiction over the commodities exchanges, only began issuing spoofing guidance in 2011, and other agencies are just beginning to understand the scope of spoofing activities.

Actual enforcement of spoofing regulations is younger still. The CFTC fined its first trader for spoofing in July 2013. His name was

18. See Henning, supra note 17 (explaining that spoofing can inflate the target’s price by creating the illusion of higher demand through fraudulent buy orders and deflate the price by creating the illusion of higher supply through fraudulent sell orders).
19. See About the CFTC, U.S. Commodity Futures Trading Commission, http://www.cftc.gov/About/index.htm (last visited Oct. 26, 2015) (stating that the mission of the Commodity Futures Trading Commission (“CFTC”) is to promote market integrity and ensure “the integrity of futures & options markets”). This Comment focuses on CFTC regulation of spoofing because of the Commission’s past involvement with Michael Coscia. See infra note 26 and accompanying text (emphasizing the CFTC’s past litigation with Coscia over his spoofing activities).
22. See McCrank, supra note 11 (noting that the SEC told its staff in March 2011 that it was interested in any “tips, complaints, or referrals” concerning high-frequency trading).
23. See Henning, supra note 17 (noting the new prosecutorial priority of prosecuting spoofing).
Michael Coscia, and the nearly $3.1 million in penalties levied by various entities on his company, Panther Energy Trading LLC, signaled a new willingness of regulators to investigate and punish spoofers. However, until very recently, penalties for spoofing remained civil in nature, consisting of mostly fines, profit disgorgements, and trading bans. But, in October 2014, the high-frequency trading industry was put on notice when a federal grand jury issued the first criminal indictment for spoofing.

The indictment involved a familiar party: Michael Coscia of Panther Energy Trading LLC. However, Coscia's indictment was unique in that his twelve criminal counts attached to only six total transactions. Each transaction involved carried one count of spoofing and one count of commodities fraud. As each transaction carried both charges, the question then arose: what is the difference between commodities fraud and spoofing? If Coscia is convicted on all counts, the answer to that question may render future convictions—where the defendant is charged with both spoofing and

25. Id.
26. See id. (calculating that of the $3.1 million in total penalties, $1.4 million came from a settlement with the CFTC, $800,000 from the Chicago Mercantile Exchange, and approximately $900,000 from the Financial Conduct Authority, a U.K. financial regulator).
27. See ElBoghdady, supra note 13 (describing new enforcement actions from the CFTC and the Financial Industry Regulatory Authority to address high-frequency trading).
28. See, e.g., In re Panther Energy Trading LLC, CFTC No. 13-26, 2013 WL 3817473 (July 22, 2013) (offering a settlement agreement with the agency consisting of admission of jurisdiction, waiver of hearing, judicial review, any claims of double jeopardy stemming from the civil penalty, consent to fines from the various involved agencies, and agreement to a one-year trading ban).
31. Id. at 1, 9–19.
32. Id.
commodities fraud—vulnerable to a constitutional challenge grounded in double jeopardy
jurisprudence.

This Comment will argue that defendants might successfully challenge convictions where both commodities fraud and spoofing charges attach to the same transaction under a theory of double jeopardy. It will argue that although commodities fraud and spoofing are two distinct statutory provisions, they fail the "same transaction" test established in \textit{Blockburger v. United States}, which prohibits multiple punishments for two charges where proof of one necessarily constitutes proof of the other. It will show that, once distilled into their simplified components, the elements of spoofing and commodities fraud overlap such that proving the former will always prove the latter. Additionally, this Comment will explore several canons of statutory construction to illustrate some relevant legal underpinnings to the \textit{Blockburger} rule.

Part I of this Comment will provide background on the nature and character of spoofing and commodities fraud charges. It will also provide an overview of the \textit{Blockburger} standard and subsequent iterations, as well as explore the relevant canons of statutory construction. Part II of this Comment will first interpret the elements of both charges in light of relevant case law to distill elements for comparison. It will then evaluate and analyze those elements in light of the \textit{Blockburger} test to show that proving a spoofing violation will always prove commodities fraud; therefore, a defendant may only constitutionally be convicted of one of the offenses for each transaction in a given indictment. Additionally, it will show how certain canons of statutory construction help illuminate the intent and application of the \textit{Blockburger} test.

\footnote{33. See U.S. CONST. amend. V (prohibiting any individual from being "subject for the same offense to be twice put in jeopardy of life or limb").}
\footnote{34. 284 U.S. 299 (1932).}
\footnote{35. See \textit{id.} at 303–04 (analyzing two sections of the Narcotics Act to determine "whether, both sections being violated by the same act, the accused committed two offenses or only one").}
\footnote{36. Specifically, this Comment will analyze the maxims of \textit{lex specialis derogat lex generalis} (specialized laws prevail over general laws), the "merger doctrine," and the rule of lenity. See Otto Kirchheimer, \textit{The Act, The Offense and Double Jeopardy}, 58 YALE L.J. 513, 517–18 (1949) (introducing the "speciality" principle as a type of offense scheme where concurrent application of different norms applies).}
I. BACKGROUND

A. Historical Overview of Spoofing Regulation

Spoofing regulation originated in the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank). Section 747 of Dodd-Frank amended the Commodity Exchange Act (CEA) to add a section governing trading activities deemed to be "Disruptive Practices." The Disruptive Practices section declares 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 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).

But, in an industry where upwards of ninety percent of all trades are cancelled before execution, uncertainty remains as to the exact scope of the regulation and as to the kinds of activities it is attempting to regulate. These questions were the subject of substantial discussion between regulators and industry representatives. Those discussions yielded guidance from the CFTC.

38. See id. (containing the initial language prohibiting spoofing); Commodity Exchange Act (CEA), 7 U.S.C. §§ 1-27f (2012).
39. See Dodd-Frank § 747 (amending the CEA to include identical language to the current spoofing statute).
40. Id.
41. See Scott Patterson & Andrew Ackerman, SEC May Ticket Speeding Traders; High-Frequency Firms Face Fees on Cancelled Transactions, WALL ST. J. (Feb. 23, 2012), http://www.wsj.com/articles/SB10001424052970203918304577239440668644280 (quoting the Tabb Group, an electronic trading tracking organization, to estimate that between ninety-five and ninety-eight percent of all trades made by high-frequency traders are cancelled before execution to adjust instantaneously to changing market conditions).
43. See generally Roundtable, supra note 42 (quoting several prominent members of the high frequency trading industry to show the lack of unified
clarifying that actionable spoofing includes both an element of scienter (intent to deceive) and a corresponding good faith defense.\textsuperscript{44} The guidance from the CFTC, published in the Federal Register in March 2011,\textsuperscript{45} addressed a variety of stock trading industry concerns over the parameters for spoofing regulation.\textsuperscript{46} Chief among these concerns was that CEA § 6c(a)(5)(C), which purported to regulate spoofing, actually provided little clarity as to a universally accepted definition.\textsuperscript{47} The resulting CFTC guidance provided a unifying concept—that spoofing necessarily incorporates an element of intent—which was followed by a patchwork of examples.\textsuperscript{48} Such vagaries and inconsistencies in definition persist even in common usage.\textsuperscript{49} Regardless of the uncertainty as to the exact parameters of spoofing, the central elements remain clear: bidding with the intent to cancel so as to deceive or otherwise manipulate other market participants or machinations.\textsuperscript{50}

\begin{itemize}
\item \textsuperscript{44} See Disruptive Practices Guidance, 76 FED. REG. at 14,947 (clarifying the Commission's view that spoofing requires a bad-faith intent to cancel, which accommodates a corresponding good faith trading defense).
\item \textsuperscript{45} Id. at 14,943.
\item \textsuperscript{46} See id. at 14,947 (noting in the introduction to the spoofing portion that the guidance responded to industry concerns about a lack of a unified definition of spoofing, the treatment of legitimate trading behavior, and possible exemptions for partial fill orders).
\item \textsuperscript{47} See Roundtable, supra note 42, at 64 (statement of Gary DeWaal, Newedge USA, LLC) ("I'm not sure of [sic] the definition of spoofing can be agreed upon by the ten people around this table."); see also id. at 111 (statement of Cameron Smith, Quantlab Financial, LLC) ("I wish I could give you a little pithy definition that would capture it all, but it's not easy.").
\item \textsuperscript{48} See Disruptive Practices Guidance, 76 FED. REG. at 14,947; see also Roundtable, supra note 42, at 28, 90, 93, 133 (listing practices such as submitting and cancelling bids, submitting and cancelling to overload the quotation system, submitting or cancelling bids to delay another's trading, and submitting or cancelling bids to create false market depth, as other examples of spoofing behavior).
\item \textsuperscript{49} Compare Henning, supra note 17 (defining spoofing as an act of attracting market participants by fooling them "into believing there are large orders for futures contracts"), with Gulino, supra note 29 (defining spoofing as a practice of placing and almost instantaneously canceling orders to, among other things, "gauge demand" and "set up opposing trades").
\item \textsuperscript{50} See Disruptive Practices Guidance, 76 FED. REG. at 14,947 (referencing the inclusion of the bidding with intent to cancel the mechanism in all identified spoofing practices); see also Roundtable, supra note 42, at 36 (statement of Adam Nunes, Hudson River Trading Group) (specifying that spoofing clearly must involve illegitimate trading behavior and an intent to manipulate).
\end{itemize}
B. Commodities Fraud: A New Weapon From Sarbanes-Oxley

The commodities fraud statute was enacted as part of the Sarbanes-Oxley Act in 2002. The fraud provision is triggered when a party knowingly executes, or attempts to execute, a scheme or artifice... (1) to defraud any person in connection with any commodity for future delivery, or... (2) to obtain, by means of false or fraudulent pretenses, representations, or promises, any money or property in connection with the purchase or sale of any commodity for future delivery...

The provision's language is purposefully broad so as to divorce its elements from more technical securities laws requirements and to give prosecutors a more versatile weapon to fight fraud.

Prosecutors apply the statute in a similar manner to the mail and wire fraud statutes. A prosecutor must first prove a violation of either subsection one or two, but not both, for there to be a violation. Even so, the elements of commodities fraud may be simply stated as only: (1) a fraudulent intent; (2) a scheme or artifice; and (3) a connection with a security.

The exact level of fraudulent intent required is of some dispute, as different courts have used a variety of standards to satisfy the

---

53. See Kathleen F. Brickey, From Enron to Worldcom and Beyond: Life and Crime After Sarbanes-Oxley, 81 Wash. U. L.Q. 357, 377 n.86 (2003) (noting the accepted interpretation that § 1348 of 18 U.S.C. is not to be read to require the technical elements of other securities fraud statutes); see also 148 Cong. Rec. S7421 (daily ed. July 26, 2002) (statement of Sen. Leahy) (discussing the intent behind § 1348, which was not to "require proof of technical elements from the securities laws," but rather to create a protection mechanism for the shareholders and prospective shareholders of publicly traded companies that has a flexible enforcement scheme to protect against "all the types [of] schemes and frauds [that] inventive criminals may devise in the future").
54. See 148 Cong. Rec. S7421 (daily ed. July 26, 2002) (statement of Sen. Leahy) (arguing that the use of the phrase all "schemes and artifices to defraud" is broad enough to allow prosecutors to adequately enforce the law despite future challenges to it).
55. See United States v. Mahaffy, No. 05-CR-613, 2006 WL 2224518, at *11 (E.D.N.Y. Aug. 2, 2006) (noting that since the language in § 1348 was drawn from the mail and wire fraud statutes, the court should construe § 1348 in a manner similar to those statutes); see also Don Mayer et al., Crime and Punishment (Or the Lack Thereof) for Financial Fraud in the Subprime Mortgage Meltdown: Reasons and Remedies for Legal and Ethical Lapses, 51 Am. Bus. L.J. 515, 527 (2014) (explaining that § 1348 was modeled after the mail and wire fraud statutes).
requirement. A "scheme or artifice" is generally thought of in terms of harm to the property rights of another. If the act caused economic harm, or would have had the plan been executed, then a scheme or artifice generally exists. Prosecutors also have broad leeway in connecting the scheme to a security, consistent with similarly broad interpretations of mail and wire fraud statutes.

C. The Michael Coscia Indictment

On October 1, 2014, an Illinois grand jury issued the first-ever criminal indictment for spoofing activities. Michael Coscia was the manager and sole owner of Panther Energy Trading LLC, a New Jersey-based trading firm engaged in speculating on a wide variety of commodities on Globex, a Chicago Mercantile Exchange (CME) electronic trading platform. Coscia was not new to government


59. See, e.g., Stinn v. United States, 856 F. Supp. 2d 531, 536 (E.D.N.Y. 2012), aff'd, 515 F. App'x 4 (2d Cir. 2013) (affirming jury instructions defining "scheme or artifice" as a "plan or course of action that intends some harm to the property rights of another"). Courts have traditionally recognized two types of schemes: those that qualify under the Stinn formulation and those that fall under the "honest services doctrine." See id. at 537 (differentiating the type of "scheme or artifice" in the jury instructions with that of the "honest services" doctrine); see also Skilling v. United States, 561 U.S. 358, 408–09 (2010) (limiting liability for depriving others of honest services only to cases involving bribes and kickbacks in a suit arising from the Enron collapse of 2001).

60. See, e.g., United States v. Chandler, 98 F.3d 711, 715 (2d Cir. 1996) (implying a potentiality-of-harm standard for § 1348 by requiring an intent to deceive and cause harm).

61. See United States v. Lucien, 347 F.3d 45, 51 (2d Cir. 2003) (declining a narrow construction of "scheme or artifice" in healthcare fraud cases). The court found that the "broad language of § 1347 show[ed] that Congress intended for [the] statute" to govern all manners of health care fraud rather than limit it to specific types of schemes. Id.

62. Indictment, supra note 30, at 1; see Harris & Leising, supra note 17 (noting the unprecedented nature of the criminal spoofing charges).


64. See Electronic Trading: CME Globex, CHI. MERCANTILE EXCHANGE, http://www.cmegroup.com/globex (last visited Oct. 26, 2015) (stating that, as one of the largest derivatives trading centers in the world, the Chicago Mercantile
investigations or spoofing; in 2013, Panther Energy Trading LLC settled a spoofing investigation with the CFTC for nearly one-and-a-half million dollars in remedial sanctions.\(^\text{65}\) However, a criminal spoofing conviction presents a far more nightmarish penalty than mere profit disgorgement\(^\text{66}\) for civil spoofing.\(^\text{67}\) Coscia could face anywhere from five to twenty-five years in prison depending on the application of the U.S. Sentencing Guidelines, along with millions of dollars in fines.\(^\text{68}\) Coscia’s criminal indictment contains twelve counts for six total transactions.\(^\text{69}\) Each transaction has attached to it one count of commodities fraud\(^\text{70}\) and one count of spoofing.\(^\text{71}\)

The indictment uses similar language to describe the transaction in each count. For example, counts two (commodity fraud) and eight (spoofing) concern a gold futures contract order transaction that resulted in $560 of profit.\(^\text{72}\) Count two describes how Coscia committed commodities fraud by entering into gold futures contracts that he “caused to be programmed to quickly cancel” in order to trade at a slightly different price from his competitors.\(^\text{73}\) That language neatly overlays the language of the corresponding count eight for spoofing, which details how Coscia “transmitted to a CME Group server gold commodity futures contract orders that he intended to cancel before execution” for ostensibly the same purpose.\(^\text{74}\) This kind of

---

\(^\text{65}\) In re Panther Energy Trading LLC, CFTC No. 13-26, 2013 WL 3817473 (July 22, 2013). The final settlement was for $1,400,000 in disgorgement penalties. Id.

\(^\text{66}\) R.B. Grantham & C.E.F. Rickett, Disgorgement for Unjust Enrichment?, 62 CAMBRIDGE L.J. 159, 159 (2003) (providing that disgorgement is the process of giving up any gain made from a wrongdoing to a claimant).

\(^\text{67}\) Compare Maria LaMagna, Panther Energy to Pay $2.8M to Settle CFTC Charges, MARKETWATCH (July 22, 2013, 9:37 AM), http://www.marketwatch.com/story/panther-energy-to-pay-28m-to-settle-cftc-charges-2013-07-22 (detailing civil penalties for spoofing ranging from $1.4 million in profit disgorgement to nearly $1 million in fines), with Henning, supra note 17 (estimating a potential prison sentence of more than five years for a spoofing conviction).

\(^\text{68}\) See Henning, supra note 17 (noting that the U.S. Sentencing Guidelines provide a sentencing floor of five years); see also Gulino, supra note 29 (explaining that the U.S. Sentencing Guidelines provide a sentencing ceiling of twenty-five years, depending on prosecutorial recommendations).

\(^\text{69}\) Indictment, supra note 30, at 1, 9–19.

\(^\text{70}\) Id. at 1, 8–13.

\(^\text{71}\) Id. at 14–19.

\(^\text{72}\) Id. at 9, 15.

\(^\text{73}\) Id. at 9.

\(^\text{74}\) Id. at 15.
similarity between the corresponding counts is not uncommon in the indictment and will be analyzed later in this Comment.\textsuperscript{75}

\section*{D. The Blockburger Test and Double Jeopardy Jurisprudence}

Double jeopardy protection originates in the Fifth Amendment, which provides in relevant part that “[n]o person \ldots be subject for the same offence [or] be twice put in jeopardy of life or limb.”\textsuperscript{76} This prohibition covers both successive prosecutions and multiple punishments for the “same offense.”\textsuperscript{77} Though double jeopardy analyses for multiple punishments vary, the “same elements” test is the most widely used and accepted in a majority of jurisdictions, while a small minority favor the “same transaction” test.\textsuperscript{78} This Comment will focus on the same elements test.

The modern same elements test derives from the \textit{Blockburger} case,\textsuperscript{79} though the underlying legal notions developed some time prior to the decision.\textsuperscript{80} The case provides that where the same actions constitute violations of two statutes, the test to determine whether there are two offenses or only one offense is “whether each provision

\begin{itemize}
\item \textsuperscript{75} See infra notes 191–99 and accompanying text (analyzing the content and character of Coscia’s indictment).
\item \textsuperscript{76} U.S. CONST. amend. V.
\item \textsuperscript{77} See Witte v. United States, 515 U.S. 389, 395–96 (1995) (clarifying that the constitutional protection from double jeopardy is broader than the traditional protection from successive prosecution).
\item \textsuperscript{78} See Note, \textit{Double Jeopardy and the Multiple-Count Indictment}, 57 YALE L.J. 132, 134 (1947) (noting that the same transaction test asks whether the proof of one count would sustain conviction under the other count and that the same transaction test asks whether there exists a “common motivating intent aimed at a single ultimate goal, \ldots which \ldots depend[s] on whether the statute prohibits the individuals acts or the course of action which they comprise”); George C. Thomas III, \textit{The Prohibition of Successive Prosecutions for the Same Offense: In Search of a Definition}, 71 IOWA L. REV. 323, 332–34 (1986) (noting that at least four Supreme Court Justices have advocated for a “same transaction” test; however, the “same evidence” test has proven to be the most popular in analyzing same offense questions); see also Witte, 515 U.S. at 396 (applying the “same elements” test, also called the \textit{Blockburger} test); United States v. Dixon, 509 U.S. 688, 696 (1993) (applying the \textit{Blockburger} test).
\item \textsuperscript{79} See Blockburger v. United States, 284 U.S. 299, 304 (1932) (articulating the same elements test); see also Dixon, 509 U.S. at 696 (referencing \textit{Blockburger} and applying the same elements test in a cocaine possession case); Witte, 515 U.S. at 396 (quoting \textit{Blockburger} and applying the same elements test in a federal marijuana case).
\item \textsuperscript{80} See, e.g., Gavieres v. United States, 220 U.S. 338, 342 (1911) (stating—over twenty years before \textit{Blockburger}—that one transaction may only satisfy two different statutes if such statutes require different elements of proof); Morey v. Commonwealth, 108 Mass. 433, 434 (1871) (stating—over sixty years before \textit{Blockburger}—the principles of the “same elements” test).\end{itemize}
requires proof of a fact which the other does not." Blockburger concerned a defendant convicted under a multi-count indictment of various drug-related offenses. The case involved two factual scenarios implicating double jeopardy analysis, but only the second is relevant for the purposes of this Comment. The defendant’s indictment included multiple counts under different sections of the Narcotic Act connected to a single sale of morphine. The Court had to decide whether the single transaction could constitute multiple violations without implicating double jeopardy protection.

To do so, the Court evaluated the elements of the two statutes to determine if one required an element of proof that the other did not. The first violation was for selling prohibited drugs in something other than their original packaging; the second was for selling them without a prescription. Without involving much analysis, the Court decided that the provisions required sufficiently distinct evidence so as to constitute two separate violations for the defendant’s one sale. Though the Blockburger Court did not spend much energy analyzing the two statutory provisions, its analysis rested on other cases in which the Court distilled statutory elements into their component parts to conduct a straight comparison. For example, in Gavieres v. United States, the Court evaluated a double

81. Blockburger, 284 U.S. at 304.
82. Id. at 300–01.
83. Id. at 303–04 (affirming that multiple drug sales made to the same customer at the same time could be charged as multiple counts in a single indictment and evaluating the second question of whether the defendant could be convicted of violations of different sections of the Narcotic Act based on one drug sale). This Comment concerns only the second question.
85. Blockburger, 284 U.S. at 301.
86. Id. at 304.
87. Id.
88. Id. at 301.
89. Id.
90. See id. at 304.
91. See, e.g., Gavieres v. United States, 220 U.S. 338, 342 (1911) (breaking down the elements of two statutes to compare them: an old iteration of a public intoxication statute and a variation of a disturbing the peace statute). The Blockburger Court relied on Gavieres as the foundation for its now-famous mandate to compare statutory elements when determining whether unitary conduct in violation of two statutes constitutes two offenses or one. See Blockburger, 284 U.S. at 304.
92. 220 U.S. 338 (1911).
jeopardy challenge stemming from the defendant's conviction for insulting or threatening a public official and for public intoxication or indecency.\footnote{See id. at 340-41 (noting that the first statute applied to "those who outrage, insult, or threaten, by deed or word, public officials or agents of the authorities, in their presence, or in a writing addressed to them," and the second prohibited being "drunk or intoxicated or behav[ing] in a drunken, boisterous, rude, or indecent manner in any public place open to public view").} To begin its analysis, the Court converted the statutory language of the ordinances into simple elements to use for straight comparison.\footnote{See id. at 342 (reducing the public intoxication statute to the "gist" of its components).} Upon comparing the distilled language of the statutes, the Court determined that they created two, separately punishable offenses because threatening a public official is a superfluous element not required to prove public intoxication and indecency.\footnote{Id. at 343-44 (finding that evidence sufficient for a public intoxication conviction would not be sufficient for an insulting a public official conviction).}

Nearly forty years after the \textit{Blockburger} decision, the Supreme Court decided \textit{Whalen v. United States},\footnote{445 U.S. 684 (1980).} one of several important cases elaborating further on the application of the \textit{Blockburger} test. In \textit{Whalen}, the defendant was convicted of both felony murder and rape.\footnote{See id. at 694 (developing the application of the rule of lenity where Congress fails to specify whether multiple punishments are warranted for one offense that violates two different statutes); \textit{see also} Ball v. United States, 470 U.S. 856, 861 (1985) (determining the rules for \textit{Blockburger} application in the case of "compound" statutes, meaning statutes with elements that incorporate other statutes). \textit{But see} Albernaz v. United States, 450 U.S. 333, 343 (1981) (rejecting in part the \textit{Whalen} implementation of the rule of lenity in cases where Congress is silent on the applicability of two statutes to the same conduct).} The District of Columbia felony murder statute defined the crime as the killing of a human in the course of any of six specified felonies, including rape, among others.\footnote{Whalen, 445 U.S. at 685.} The lower court found against the defendant on the merits of his merger doctrine\footnote{Id. at 686.} argument, leading to his constitutional challenge under a theory of double jeopardy.\footnote{See id. (explaining that the defendant argued in the lower court that his commission of rape merged into the crime of felony murder once the killing took place).} The Supreme Court began its analysis by noting the lack of legislative history available to help define certain portions of the statutes.\footnote{Id. at 687.} In the absence of such history, which might have
led to a presumption of leniency or harshness, the Court held that the two convictions failed the \textit{Blockburger} test because they did not clearly require different elements of proof.\footnote{103} Importantly, the Court in \textit{Whalen} resolved the issue of congressional silence on whether the statutes could be punishable together or separately with leniency towards the defendant.\footnote{104} The Court’s later decision in \textit{Albernaz v. United States},\footnote{105} in which the Court refused to apply the rule of leniency where the statute was unambiguous and the legislative history did not cause the Court to pause,\footnote{106} created tension with this determination.

The final seminal case in this corner of double jeopardy jurisprudence is \textit{Ball v. United States}.\footnote{107} In \textit{Ball}, the defendant was convicted of violating two firearm statutes, one that prohibited receiving a firearm in interstate commerce and another prohibiting the receipt, transportation, or possession of a firearm in interstate commerce.\footnote{108} The defendant was convicted of both and sentenced to successive jail sentences.\footnote{109} The \textit{Ball} Court seemingly rejected the threshold question offered in \textit{Albernaz} regarding the effect of congressional silence on the application of the rule of leniency.\footnote{110} In this manner, the \textit{Ball} Court did not first analyze congressional silence on the application of the two firearm statutes with a presumption favoring the defendant; the Court instead used the \textit{Blockburger} test as the first mode of analysis.\footnote{111} Importantly, the \textit{Ball} Court further developed the \textit{Blockburger} test by applying it to two different compound statutes.\footnote{112}

The \textit{Blockburger}, \textit{Whalen}, and \textit{Ball} cases comprise a substantial amount of modern double jeopardy jurisprudence specific to

\footnote{103. See \textit{Whalen}, 445 U.S. at 693–94 (finding that the added required element of a killing for a felony murder conviction did not sufficiently differentiate the charges so as to fail the \textit{Blockburger} test).}

\footnote{104. \textit{Id.} at 694.}

\footnote{105. 450 U.S. 333 (1981).}

\footnote{106. \textit{Id.} at 342–43.}

\footnote{107. 470 U.S. 856 (1985).}

\footnote{108. \textit{Id.} at 857.}

\footnote{109. \textit{See id.} at 857–58 (sentencing Ball to three years for the receipt of the firearm followed by two years for the possession of the firearm).}

\footnote{110. \textit{See id.} at 861 (applying \textit{Blockburger} without first using the \textit{Albernaz} framework to say that congressional silence on the application of statutes should be read as precluding two convictions for the same conduct).}

\footnote{111. \textit{Id.} at 862.}

\footnote{112. \textit{See Thomas III, supra} note 102, at 85 (citing \textit{Whalen v. United States}, 445 U.S. 684 (1980)) (explaining that compound statutes are formed when a predicate offense morphs into a different offense after an additional element is introduced).}
multiple punishment questions. Those three cases, taken together with *Gaviere*, form a workable framework within which to evaluate statutes for double jeopardy questions. This framework is incomplete, however, without an understanding of some of the canons of statutory construction that provide context for the analysis.

E. *Lex Generalis, Merger Doctrine, and the Rule of Lenity*

Canons of construction are guides meant to help courts understand the meaning of legislation. Three canons help to illustrate the legal theorem relevant to the *Blockburger* decision. The first canon is *lex specialis derogat lex generalis*, meaning specialized laws prevail over general laws. For example, a statute specifically governing bank robbery will supersede a more generic robbery statute when indicting a bank robber. Applying this canon necessitates an understanding of the policy underlying the statutes to decide whether construing one at the expense of the other is appropriate and whether it keeps in line with the larger statutory regime.

The second important canon of construction is the merger doctrine. The merger doctrine holds that, absent clear evidence to the contrary, where one offense merges into another during commission of a crime, the later offense should consume the former in an indictment. The purpose of merger is to ensure that

113. See supra notes 78-112 and accompanying text (tracing the developments in double jeopardy theory).
114. See supra notes 92-95 and accompanying text (completing the framework by adding the preliminary analysis focusing on simplifying the statutory elements into their basic components).
116. See In re Lazarus, 478 F.3d 12, 18 (1st Cir. 2007) (phrasing the maxim as “the more specific treatment prevails over the general” (citing United States v. Lara, 181 F.3d 183, 198 (1st Cir. 1999))); see also Kirchheimer, supra note 36, at 517 (showing common uses of the *lex specialis* doctrine, such as convicting under the specific bank robbery statute instead of under the more general robbery statute).
117. See Kirchheimer, supra note 36, at 517-18 (noting that the same canon governs the relationship between larceny and robbery; intoxication on a public highway and driving on a public highway while intoxicated; and certain lesser-included offenses).
118. See Varity Corp., 516 U.S. at 511 (requiring an understanding of the policy behind the statutes in question, obtained through using canons of construction, so as to allow a meaningful comparison to determine the substantive limitations in application of each).
119. See Prince v. United States, 352 U.S. 322, 328 (1957) (merging two distinct statutory violations into one based on the absence of evidence of congressional intent to the contrary); see also Kirchheimer, supra note 36, at 518 (advocating a “consumption” principle,
overlapping statutes are applied in an orderly regime, with meaningful distinctions as to when statutes should be read as both applicable or as mutually exclusive.\textsuperscript{120} Major authority for this proposition comes from \textit{Prince v. United States}.\textsuperscript{121} In \textit{Prince}, the Supreme Court decided whether the crime of entering a bank with the intent to commit a robbery merges with the crime of bank robbery once the robbery is committed.\textsuperscript{122} The defendant in \textit{Prince} robbed a Malone, Texas bank with a revolver and was later apprehended.\textsuperscript{123} A grand jury issued a two-count indictment, charging him with one count of robbery and one count of entering the bank with the intent to commit a felony.\textsuperscript{124} He was convicted on both counts and was to serve, consecutively, twenty years for the robbery and fifteen years for entering.\textsuperscript{125}

The Court determined that, absent congressional intent or legislative history to the contrary, the unlawful entry provision was inserted to cover factual scenarios in which a defendant entered a bank with the intent to rob it, but, for whatever reason, failed to accomplish his illicit aims.\textsuperscript{126} The Court surmised that the two punishments were supposed to work side-by-side to ensure application across all factual scenarios, rather than stack atop each other for every basic bank robbery.\textsuperscript{127} To reach that conclusion, the Court used the merger canon to evaluate the gravamen of both offenses and discovered that it remained constant for both.\textsuperscript{128} Although one crime focused on the entry and the other on the act of robbery, the

\begin{itemize}
\item \textit{Prince}, 352 U.S. at 327–28 (attributing the Court’s merger analysis to the need to preserve an orderly interpretation of criminal statutes).
\item 352 U.S. 322, 328 (1957).
\item \textit{Id.} However, it is important to note that the Court specifically stated that its holding in the case was to be narrowed to the statute at issue and not expanded to cases at large involving “fragmentation of crimes for the purposes of punishment.” \textit{Id.} at 325.
\item \textit{Id.} at 324.
\item \textit{Id.} at 324.
\item \textit{Id.}
\item \textit{Id.} at 328.
\item \textit{Id.} at 327 (rejecting the government’s request to interpret the statute as amended as making each offense independent). The Court in this case was attempting to reconstruct an enforcement regime by applying sparse congressional intent. The result was a finding that Congress intended to establish lesser offenses, but that it did not intend to stack the penalties. \textit{Id.} The finding was based on the fact that the Attorney General’s letter to Congress only stressed the “possibility that a thief might not commit all of the elements of the crime of robbery.” \textit{Id.}
\item \textit{Id.} at 328.
\end{itemize}
Court found that the most significant element of both crimes was the intent to steal. In this manner, the "merger" of the intent to rob and the act of robbing shows the Court's interpretation of how Congress intended the bank robbery statutory scheme to function. The use of the merger doctrine is distinct from the now-outdated common law principle of merger. The use functions more like a supplementary analysis to the Blockburger test, extending double jeopardy protections from simply a strict comparison of elements to also include an examination of congressional intent.

The Prince Court proceeded with its double jeopardy analysis through the lens of another canon of construction: the rule of lenity. The rule of lenity invokes similar themes to the merger theory in that it only operates in the absence of congressional intent to guide the court. In such a case, the role of lenity is a presumption against the more severe punishment that could be possibly attributed in the reading of an unclear statute. The Prince Court interpreted this rule as an inherent limitation on multiple punishments, attributing to Congress the presumption of lenity absent clear legislative evidence to the contrary. The Court's treatment of this maxim as a guiding principle in the absence of clear legislative intent is critical to the double jeopardy analysis because the only time a court engages in substantive analysis is when the threshold requirement of no legislative intent is first met.

129. Id. (denying to go beyond the given analysis because it would compel a finding that Congress intended to make drastic changes in authorized punishments).

130. See id. (merging the intent to rob with the act of robbing to differentiate statutes Congress intended to stack with those Congress intended to complement).

131. See Thomas III, supra note 102, at 40–41 (theorizing that the Prince Court's use of the merger doctrine was more of a shorthand used to describe a "merger" of offenses when one crime violated two statutes and where congressional intent is clear, rather than an expression of the common law doctrine); see also Callanan v. United States, 364 U.S. 587, 589–90 (1961) (declaring with finality the abandonment of common law merger in modern jurisprudence).

132. See Thomas III, supra note 102, at 37–39 (claiming the Prince case as the Supreme Court's realization that a strict Blockburger analysis provided too little protection against double jeopardy to defendants); see also Prince, 352 U.S. at 325 (prefacing a traditional Blockburger analysis with an evaluation of congressional intent).

133. Prince, 352 U.S. at 329 (applying criminal penalties with leniency towards the defendant if doing so is consistent with "pertinent legislative history").

134. Id. (emphasizing the necessary condition of a lack of clear congressional intent).

135. See id. (noting the Court's policy of not attributing to Congress an intention to punish more severely than the statute's clear language).

136. Id.

137. See supra note 132 and accompanying text (explaining double jeopardy's threshold question of whether there is clear legislative intent to enforce multiple or
The theories of lex generalis, merger, and lenity are not binding rules; rather, they are guiding principles to help broaden and enhance understanding of statutory language and intent.\(^{138}\) However, they do carry substantial weight in interpreting vague statutes or statutes in which the underlying congressional intent is unclear.\(^{139}\) As such, this Comment will treat them as supplementary in nature, aiding in the main comparative elements analysis below.

II. A CRIMINAL INDICTMENT FOR BOTH SPOOFING AND COMMODITIES FRAUD FOR THE SAME TRANSACTION IMPLICATES DOUBLE JEOPARDY

If proving a spoofing violation always proves a commodities fraud violation, or vice versa, then the *Blockburger* test would reveal a presumption that the legislature intended not to create two separate offenses, but instead that it intended to create alternative statutory grounds for punishment.\(^{140}\) The first step in the *Blockburger* analysis is distilling the statutory elements into usable component parts, as per the *Gavieres* requirement.\(^{141}\) The statutes at issue in *Gavieres* were fairly straightforward,\(^{142}\) unlike the spoofing and commodities fraud statutes. As such, the *Gavieres* analysis that follows is substantially more in depth to discern the true meaning of those statutes.

A. *Spoofing and Commodities Fraud Under the Gavieres Mandate*

The spoofing statute itself is largely unhelpful in providing a workable plain meaning. It reads as follows:

> It shall be unlawful for any person to engage in any trading, practice, or conduct on or subject to the rules of a registered entity that... 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).143

Taking the elements in order, the first ambiguity is what it means
to be engaged in any trade, practice, or conduct subject to the rules
of a registered entity. Registered entities are generally market
oversight and organizational authorities that register with the CFTC
to promulgate rules and regulations that govern their member-
participants.144 These entities include designated contract markets,145
swap execution facilities,146 derivatives clearing organizations,147 and
swap data repositories.148 The CFTC heavily relies on these
organizations as industry self-regulators to submit and enforce rules
to govern their members.149 The spoofing statute applies to any
trader operating on one of these entities, but, for the sake of
simplicity, we will simply call them "market participants."150

144. See Rules and Rule Amendments, U.S. COMMODITY FUTURES TRADING
(last visited Oct. 26, 2015) (illustrating that registered entities are essential to
maintaining market integrity and protecting the consumer through drafting and
implementing smart and effective rules to help self-regulate).
145. See Designated Contract Markets, U.S. COMMODITY FUTURES TRADING
index.htm (last visited Oct. 26, 2015) (describing designated contract markets ("DCMs")
as boards of trade or exchanges based on an underlying commodity or index).
146. See Swap Execution Facilities, U.S. COMMODITY FUTURES TRADING
(last visited Oct. 26, 2015) (explaining that swap execution facilities ("SEFs")
function like trading platforms and help maintain pre-swap price transparency and
orderly market orientation by providing pre-trade information, such as bids, offers,
and methods of execution, to its participants).
147. See Derivatives Clearing Organizations, U.S. COMMODITY FUTURES TRADING
index.htm (last visited Oct. 26, 2015) (demonstrating that derivatives clearing
organizations ("DCOs") are entities that facilitate mutualization of credit risk among
participants through contracted credit swaps, allowing participants to substitute the
credit of the DCO for their own credit and to settle outstanding obligations).
148. See Data Repositories, U.S. COMMODITY FUTURES TRADING
26, 2015) (defining swap data repositories ("SDRs") as entities that provide
centralized facilities for swap data recordkeeping and reporting).
149. See Rules and Rule Amendments, supra note 144 (reiterating the role of
registered entities in promoting and maintaining orderly market functionality, as
well as supplementing regulators in market oversight).
150. See Disruptive Practices Guidance, 76 FED. REG. 14,943, 14,947 (proposed
Mar. 18, 2011) (referring to traders eligible for regulation under the spoofing statute
as "market participants").
The next element for interpretation is what actions are, are of the character of, or are commonly known to the trade as spoofing. The CFTC released guidance in March 2011 that sheds some light on this section.\textsuperscript{151} The CFTC's spoofing definition enumerates specific actions that qualify as spoofing, but connects them under a central theme.\textsuperscript{152} Specifically, spoofing can include, but is not limited to: "(i) [s]ubmitting or cancelling bids or offers to overload the quotation system of a registered entity[;] (ii) submitting or cancelling bids or offers to delay another person's execution of trades; and (iii) submitting or cancelling multiple bids or offers to create an appearance of false market depth."\textsuperscript{153} Although when taken separately these actions cover fragmented illicit trading strategies, together they reveal the CFTC’s aim of regulating specifically the practice of entering into trades with the intent to cancel; in other words, to regulate only illicit trading behavior.\textsuperscript{154}

The Agency itself has explicitly revealed this goal through its promulgation and reiteration of an intent requirement.\textsuperscript{155} In the 2011 guidance, the agency declared that "a market participant must act with some degree of intent, or scienter" and that, therefore, "reckless trading, conduct, or practices will not result in violations."\textsuperscript{156} Limiting the scope of the spoofing statute to preserve legitimate trading was clearly an important goal to the Agency, as it was a central conversation topic in the Agency's talks with industry representatives before releasing the guidance.\textsuperscript{157} This goal, combined with the enumerated and broad examples in the guidance, provides a starting point for interpreting the statute. However, the next portion of the statute draws a spoofing definition from the industry's definition of the term.\textsuperscript{158}

\begin{itemize}
  \item 151. \textit{See id.} This guidance released by the CFTC is the most helpful source of information on the Commission's priorities with regards to prosecuting spoofing. It elaborates not only on some definitional issues surrounding spoofing enforcement, but also on the scope and nature of the spoofing provisions themselves. \textit{Id.}
  \item 152. \textit{See id.} (connecting the enumerated actions under the common theme of entering into bids with the intent to cancel). \textit{Id.}
  \item 153. \textit{Id.}
  \item 154. \textit{See id.} (noting that by stressing "intent," the Commission does not intend to cover reckless trading, conduct, or practices in the definition of spoofing). \textit{Id.}
  \item 155. \textit{Id.}
  \item 156. \textit{Id.}
  \item 157. \textit{See id.} (reiterating the Commission's goal of limiting spoofing violations to actions with a provable scienter element so as to exempt innocent trading and noting that the guidance was influenced in large part by a noticeable industry concern for preserving honest trading activity).
  \item 158. \textit{See 7 U.S.C. § 6c(a)(5)(C) (2012) (criminalizing trading, practice, or conduct that "is, is of the character of, or is commonly known to the trade as, 'spoofing'")}
\end{itemize}
Spoofing has a murky and controversial definition within the commodities trading industry.\textsuperscript{159} Even beyond the lack of an agreeable definition of spoofing, some industry insiders have difficulty deciphering other parts of the statute.\textsuperscript{160} For example, one of the industry representatives at the CFTC roundtable discussion leading up to the guidance publication asked the group why the statute differentiated “practice” and “conduct” from trading, noting that the obscure language made it difficult to comfortably take a position on the legitimacy of certain trades.\textsuperscript{161} Others in the roundtable took issue not with the lack of a definition of spoofing, but with the multitude of definitions.\textsuperscript{162} The CFTC incorporated these concerns when drafting their guidance, and produced regulations that make an effort to distinguish spoofing from legitimate trading activity.\textsuperscript{163} In fact, the Agency provided increased protection to traders by adding in a good faith defense clause, reflecting industry concerns that good faith trading might still technically qualify as spoofing.\textsuperscript{164} As such, the elements of spoofing may be fairly reduced to two: (1) the common theme of entering orders with the intent to cancel; and (2) an intent to cancel in bad faith with no legitimate underlying business reason.\textsuperscript{165} These new elements satisfy the

\textsuperscript{159} See, e.g., Roundtable, \textit{supra} note 42, at 82 (statement of John Lothian, John J. Lothian & Company) (noting that spoofing is “a very undefined type of a term within the industry”).

\textsuperscript{160} Id. at 59.

\textsuperscript{161} Id. at 59–60.

\textsuperscript{162} See \textit{id.} at 64 (statement of Gary DeWaal, Newedge USA, LLC) (“I’m not sure of [sic] the definition of spoofing can be agreed upon by the ten people around this table.”); \textit{id.} at 82 (statement of John Lothian, John J. Lothian & Company) (“[I]t’s a very undefined type of a term within the industry.”); \textit{id.} at 111 (statement of Adam Nunes, Hudson River Trading Group) (“[T]here’s a fundamental question which is, if you’re putting orders out that are taking risk, can you be defined as spoofing?”).

\textsuperscript{163} \textit{See} Disruptive Practices Guidance, 76 \textit{Fed. Reg.} 14,943, 14,947 (proposed Mar. 18, 2011) (emphasizing that the spoofing guidance only applies to illegitimate trading).

\textsuperscript{164} \textit{See} Roundtable, \textit{supra} note 42, at 35 (statement of Raj Fernando, Chopper Trading, LLC) (explaining that a trader can enter a bid with the intent to cancel it to legitimately test risk procedures); \textit{see} also Disruptive Practices Guidance, 76 \textit{Fed. Reg.} at 14,947 (clarifying that orders would not be considered spoofing if they were “part of a legitimate, good-faith attempt to consummate a trade”).

\textsuperscript{165} Whether referring to broad rules or specific examples, the CFTC guidance and codified statute consistently cite the need for orders to be entered with the intent to cancel. \textit{See}, e.g., Disruptive Practices Guidance, 76 \textit{Fed. Reg.} at 14,947. The good faith trading exception appears to reflect industry concerns that the rule might have ill-effects without distinguishing manipulative, bad-faith cancellations from regular cancellations. \textit{See}, e.g., Roundtable, \textit{supra} note 42, at 21 (statement of Adam Nunes, Hudson River Trading Group) (demonstrating how spoofing can be fairly
first half of the required *Gavieres* analysis as a preliminary step in the larger *Blockburger* test. What follows is the same application of *Gavieres* to distill the commodities fraud statute for comparison.

Securities fraud regulation passed as part of the Sarbanes-Oxley Act of 2002. In 2009, the Act was amended to include commodities as well. The Act proscribes a fine and/or twenty-five year penalty for anyone who:

- knowingly executes, or attempts to execute, a scheme or artifice . . .
  - (1) to defraud any person in connection with any commodity for future delivery, or any option on a commodity for future delivery, or any security of an issuer with a class of securities registered under section 12 of the Securities Exchange Act of 1934 . . . or
  - (2) to obtain, by means of false or fraudulent pretenses, representations, or promises, any money or property in connection with the purchase or sale of any commodity for future delivery, or any option on a commodity for future delivery, or any security of an issuer with a class of securities registered under section 12 of the Securities Exchange Act of 1934 . . .

Mechanically speaking, the commodities fraud statute has three elements: (1) a fraudulent intent; (2) a scheme or artifice; and (3) a connection to a security or commodity. The statute requires the fraudulent intent to rise to the level of "knowing." The statute’s legislative history indicates that the intent provision is supposed to mirror that of the mail, wire, and bank fraud statutes.

---

166. See *Gavieres* v. United States, 220 U.S. 338, 342 (1911) (referencing the reduced elements of each statute in simplified language).


169. Id.

170. See, e.g., United States v. Mahaffy, 693 F.3d 113, 125 (2d Cir. 2012) (analyzing these three elements of commodities fraud in the context of insider trading); United States v. Motz, 652 F. Supp. 2d 284, 289, 294 (E.D.N.Y. 2009) (undertaking the same analysis to evaluate a "cherry-picking" scheme, whereby a broker executes trades but leaves them without an assigned account until the securities either appreciate or depreciate during the trading day).


172. See S. Rep. No. 107-146, at 20 (2002) (reiterating the Senate’s will to apply the intent requirement consistently with the intent requirements in 18 U.S.C. §§ 1341, 1343–44, 1347). The section numbers indicated in the Senate Report correspond to the mail, wire, bank, and health care fraud statutes, respectively. See Luke A. E.
language tracks that of other fraud statutes, the intent element can be explained in a similar manner.\(^{173}\) As with the accompanying fraud statutes, § 1348 intent generally requires a showing that the defendant had a “conscious knowing intent to defraud.”\(^{174}\) This scienter standard separates simply reckless behavior from behavior that the defendant knows is fraudulent and harmful.\(^{175}\) The harm component by definition excludes mere misrepresentations as satisfactory on their own, but in most cases, the intent can be inferred as the “necessary result” of the scheme itself.\(^{176}\)

The second element of the statute is a “scheme or artifice” used to defraud.\(^{177}\) The term “scheme or artifice” carries with it a connotation of deceit and illegitimacy, and it is construed as such in the corresponding fraud statutes.\(^{178}\) Courts have used the term to serve as a stark distinction from legitimate activity, keeping in line with the statutory aim of protecting innocent behavior.\(^{179}\) This statutory aim is one of the only legislated guiding principles that limit the scope of what exactly a “scheme or artifice” is, as Congress failed to define the term in the statute.\(^{180}\) As such, courts have shouldered

---


\(^{175}\) See, e.g., United States v. Kelly, Criminal No. 3:11-cr-192 (JCH), 2014 WL 3565957, at *5 (D. Conn. July 18, 2014) (interpreting the wire fraud statute to require a “conscious knowing intent to defraud” (quoting United States v. Autuori, 212 F.3d 105, 116 (2d Cir. 2000))).

\(^{176}\) See Autuori, 212 F.3d at 116 (“Essential to a scheme to defraud is fraudulent intent.” (citing United States v. D’Amato, 39 F.3d 1249, 1257 (2d Cir. 1994))); see also United States v. Gabriel, 125 F.3d 89, 96–97 (2d Cir. 1997) (“[A] defendant acts with a[n] . . . intent to defraud if he participates in the fraudulent scheme with some realization of its fraudulent or deceptive character and with recognition of its capacity to cause harm to the victims of such deception.”).

\(^{177}\) See Horman v. United States, 116 F. 350, 352–53 (6th Cir. 1902) (finding that a scheme to defraud and defame investors necessarily involved harming the victims, and that, therefore, it automatically satisfied the scienter requirement).

\(^{178}\) See, e.g., Horman, 116 F. 350 at 352 (construing “scheme or artifice” in mail fraud cases against the backdrop of the underlying purpose to preserve legitimate uses of the postal service).

\(^{179}\) See id. (observing that guilty intent is proven “when the act is proved to have been knowingly committed” (quoting United States v. Taintor, 28 F. Cas. 7, 9 (C.C.S.D.N.Y. 1873) (No. 16,428))).

\(^{180}\) See United States v. Von Barta, 635 F.2d 999, 1005 (2d Cir. 1980) (analyzing the “sparse” guiding legislative history accompanying § 1341 to reveal “only one clearly articulated purpose: to prevent the use of the mails in furtherance of fraudulent
the responsibility to clarify the definition.\textsuperscript{181} Though there are many nuances and facets to interpreting a scheme or artifice, courts generally identify such schemes by connecting them to the fraudulent intent, thereby ensuring that they are only capturing schemes that required planning and the intent to defraud.\textsuperscript{182}

The third element is a connection to a commodity.\textsuperscript{183} There is virtually no limit on the range of victims that a scheme must touch for it to be “in connection with [a] security.”\textsuperscript{184} Conceivably, this connection could even be established between two computers engaged in algorithmic trading so long as the software was programmed to derive a benefit from the trading activity. This interpretation of establishing connections through the pursuit of gain is firmly rooted in Supreme Court jurisprudence.\textsuperscript{185} This broad interpretation is consistent not only with the broad nature of the preceding elements, but also with the intent of the statute’s drafters.\textsuperscript{186}

As such, the elements of commodities fraud may be more simply stated as: (1) a fraudulent intent to knowingly and harmfully deceive (2) through the use of a scheme or artifice furthering the fraudulent intent (3) in connection with a commodity. Now that the elements of both spoofing and commodities fraud have been reduced to their plain meaning per the \textit{Gavieres} mandate, the next step in the \textit{Blockburger} test will compare the distilled elements to show that proof of spoofing will always constitute proof of commodities fraud.

\textbf{B. A Comparison of the Spoofing and Commodities Fraud Elements Post-\textit{Gavieres} Fails the Blockburger Sameness Test}

In a multi-count indictment, where the proof of one offense necessarily proves another offense in its entirety, the \textit{Blockburger} test

\textsuperscript{181} See \textit{McNeive}, 536 F.2d at 1248 (recapping the role courts have had in supplementing sparse legislative history to discern the purpose and reach of the statute).

\textsuperscript{182} See, \textit{e.g.}, \textit{id.} (establishing that schemes intended to defraud individuals fall under the mail fraud statute); United States v. Nance, 502 F.2d 615, 618 (8th Cir. 1974) (imputing an element of planning or pattern into the concept of a “scheme”).

\textsuperscript{183} \textit{Id.}; \textit{see United States v. Mahaffy}, No. 05-CR-613, 2006 WL 2224518, at *12 (E.D.N.Y. 2006) (noting that the phrase “in connection with” has such a broad definition that it does not even concern the status of the victim).


will prohibit punishment for both offenses. Though *Blockburger* has never been used to evaluate the spoofing and commodities fraud statutes, the Supreme Court used it to examine firearm receipt and firearm possession statutes in *Ball v. United States*.188

It is this analysis—that committing one offense necessarily involves total proof of the other—that shows why spoofing and commodities fraud may be incompatible on the same indictment. Committing “spoofing” necessarily involves the commission of commodities fraud. This proposition does not hold true when reversed, as commodities fraud can involve the commission of a fraud more general than the specific schemes or artifices articulated in the spoofing statute.189 However, spoofing appears to function as more of a specific subset of larger manipulation.190

This theory holds when comparing the distilled elements of the two statutes side-by-side. When committing a spoofing violation, a defendant must: (1) enter orders with the intent to cancel, and (2) the intent to cancel must be in bad faith with no legitimate underlying business reason.191 For the purposes of illustrating a

---


188. Recall that in *Ball*, the defendant was convicted on violations of 18 U.S.C. § 922(h)(1) and § 924(a), receiving and possessing a firearm shipped in interstate commerce. *Ball*, 470 U.S. at 857. The Court noted that the *Blockburger* inquiry is whether one offense requires proof of an element that the other does not, as Congress does not ordinarily intend to punish the same offense twice. Id. at 861.

189. Compare *Disruptive Practices Guidance*, 76 FED. REG. 14,943, 14,947 (proposed Mar. 18, 2011) (deeming that spoofing requires the specific action of entering a bid with the intent to cancel before execution), with United States v. McNeive, 536 F.2d 1245, 1248 (8th Cir. 1976) (describing the absence of congressionally established parameters defining “scheme or artifice” with regards to mail fraud). Also note that the mere fact that the elements of commodities fraud can be met by other actions besides spoofing does not automatically mean that the two statutes pass the Blockburger test. See Whalen, 445 U.S. at 694 (rejecting the government’s contention that felony murder and rape charges should be separately punishable because felony murder can be satisfied by the killing of a person during the commission of other felonies besides rape).

190. See *Roundtable*, supra note 42, at 92 (statement of Adam Nunes, Hudson River Trading Group) (explaining that “spoofing” is one narrow aspect of the larger crime of manipulating the market); id. at 21 (stressing that there are rules “against submitting orders or quotes . . . with the intent of . . . effectively manipulating others to act in a way that they otherwise wouldn’t” (emphasis added)).

191. See supra notes 143–66 and accompanying text (simplifying the elements of spoofing and commodities fraud as done with different elements in Gavieres v. United States, 220 U.S. 338, 343 (1911)).
"typical" spoofing violation, we will examine one of the spoofing counts in the Coscia indictment. Coscia is accused of manipulating market prices through a carefully staged number of buy and sell orders and of exploiting the slight movement to make small profits. The indictment alleges that he entered into preliminary buy orders, then artificially depressed market prices for those orders by putting out large sell orders. Coscia then filled his buy orders and raised prices past their original level by cancelling his large sell orders. Coscia then finished the series by selling the orders he purchased at the higher price that he allegedly created.

Coscia's alleged spoofing operation and the more general CFTC spoofing guidance provide working models to compare with commodities fraud. First, the spoofing element of entering orders with the intent to cancel them will always satisfy the commodities fraud element of using a scheme or artifice to achieve an illicit end. To qualify as spoofing, the participant must enter orders with the intent to cancel them as part of a bad faith effort unrelated to any legitimate business purpose. This requirement manifests in the CFTC's grant of a good faith trading defense so as to limit its regulation to only cover illicit activity. As such, the spoofing activity must be perpetrated to reach an illicit end. Because of this requirement, spoofing techniques will always be a "scheme or artifice" for the purposes of commodities fraud. This connotation manifests not only in a clear

192. There is no precedent examining the elements of spoofing, so Coscia's indictment will suffice for the purposes of this Comment. See Indictment, supra note 30, at 6–7 (alleging that Coscia placed sell orders to drive down prices, filled buy orders, then cancelled the sell orders to let prices rise, and resold the filled buy orders at a profit).
193. Id.
194. Id. at 6.
195. Id.
196. Id. at 6–7.
198. See Disruptive Practices Guidance, 76 FED. REG. 14,943, 14,947 (proposed Mar. 18, 2011) (providing a good faith cancellation defense so as to differentiate legitimate trading activity).
199. Id.
200. Id.
congressional attempt to distinguish activities as part of a scheme or artifice from legitimate trading activity, but also in how the courts determine what kinds of set-ups qualify. As such, every spoofed trade entered into with the bad faith intent to cancel before execution that would fall outside of the good faith trading defense provided in the CFTC guidance would also satisfy the § 1348 scheme and artifice requirement of servicing an illegitimate or deceitful goal. Both the spoofing and commodities fraud statutes explicitly attempt to limit their scope to only illegitimate trading behavior in the same manner; so, impermissible behavior under the former also qualifies as such under the latter.

Furthermore, the fact that the intent to cancel must be present at the time the trade was entered to trigger the spoofing statute also implicates the court-developed notion that schemes and artifices for commodities fraud usually involve a degree of planning to evince intent. By definition, spoofing requires planning because it is a two-step process: the spoofer has to first enter into, and subsequently cancel, the trades. If this process does not happen with the requisite precision, the cancelled trades will not shift the market, and the spoofer will derive no benefit and cause no harm.

Spoofing also satisfies the intent required to commit commodities fraud. Both statutes require scienter on behalf of the defendant to

203. Id.; see Hornan v. United States, 116 F. 350, 352 (6th Cir. 1902) (attempting to protect innocent behavior while regulating illicit actions).


205. See, e.g., Hornan, 116 F. at 352 (interpreting the scheme or artifice requirement broadly to include attempts to injure another).

206. Compare id. ("The phrase 'scheme or artifice to defraud' is to be construed bearing in mind the underlying purpose of the statute to preserve the use of the mails to legitimate ends.")., with Disruptive Practices Guidance, 76 Fed. Reg. at 14,947 ("Furthermore, orders, modifications, or cancellations will not be classified as 'spoofing' if they were submitted as part of a legitimate, good-faith attempt to consummate a trade.").


208. Id.

209. Michael Coscia, on the other hand, is accused of perpetrating successful spoofing. See Indictment, supra note 30, at 6 (describing Coscia's spoofing actions of successfully entering into and cancelling trades to make a profit).

210. The commodities fraud statute requires the defendant to "knowingly" commit the fraud. 18 U.S.C. § 1348 (2012). Previously discussed case law interprets this standard to mirror that of the wire fraud statute, which requires a conscious intent to defraud. United States v. Kelly, Criminal No. 3:11-cr-192, 2014 WL 3565957, at *5 (D. Conn. July 18, 2014). The spoofing statute does not specify what intent would qualify, but the intent can be inferred from the CFTC guidance's
separate intentional behavior from reckless behavior. The scienter requirement for spoofing necessitates trading in bad faith, which appears to be akin to market deception. The scienter requirement for commodities fraud necessitates intentional deception with the intent to harm the victims. A spoofer will always act with the requisite intent for commodities fraud because spoofing can only work through deceptive trading and is always done to the detriment of other traders. Courts have consistently upheld that when the necessary result of a scheme or artifice is to injure others, the requisite intent can be inferred simply from the defendant's execution of the scheme. Such is the case with spoofing: the trades are not made in a vacuum—spoofed trades harm anyone relying on those trades as good faith representations of actual buy-and-sell orders.

When compared side-by-side, the elements of spoofing appear to overlay the elements of commodities fraud. Thus, a defendant who commits a true spoofing transaction will always also commit commodities fraud, even if the reverse is not true. This situation is similar to that which the Court faced in Ball. Though the Court


212. Id.

213. See, e.g., Henning, supra note 17 (describing spoofing as a form of market manipulation); Roundtable, supra note 42, at 6 (identifying spoofing as a subset of broader market manipulation).

214. See, e.g., United States v. Gabriel, 125 F.3d 89, 97 (2d Cir. 1997) (requiring an intent to harm because the more inclusive standard of simply recognizing the possibility of harm could ensnare innocent bystanders).

215. See Henning, supra note 17 (describing how spoofed trades manipulate traders into disadvantageous positions, thereby reaping profit at the expense of other participants).

216. United States v. D'Amato, 39 F.3d 1249, 1257 (2d Cir. 1994) ("When the ‘necessary result’ of the actor’s scheme is to injure others, fraudulent intent may be inferred from the scheme itself."); United States v. Regent Office Supply Co., 421 F.2d 1174, 1182 (2d Cir. 1970) ("Although proof that the injury was accomplished is not required, . . . we believe the statute does require evidence from which it may be inferred that some actual injury to the victim . . . is a reasonably probable result of the deceitful representations if they are successful.").

217. See Henning, supra note 17 (explaining how, given the automated nature of a substantial percentage of U.S. trading activity, spoofed trades affect the calculations of other trading computers, resulting in rapid market movement).

218. See supra notes 189–217 and accompanying text (comparing the elements of spoofing to the elements of commodities fraud to show that proof of spoofing will always prove commodities fraud).

219. See Ball v. United States, 470 U.S. 856, 857 (1985) (determining whether the
was content to merely state the proposition that gun receipt necessitates possession and that, therefore, a defendant could not be convicted of both,²²⁰ the underlying inquiry is the same: "whether each provision requires proof of a fact which the other does not."²²¹ Applying this test to spoofing and commodities fraud, it is clear that proof of spoofing by definition proves commodities fraud; therefore, the Blockburger test constitutionally precludes convicting and sentencing a defendant with both violations for a single transaction.²²²

C. The Canons of Lex Specialis Derogat Lex Generalis and Merger Doctrine Show How Spoofing Operates as a Mechanical Subset of Commodities Fraud, Rather Than as a Different Act

Though the Blockburger test has become a bedrock principle in multiple-punishment jurisprudence,²²³ it may be helpful to explore some canons of statutory construction so as to further illuminate the underlying principles. One such maxim is lex specialis derogat lex generalis, or, specialized laws prevail over general laws.²²⁴ This principle is most often seen when dealing with two provisions in the same enactment.²²⁵ However, it may also be used to construe statutes that are “interrelated and closely positioned.”²²⁶ Though spoofing and commodities fraud are not closely positioned within the United

---

²²⁰ Id. at 862.
²²² See id. at 304 (holding that if the same conduct is used to prove violation of two different statutory provisions using the same elements, the defendant may only be prosecuted and punished under one statute).
²²³ See Ball, 470 U.S. at 861 (noting that the Court has “consistently” relied on the Blockburger test).
²²⁴ See, e.g., Varity Corp. v. Howe, 516 U.S. 489, 507-08 (1996) (authorizing a lawsuit for individual relief under specialized employment benefits law rather than under a broader statute); In re Lazarus, 478 F.3d 12, 18 (1st Cir. 2007) (“In statutory construction, the more specific treatment prevails over the general.”); Diaz v. Cobb, 435 F. Supp. 2d. 1206, 1216 (S.D. Fla. 2006) (dismissing a lawsuit for failing to state a claim under the federal Voting Rights Act when the plaintiffs instead stated their claim under the National Voter Registration Act); Kirchheimer, supra note 36, at 515–17 (explaining the specialty principle as one approach to situations where several legal prescriptions are applicable to the same offense).
²²⁵ See Fourco Glass Co. v. Transmirra Prods. Corp., 353 U.S. 222, 228–29 (1957) (“Specific terms prevail over the general in the same or another statute which otherwise might be controlling.” (quoting D. Ginsberg & Sons, Inc. v. Popkin, 285 U.S. 204, 208 (1932))).
²²⁶ HCSC-Laundry v. United States, 450 U.S. 1, 6 (1981) (per curiam); see id. (explaining that, of two sections of the same broader statute dealing with income tax exemption, the specific statute controlled over the general one).
States Code, they are certainly interrelated as they apply to deceptive or illegitimate trade practices. If the statutes in question are of such a relation that this maxim is applicable, then the construction evinces an "either/or" approach in that it forces the construer to choose between the two statutes.

Furthermore, this maxim becomes particularly pertinent when Congress has enacted a broad regulatory regime in one area, complimented by carve-outs to address specific concerns. Spoofing and commodities manipulation exist in such a framework. For commodities fraud, the legislative history shows that the statute was passed as part of a broad framework to allow prosecutors more freedom and "flexibility" in pursuing fraudsters. That the commodities fraud framework is broad enough to encompass spoofing is almost explicitly endorsed in Senator Pat Leahy's statement upon passage of the bill where he noted that "[b]y covering all 'schemes and artifices' . . . [the] new § 1348 will be more accessible to investigators and prosecutors and will provide needed enforcement flexibility . . ." Clearly, § 1348 fraud was intended to be a "catch-all" to cover all new kinds of scheme, and not stack on top of other criminal violations for the same conduct. As such, if an individual is accused of committing a spoofing violation, the statute specific to spoofing should replace the more general violation of commodities fraud.


228. See HCSC-Laundry, 450 U.S. at 6 (deciding whether a more specific tax statute denied petitioner an exemption or whether a related but more general statute granted one).

229. See Varity Corp., 516 U.S. at 511–12 (applying lex generalis when evaluating whether a specific provision relating to fiduciary breaches made inapplicable a broad catch-all provision, but finding that because the specific statute reflected a certain congressional concern in addition to the catch-all provision, the general statute did not undermine the specific and both were applicable).


232. Id. (emphasis added).

233. See id. (noting that § 1348 will protect investors against "all the types [of] schemes and frauds which inventive criminals may devise in the future").
The second canon of construction that helps clarify the legal questions underlying this particular double jeopardy inquiry is the merger doctrine, exemplified in the *Prince* case. In *Prince*, the Supreme Court addressed the question of whether the crime of entering a bank with the intent to commit a robbery merges with the crime of bank robbery once the robbery is committed. The defendant in *Prince* robbed a bank with a revolver and was charged in a two-count indictment with one count of robbery and one count of entering the bank with the intent to commit a robbery. Despite the government's arguments, the Court found that each offense contained the same essential nature and, therefore, merged.

Applying this maxim to spoofing and commodities fraud, we can see that the two statutes share the same essential nature. The heart of each crime is intentional deception resulting in harm, as exemplified by each statute's focus on bad faith manipulative trading. The two statutes appear to work together within a regulatory regime to ensure that all types of schemes and artifices are punishable and that crimes do not go unpunished as criminals become more "inventive." Furthermore, like the regulations in *Prince*, there is no clear congressional intent to stack penalties for these offenses. As such, the spoofing and commodities fraud

---

234. See Kirchheimer, *infra* note 36, at 518 (exploring the merger doctrine as it relates to the intersection of a preparatory, attempted, and consummated crime).

235. *Prince v. United States*, 352 U.S. 322, 328 (1957) (holding that the defendant must be convicted on the robbery count only). However, it is important to note that the Court specifically stated that its holding in the case was to be narrowed to the statute at issue and not expanded to cases at large involving "fragmentation of crimes for the purposes of punishment." *Id.* at 325.

236. *Id.* at 324.

237. *Id.* at 328 (noting that the gravamen of the offense of entering is not the actual act of entering, which would be satisfied by "simply walking through an open, public door").

238. See Disruptive Practices Guidance, 76 FED. REG. 14,943, 14,947 (proposed Mar. 18, 2011) (trading an increased scope of enforcement for greater security in preserving legitimate trading activity).

239. See *id.* (creating a good faith trading exception consistent with statutory priorities); see also Pazicky, *infra* note 172, at 811–12 (discussing how a "scheme or artifice" that constitutes commodities fraud must be construed in light of the statute's protection of legitimate mail and wire activity).


241. See *Prince*, 352 U.S. at 327 (finding that it was "manifestly the purpose of Congress" to create separate offenses rather than to "pyramid the penalties"); see also S. Rep. No. 107-146, at 20 (2002) (offering no evidence that commodities fraud as a charge was intended to do anything more than be a flexible option for prosecutors to use to convict criminals engaged in new, undefined crimes).
statutes should be enforced together, but punishments should be handed down under only one statute.

CONCLUSION

Indictments for criminal spoofing will only become more commonplace as regulators learn to adjust to a new breed of high-frequency traders. If the indictments continue to feature charges of both spoofing and commodities fraud for the same transaction, they will eventually be challenged under a claim of double jeopardy.

The elements of spoofing may be fairly reduced to two: (1) the common theme of entering orders with the intent to cancel before execution; and (2) the intent to cancel must be in bad faith with no legitimate underlying business reason. The elements of commodities fraud may be simply stated as: (1) a fraudulent intent to knowingly and harmfully deceive; (2) through the use of a scheme or artifice furthering the fraudulent intent; (3) in connection with a commodity.

Every act of spoofing satisfies the commodities fraud element of fraudulent intent to knowingly and harmfully deceive. A spoofed trade is intentionally fraudulent by definition—it was entered into with the intent to cancel. Additionally, a spoofed trade is harmful because it puts other market participants at an artificially disadvantageous market position until the spoof is complete. Every act of spoofing satisfies the commodities fraud element of using a scheme or artifice to further the fraudulent intent. Spoofing is a scheme or artifice because it is an intentional, planned action that results in harm to the victims, which satisfies analogous mail and wire

242. See Michaels et al., supra note 14 (reporting that the CFTC, SEC, DOJ, and the New York Attorney General are now all aggressively monitoring for spoofing activities).
243. See supra Part I.D. (discussing double jeopardy implications for charges with the same elements).
244. See supra notes 143–66 and accompanying text (simplifying the elements of spoofing under the direction of Gavieres v. United States, 220 U.S. 338 (1911)).
245. See supra notes 167–86 and accompanying text (applying Gavieres in the same manner to commodities fraud).
246. See supra notes 199–207 and accompanying text (using the CFTC’s spoofing guidance and the facts alleged in Coscia’s indictment to show how spoofing mechanically involves elements of fraud).
247. See Henning, supra note 17 (explaining how spoofing is not a victimless crime because the market distortion caused by spoofing not only forces other traders to buy at inflated prices, but also changes their trading patterns, often times at great cost).
248. See supra notes 196–204 and accompanying text (commenting that because the CFTC guidance includes a good faith defense, spoofing by definition will always satisfy the scheme or artifice requirement of commodities fraud as illicit trading behavior).
A SPOOF OF JUSTICE

fraud requirements for a scheme or artifice. Every act of spoofing
is made in connection with a commodity because the spoofed trade
involves the purchase and sale of such products.

Because every act of spoofing is also an act of commodities
manipulation, under the Blockburger test, a defendant cannot be
constitutionally convicted of both for the same illicit transaction. The test provides that where proof of one offense necessarily proves
another in its entirety, a defendant cannot be constitutionally
convicted of both offenses. As the preceding analysis shows, a
conviction for spoofing and commodities fraud attached to the same
transaction would be invalidated under Blockburger because of the
complete overlap of their elements.

Additionally, two canons of statutory construction help to
illuminate this principle further: lex specialis derogat lex generalis (specialized laws prevail over generalized laws) and the merger
doctrine. Both in operation and perception, the spoofing statute is
a specialized subset of the overarching regulatory framework created
by the commodities manipulation statute. Both the prevailing
opinions of industry insiders and explicit congressional intent evince
the understanding that commodities fraud as part of the Sarbanes-
Oxley regime is supposed to function as a fraud catch-all, whereas the
spoofing guidance is meant to apply only to a particular subset of
fraudulent behavior. As such, an act of spoofing should only be

249. See id. (emphasizing the connection between an intent to defraud, a
scheme or artifice requiring such intent, and the statutory framework established
by a good faith defense).

250. See supra notes 183–86 (expanding upon the “in connection with” principle).
A “connection with” a commodity is an extremely low standard and is essentially met
in every instance. See, e.g., United States v. Mahaffy, No. 05-CR-613, 2006 WL
2224518, at *12 (E.D.N.Y. 2006) (quipping that “in connection with” a commodity
concerns such a broad range of actions that the status of the victims—be they
pension funds or complex trading super-computers—is largely irrelevant).


252. Id.

253. See supra notes 115–39 (showing that giving priority to more specific statutes
over general ones is common practice in criminal law).

254. See supra notes 129–31 (combining two offenses into one when the elements
of the lesser offense are also contained in the other, more serious offense).

255. See supra notes 219–29 (summarizing the industry perception of spoofing as
simply a specific form of fraud and documenting the difference in legislative
implementation between spoofing and commodities fraud).

Leahy) (declaring in no uncertain terms that commodities fraud under Sarbanes-
Oxley gives prosecutors a broad, flexible cause of action); see also Roundtable, supra
note 42, at 21 (describing how most traders view spoofing as merely one way to
spoofing, and not both. The merger doctrine allows for a construction of two statutes whereby the lesser can be merged into the greater if the two share a gravamen, or essential nature.\(^{257}\) Spoofing and commodities fraud share an essential nature—that of deceitfully bending and manipulating other market actors for personal gain.\(^{258}\) As prosecutors adapt to chase new types of cyber-criminals, they should be wary of the double jeopardy implications for layered indictments. Convenience or uncertainty should not determine the charges a criminal defendant faces.

\(^{257}\) See supra notes 119–32 and accompanying text (explaining the difference between the unused common law merger and the merger found in Prince v. United States, 352 U.S. 322, 328 (1957), which determines whether statutes are meant to operate together or to the exclusion of one another).

\(^{258}\) See supra notes 235–38 and accompanying text (noting the similarities between the spoofing guidance’s focus on completely illegitimate trading behavior with the commodities fraud statute’s definition of “scheme or artifice”).