Vanderbilt Law Review

Volume 74
Issue 2 *March 2021*

Article 2

3-2021

Deterring Algorithmic Manipulation

Gina-Gail S. Fletcher

VANDERBILT LAW REVIEW

VOLUME 74 MARCH 2021 NUMBER 2

ARTICLES

Deterring Algorithmic Manipulation

*Gina-Gail S. Fletcher**

Does the existing anti-manipulation framework effectively deter algorithmic manipulation? With the dual increase of algorithmic trading and the occurrence of "mini-flash crashes" in the market linked to manipulation, this question has become more pressing in recent years. In the past thirty years, the financial markets have undergone a sea change as technological advancements and innovations have fundamentally altered the structure and operation of the markets. Key to this change is the introduction and dominance of trading algorithms. Whereas initial algorithmic trading relied on preset electronic instructions to execute trading strategies, new technology is introducing artificially intelligent ("AI") trading algorithms that learn dynamically from data and respond intuitively to market changes. These technological developments have exposed significant shortcomings in the effectiveness of anti-manipulation laws, particularly regarding one of their fundamental goals: deterring market manipulation.

Preventing manipulation remains a key feature of the legal regime governing the financial markets. Rampant manipulation undermines the

* Professor of Law, Duke University School of Law. J.D., Cornell Law School. For their helpful comments on this project, many thanks to participants at the 2018 AALS Financial Regulation Workshop. For helpful conversations and comments, I am grateful to Hilary J. Allen, Guy Charles, James D. Cox, Nakita Q. Cuttino, Onnig H. Dombalagian, Jessica M. Eaglin, Gregory Edwards, Jill Fisch, Gizelle Fletcher, Ajay Mehrotra, and Veronica Root Martinez. Chelsea Carlson, Madalyn Clary, Alyssa Gerstner, Emily Guillaume, Zoe Gyampoh, Michelle Le, and Mary Morris provided invaluable research assistance. All errors and omissions are my own.

viability of the market and, in the case of algorithmic manipulation, increases systemic risks within the market. Deterring algorithmic manipulation is thus essential to the viability and stability of the market. But credible and effective deterrence of wrongdoing requires certainty of punishment, which is increasingly unattainable with respect to algorithmic manipulation under the existing legal regime. Specifically, the law of manipulation tethers liability to scienter, which algorithms cannot legally form. Further, deciphering the intent of the human behind the algorithm can be a near-impossible task in all but the most egregious cases. The scienter-focused nature of the anti-manipulation framework therefore diminishes the disciplinary power of the law, weakening deterrence and incentivizing algorithmic manipulation.

This Article demonstrates that the scienter-centric analysis undergirding anti-manipulation laws creates gaps in the detection and punishment of algorithmic manipulation that weaken the current legal regime's deterrent effect. The acute failure of the law to punish algorithmic manipulation incentivizes potential wrongdoers to utilize algorithms to cloak their misdeeds, exposing the markets to significant systemic harm. Notably, unlike other scholars and policymakers that view transparency as the ultimate solution to increase accountability for algorithms, this Article highlights the potential limitations of relying primarily on transparency. Rather, the Article urges changes to the legal framework to modernize its applicability: eschew the scienter requirement and, instead, focus on the resulting harm of the algorithm on the market. Together, these proposals are likely to credibly deter algorithmic manipulation, safeguarding the viability, efficiency, and stability of the markets.

INTRODUCTION

To state the obvious: human traders are no longer at the epicenter of the financial markets. Computers running algorithmic trading programs have taken over as the primary "traders" in the market, while humans execute merely ten percent of all trades today.[1] Algorithmic trading can be categorized broadly as either preset algorithms or artificial intelligence ("AI") algorithms. Preset algorithms rely on programmed instructions to execute a specified trading strategy. These algorithms respond to new data and change their strategies within determined parameters, operating according to precise

1. Evelyn Cheng, *Just 10% of Trading Is Regular Stock Picking, JPMorgan Estimates*, CNBC (June 13, 2017, 4:49 PM), https://www.cnbc.com/2017/06/13/death-of-the-human-investor-just-10-percent-of-trading-is-regular-stock-picking-jpmorgan-estimates.html [https://perma.cc/DXZ3-YAFJ].

electronic commands. AI algorithms, on the other hand, differ meaningfully from preset algorithms—they are tasked with accomplishing a goal and left to figure out the best way to do it. AI algorithms learn from prior decisions, dynamically assess new information, and optimize their solutions to reflect new data.[2] Both forms of algorithmic trading programs are well suited for the financial markets because of their capacity to analyze large swaths of data and to execute complex trading strategies, responding almost instantaneously to new information and changed market conditions.[3]

In the past thirty years, algorithmic trading has come to dominate the financial markets, and algorithms are involved in almost every aspect of trading today. The dominance of algorithmic trading has resulted in significant benefits, including lowered trading costs, greater market accessibility, faster trade execution, and greater market efficiency and liquidity.[4] Notwithstanding these benefits, algorithms also make it easier for would-be manipulators to distort the markets, with potentially disastrous consequences, and cloak their misdeeds to avoid detection and punishment. For example, in 2010, the Dow Jones Index experienced one of the largest single-day drops in history because of the efforts of a trader to create fake buy-sell orders using an algorithmic trading program that went haywire.[5] The "2010 Flash Crash" roiled the markets for less than a half hour and yet resulted in billions of dollars of losses in market capitalization for companies and in investor funds.[6] Since then, mini-flash crashes have become more commonplace, spurred to a large extent by the prevalence of algorithmic trading and exacerbated by the use of algorithms to distort and deceive

---

2. *See, e.g.*, Michael J. McGowan, iBrief, *The Rise of Computerized High Frequency Trading: Use and Controversy*, 9 DUKE L. & TECH. REV., 2010, ¶ 2 (discussing how high frequency ("HF") trading firms use algorithms to make assumptions about the market and trade stocks in milliseconds).

3. *See id.* ¶¶ 15–18.

4. *See* Rajan Lakshmi A. & Vedala Naga Sailaja, *Survey of Algorithmic Trading Strategies in Equities and Derivatives*, 8 INT'L J. MECH. ENG'G & TECH. 817, 821 (2017) (describing the positive market impacts of algorithmic and high-frequency trading).

5. Jill Treanor, *The 2010 'Flash Crash': How It Unfolded*, GUARDIAN (Apr. 22, 2015, 1:43 PM), https://www.theguardian.com/business/2015/apr/22/2010-flash-crash-new-york-stock-exchange-unfolded [https://perma.cc/542L-JMHV]:

> In a matter of minutes the Dow Jones index lost almost 9% of its value – in a sequence[ ] of events that quickly became known as "flash crash" . . . . [O]fficials in the US [blamed the crash on] big bets by a trader on Chicago's derivatives exchange. . . . [A] mutual fund had used an automated algorithm trading strategy to sell contracts known as e-minis. It was the largest change in the daily position of any investor so far that year and sparked selling by other traders, including high frequency traders.

6. *Id.*

the markets.[7] In the past five years, both the Securities and Exchange Commission ("SEC") and the Commodity Futures Trading Commission ("CFTC") (collectively, the "Commissions") have increased their enforcement actions for market manipulation, many involving algorithmic trading, but with mixed results.[8]

The prevention of market manipulation was, and remains, a key feature of the laws governing the securities and commodities markets.[9] Rampant and unfettered market manipulation threatens the viability of the financial markets, thereby making the deterrence of market manipulation foundational to the markets' survival.[10] The Securities Exchange Act of 1934 ("Exchange Act") and the Commodity Exchange Act of 1936 ("CEA") (collectively, the "Acts"), which govern the securities and commodities markets respectively, provide the legal anti-manipulation framework applicable to the financial markets.[11] Importantly, under both Acts, liability for market manipulation hinges on proving that the accused acted with scienter—that is, intentionally or recklessly—in distorting the market. Historically, the emphasis on scienter has proven to be a difficult hurdle for regulators to overcome in enforcing anti-manipulation laws against human traders.[12] These challenges are only further exacerbated in algorithm-dominated markets, as scienter becomes more difficult to identify, decreasing the likelihood that the existing legal framework can detect and punish market manipulation.[13]

The recurrence of algorithm-related market distortion coupled with inconsistent regulatory enforcements against such misconduct raise questions about the capacity of the anti-manipulation legal framework to achieve one of its most fundamental tasks: deterring market manipulation. In today's markets, credibly deterring market

---

7. Alexander Munk & Erhan Bayraktar, *Opinion: The Stock Market Has About 12 Mini Flash Crashes a Day — and We Can't Prevent Them*, MARKETWATCH (July 31, 2017, 12:47 PM ET), https://www.marketwatch.com/story/the-stock-market-has-about-12-mini-flash-crashes-a-day-and-we-cant-prevent-them-2017-07-31 [https://perma.cc/85Y3-936H].

8. *See* Gina-Gail S. Fletcher, *Legitimate Yet Manipulative: The Conundrum of Open-Market Manipulation*, 68 DUKE L.J. 479, 484 (2018).

9. *Id.* at 488 ("Preventing market manipulation was one of the initial motivators behind the adoption of the securities and commodities laws.").

10. *See id.* at 488–90 (explaining the far-reaching consequences of market manipulation).

11. Securities Exchange Act of 1934, 15 U.S.C. §§ 78a–78qq; Commodity Exchange Act of 1936, 7 U.S.C. §§ 1–27f.

12. *E.g.*, DiPlacido v. CFTC, 364 F. App'x 657 (2d Cir. 2009). *DiPlacido* was the CFTC's first court win against price manipulation. *See id.*; *see also* Fletcher, *supra* note 8, at 501 (discussing the difficulty the SEC and the CFTC have historically had in successfully bringing price manipulation claims).

13. *See, e.g.*, United States v. Coscia, 100 F. Supp. 3d 653, 659 (N.D. Ill. 2015) (discussing the challenge of proving intent in a spoofing case, as legitimate trading and spoofing are both intentional acts).

manipulation is both a practical and philosophical issue that strains—and will continue to strain—the boundaries of how the legal framework defines and conceptualizes punishable misconduct in an increasingly algorithm-dominated market. The inability of the legal regime to credibly deter algorithm-related manipulation poses significant challenges for the efficacy of the legal framework, the reputation of the regulators, and the viability of the market. This Article grapples with the questions that arise when laws intended for humans are applied to algorithms and the consequences of the resulting mismatch.

This Article demonstrates that the application of existing anti-manipulation laws and regulations to algorithmic trading is ineffectual in holding anyone accountable for an algorithm's manipulative behavior. The law's emphasis on scienter to assign liability weakens the disciplinary power of the legal framework, which is only worsened with algorithms because scienter is easily obscured. With preset algorithms and in "easy cases," the intent of the programmer can be evident from the code and the paper trail left behind by the algorithm. In such cases, regulators can identify the programmer's manipulative intent and hold her liable for the algorithm's misconduct.[14]

In more complex cases, however, as when the algorithm distorts the market using facially legitimate transactions, determining the necessary scienter to hold the human behind the algorithm liable for manipulation becomes a difficult and near-impossible undertaking. The exercise becomes all the more challenging when AI algorithms employing machine learning are considered. In learning and problem-solving, there is no human involvement in the algorithm's decisionmaking, and, as such, any decision made is attributable to the algorithm exclusively.[15]

Legally, algorithms cannot have intent, which then raises the question: How does the law address manipulative behavior of an algorithm, both preset and AI-based? The traditional limitations of anti-manipulation laws, which place a heavy evidentiary burden on proving a trader's manipulative intent, are brought into sharp relief in algorithmic markets. Even in the absence of algorithms, proving a trader's mental state has always been difficult;[16] with the involvement

14. *See, e.g.*, Amanat v. SEC, 269 F. App'x 217 (3d Cir. 2008).

15. For an example of the analytical and strategic capabilities of AI, especially AI's potential to outperform human competitors in an environment that requires quick, complex analysis, see Kelsey Piper, *Starcraft Is a Deep, Complicated War Strategy Game. Google's Alphastar AI Crushed It.*, VOX, https://www.vox.com/future-perfect/2019/1/24/18196177/ai-artificial-intelligence-google-deepmind-starcraft-game (last updated Jan. 24, 2019, 7:04 PM EST) [https://perma.cc/385A-YGR3].

16. *See* Fletcher, *supra* note 8, at 515 (noting the "inherent difficulty" of proving intent, particularly because "direct evidence of a defendant's manipulative intent [is rarely] available").

of algorithms, it may be almost impossible in the absence of a metaphorical "smoking gun." Rather than credibly identifying and punishing algorithm-related manipulation, the scienter requirement reduces the disciplinary power of the anti-manipulation laws, concomitantly weakening the regime's deterrent effect. Fundamentally, there is a mismatch between the legal requirements to punish manipulation that require proving scienter and the realities of algorithmic design in which the intent of the programmer can be obscure or undecipherable. This incongruence undermines the capacity of the law to identify, detect, and effectively punish algorithm-related manipulation—all important factors in credible deterrence.

Under the theory of deterrence, credible and effective deterrence depends on certainty and severity of punishment for wrongdoing—the higher the likelihood of punishment and the greater the severity of punishment for misconduct, the more effective the liability framework in achieving deterrence. To date, regulators have focused primarily on increasing the severity of punishment to achieve deterrence. Fines and penalties for manipulation, particularly algorithm-related manipulation, have increased significantly over the past decade.[17] Similarly, there has been a notable expansion in criminal prosecutions for manipulation.[18] But, as research has shown, increasing the severity of sanctions is an unproductive approach to deterring misconduct if punishment is uncertain.[19] This Article demonstrates that, in all but the most egregious cases, the existing anti-manipulation framework's scienter requirement increases the difficulty of proving manipulation, makes enforcement uncertain and unequal across markets, and results in dissimilar liability for similar harm.[20]

To respond to the lack of accountability of algorithms, scholars and policymakers have often proposed improving the transparency and explainability of algorithms.[21] More transparent, explainable algorithms are less likely to be misused and, to the extent they are, it

17. *See* DIV. OF ENF'T, SEC, 2019 ANNUAL REPORT (2019), https://www.sec.gov/files/enforcement-annual-report-2019.pdf [https://perma.cc/KY6Z-T2BN] (noting increases in the number of actions filed by the SEC and monetary relief awarded in enforcement actions); Press Release, CFTC, CFTC Division of Enforcement Issues Annual Report for FY 2019 (Nov. 25, 2019), https://www.cftc.gov/PressRoom/PressReleases/8085-19 [https://perma.cc/KG7H-TUWR] (same, for the CFTC).

18. *See infra* Section II.C.1; *see also* sources cited *supra* note 17 (noting increased cooperation between financial regulators and criminal authorities).

19. *See* Mihailis E. Diamantis, *Clockwork Corporations: A Character Theory of Corporate Punishment*, 103 IOWA L. REV. 507, 518–27 (2018) (discussing the insufficiencies of deterrence-based punishments in a corporate context).

20. *See infra* Part III.

21. *See infra* Section IV.A. Please note, the terms transparent and explainable are synonyms in this context.

is easier for regulators to hold the human behind the algorithm liable for the effects of the algorithm's conduct and decisionmaking.[22] Regulators and academics, therefore, believe that being able to "see into" the algorithm is the best response to minimizing the potential for misconduct and, ultimately, deterring manipulative activity. While this Article recognizes the promise and potential of enhanced transparency, it highlights the inadequacy of relying exclusively on explainability as a panacea for the shortcomings of the legal framework in deterring algorithm-related manipulation.

This Article, therefore, proposes eliminating scienter from the anti-manipulation framework's requirements and, instead, advocates focusing on how the transaction harms the market in determining liability for algorithm-related manipulation. A harm-focused framework would eliminate the uncertainty that accompanies proving scienter, enabling regulators to more effectively punish manipulators. By increasing the efficacy of the legal regime in holding manipulators accountable for the misconduct of their algorithms, a harm-based liability regime would emphasize certainty of punishment, enhancing its potential deterrent effect. Additionally, this Article proposes harmonized regulatory oversight of algorithmic trading to minimize the gaps between the SEC's and the CFTC's approach to algorithms. The disjointed and inconsistent approach of the regulators results in dissimilar liability for similar conduct in related markets, diminishing the deterrent effect of the legal framework. Meaningful, consistent regulations applicable to algorithms are, therefore, key to credibly deterring algorithm-related market manipulation.

This Article proceeds as follows. Part I discusses the theory of deterrence, emphasizing the limitations of severity in achieving deterrence and how uncertainty undermines deterrence. This Part also examines the importance of deterrence to regulating the financial markets. Part II turns its attention to the anti-manipulation framework and how algorithms are used in the modern marketplace. Specifically, this Part provides a primer on relevant anti-manipulation provisions that are most applicable to algorithm-related manipulation. Part II also describes algorithmic trading and AI machine-learning trading programs and analyzes the possible ways in which algorithm-related manipulation could manifest in the financial markets. Part III analyzes the mismatch between algorithmic trading and the scienter-focused anti-manipulation framework, demonstrating the various ways and extent to which the law engenders uncertainty and reduces deterrence. Part IV addresses the market implications of the legal regime's

22. *See infra* Section IV.A.

failure to deter manipulation and explores potential pathways to minimize the uncertainty the law generates in punishing algorithm-related manipulation.

I. THE THEORY OF DETERRENCE

In the 1930s, the prevalence of manipulation and evidence of its rampant effects on the markets and investors propelled congressional action to regulate the financial markets and outlaw manipulation.[23] Today, despite the dramatic changes to the structure and operation of the financial markets, manipulation remains a common form of market misconduct and, indeed, the forms of manipulation have evolved alongside the markets.[24] Consequently, deterring market manipulation continues to be a central focus for both the CFTC and the SEC, the primary financial market regulators.[25]

This Part ties together the theory and reality of deterrence and provides foundational explanation and support for the importance of deterrence to the functioning of the financial markets. It begins with a discussion of deterrence theory, highlighting the importance of certainty and severity in deterring misconduct. Next, this Part examines the market benefits that arise from an effective manipulation deterrence regime.

A. A Primer on Deterrence Theory

Deterrence theory is a law and economics-based school of thought that posits a person will violate the law if her expected utility from the crime exceeds her disutility from not committing the crime.[26] That is, the theory presumes that a trader will weigh the costs and benefits of her conduct in deciding whether to engage in misconduct,

23. *See* Daniel R. Fischel & David J. Ross, *Should the Law Prohibit "Manipulation" in Financial Markets?*, 105 HARV. L. REV. 503, 503 (1991) (discussing the history of market regulations).

24. Tom C.W. Lin, *The New Market Manipulation*, 66 EMORY L.J. 1253, 1287–93 (2017) (describing the new forms of market manipulation that emerged following the flash crashes).

25. *See* Craig Pirrong, *Energy Market Manipulation: Definition, Diagnosis, and Deterrence*, 31 ENERGY L.J. 1, 6 (2010) ("Several statutes proscribe manipulation of commodity markets. These include the CEA, which has as its purpose the prevention and deterrence of price manipulation . . . ."); Fletcher, *supra* note 8, at 488 ("Preventing market manipulation was one of the initial motivators behind the adoption of the securities and commodities laws.").

26. *See* Gary S. Becker, *Crime and Punishment: An Economic Approach*, 76 J. POL. ECON. 169 (1968) (proposing an economic framework for analyzing criminal punishment); *see also* A. Mitchell Polinsky & Steven Shavell, *The Economic Theory of Public Enforcement of Law*, 38 J. ECON. LITERATURE 45, 47 (2000) (stating that a criminal will "commit the act if and only if his expected utility from doing so, taking into account his gain and the chance of his being caught and sanctioned, exceeds his utility if he does not commit the act").

such as manipulation. If a scheme will result in penalties that exceed her gains, the trader will be deterred from engaging in the scheme. By adopting measures that increase the cost of violating the law, a deterrence-focused legal framework decreases the likelihood that a person will commit a crime.[27] Thus, to deter market manipulation, the legal framework must focus on increasing the potential costs of manipulation to dissuade a would-be bad actor from engaging in misconduct.[28]

Under deterrence theory, two primary factors potentially increase the costs a criminal faces: the certainty of punishment and the potential severity of sanctions.[29] Certainty of punishment refers to the likelihood that the would-be perpetrator will suffer consequences for her crime.[30] More than just the likelihood of getting caught, certainty incorporates several probabilities such as the possibility of detection, apprehension, conviction, and sanctions.[31] Important to the assessment of certainty of punishment is the scope and substance of the legal regime. The legal framework must provide regulators with the necessary tools, resources, and authority to meaningfully address the misconduct.[32] For example, if regulators lack the necessary resources or expertise to identify misconduct, the law's deterrent effect is weakened. Likewise, if the applicable laws are narrow, only capturing the most

27. *See* Raymond Paternoster, *How Much Do We Really Know About Criminal Deterrence?*, 100 J. CRIM. L. & CRIMINOLOGY 765, 783 (2010) (explaining deterrence with a utility equation).

28. *See, e.g.*, Steven N. Durlauf & Daniel S. Nagin, *Imprisonment and Crime: Can Both Be Reduced?*, 10 CRIMINOLOGY & PUB. POL'Y 13, 16 (2011) ("The theory of deterrence is predicated on the idea that a sanction regime, by affecting the relative anticipated costs and benefits of a crime, can lead at least some members of a population to choose not to commit crime.").

29. *See* Paternoster, *supra* note 27, at 776 (discussing the two main factors that inform deterrence theory). A third factor is usually included in the cost calculation—celerity (i.e., the swiftness with which punishment is meted out). *See* Daniel S. Nagin & Greg Pogarsky, *Integrating Celerity, Impulsivity, and Extralegal Sanction Threats into a Model of General Deterrence: Theory and Evidence*, 39 CRIMINOLOGY 865, 865 (2006). But as deterrence theory has developed, certainty and severity have become the focus of regulators, academics, and policymakers. *See, e.g.*, Yvonne M. Dutton, *Crime and Punishment: Assessing Deterrence Theory in the Context of Somali Pirates*, 46 GEO. WASH. INT'L L. REV. 607, 628 (2014) ("Scholars typically focus on two principal considerations that inform the calculation of costs with a well-enforced criminal justice system: the certainty of punishment and its likely severity.").

30. Patrick J. Keenan, *The New Deterrence: Crime and Policy in the Age of Globalization*, 91 IOWA L. REV. 505, 519 (2006). It should be noted here that certainty does not refer to the certainty (or uncertainty) that one's actions constitute a crime.

31. Miriam H. Baer, *Linkage and the Deterrence of Corporate Fraud*, 94 VA. L. REV. 1295, 1306 (2008).

32. *See* Lin, *supra* note 24, at 1303 ("[U]ntil new precedents, principles, and rules are firmly established, there will be significant enforcement challenges for regulators as they combat the new methods of market manipulation.").

blatant misconduct, wrongdoers may not be deterred from breaking the law.[33]

Also important to the effectiveness of deterrence is that the legal regime must clearly identify for the public when conduct is illegal. A legal framework that is overly broad or vague may obscure the legality of conduct, thereby impairing the ability of market actors to reasonably assess whether their conduct is permissible.[34] Thus, on this prong, deterrence is effective if regulators have strong, suitable tools to enforce the regime and market actors know whether they are violating the law.

The second consideration that increases the likelihood of deterrence is the potential severity of the sanctions. Severity refers to the length of sentences, the size of potential monetary fines, or the magnitude of any other sanctions that may be levied against a person for breaking the law.[35] For example, it would be expected that a crime that carries a jail term may deter would-be criminals more than one that carries only a monetary fine. This highlights an important observation with respect to severity—to be effective at deterring, sanctions must be nuanced.[36] That is, if sanctions are all equally high, individuals have little reason to engage in lesser crimes.[37] Marginal deterrence responds to this issue by varying punishment based on the magnitude of the crime.[38] Thus, to deter manipulation, the sanctions must be severe enough to increase the cost calculus of the manipulative scheme to the trader, but also graduated to reflect varying levels of seriousness.

Early models of deterrence theory treated certainty and severity as the sole factors in achieving deterrence.[39] Neoclassical models,

---

33. Amanda M. Rose, *The Multienforcer Approach to Securities Fraud Deterrence: A Critical Analysis*, U. PA. L. REV. 2173, 2185 (2010) (illustrating how a narrow fraud prohibition would fail to deter subtle forms of fraud, despite lowering related "overdeterrence costs").

34. *See* John E. Calfee & Richard Craswell, *Some Effects of Uncertainty on Compliance with Legal Standards*, 70 VA. L. REV. 965, 966 (1984) ("If the legal standard is uncertain, even actors who behave 'optimally' in terms of overall social welfare will face some chance of being held liable because of the unpredictability of the legal rule.").

35. Daniel S. Nagin, *Deterrence in the Twenty-First Century*, 42 CRIME & JUST. 199, 203 (2013).

36. *See* Calfee & Craswell, *supra* note 34, at 999–1000 (explaining that one approach to correct the distortions caused by uncertainty is to "promulgat[e] enforcement guidelines to make enforcement decisions more predictable").

37. Steven Shavell, *Criminal Law and the Use of Nonmonetary Sanctions as a Deterrent*, 85 COLUM. L. REV. 1232, 1245 (1985) ("[R]aising the sanction with the expected harmfulness of acts gives parties who are not [initially] deterred incentives to do less harm.").

38. *See* Polinsky & Shavell, *supra* note 26, at 63 ("Deterrence of a more harmful act because its expected sanction exceeds that for a less harmful act is sometimes referred to as marginal deterrence." (emphasis omitted)).

39. *See* Nagin, *supra* note 35, at 205–06 ("[O]ne of the greatest curbs on crime is not the [severity] of punishments, but their infallibility. . . . The certainty of punishment even if moderate

however, have expanded the theory's focus to account for how individual behavior and subjective considerations may impact deterrence. First, deterrence depends on a would-be criminal's subjective evaluation of risk.[40] To the extent a criminal ignores or minimizes the risk of being caught, deterrence may be limited.[41] Criminals may underestimate the risk of being caught because they are overconfident in their ability to avoid detection or because they are risk seekers. Second, criminals may discount the severity of punishment, particularly if it occurs long after the misconduct.[42] A perpetrator fears criminal sanctions imposed tomorrow more than she does sanctions imposed in three or five years. As such, delays in the imposition of punishment are likely to cause a perpetrator to discount the impact of sanctions.[43] This time-related discounting of sanctions is also likely to diminish the deterrent effect of additional penalties.[44]

Both the subjective evaluation of risk, which affects certainty, and sanctions discounting, which affects severity, limit the efficacy of deterrence. But, whereas the latter can be addressed through alterations to the legal framework, the former is idiosyncratic. Individuals' risk assessments are important to consider in aiming to achieve deterrence, but liability regimes cannot be tailored to such persons because, simply put, they may be beyond deterrence.

Sanctions discounting, on the other hand, is attributable to the time lapse between misconduct and prosecution, and it is possible to address this issue through changes to the legal framework. Delays in the identification and prosecution of wrongdoers are common with regards to market manipulation. These crimes are often complex, and the legal framework makes it difficult for regulators and private plaintiffs to prove liability, thereby likely resulting in sanctions

---

will always make a stronger impression." (quoting Cesare Beccaria, ON CRIMES AND PUNISHMENTS 58 (David Young trans., Hackett Publ'g. Co. 1986) (1764))).

40. *See* Kimberly N. Varma & Anthony N. Doob, *Deterring Economic Crimes: The Case of Tax Evasion*, 40 CANADIAN J. CRIMINOLOGY 165, 167 (1998) ("Deterrence theory assumes that there are intelligent, informed individuals who calculate the costs and benefits (perceived or actual) of undertaking one choice or another.").

41. *See* Thomas A. Loughran, Raymond Paternoster, Alex R. Piquero & Greg Pogarsky, *On Ambiguity in Perceptions of Risk: Implications for Criminal Decision Making and Deterrence*, 49 CRIMINOLOGY 1029, 1029–30 (2011) (discussing how an individual's perceived certainty of punishment impacts the relative deterrent effect of that punishment).

42. Paternoster, *supra* note 27, at 820 ("[Scholars have] argued that in order to be effective in offsetting the perceived benefits of crime, punishment must come soon after the offense.").

43. *See* DAVID M. KENNEDY, DETERRENCE AND CRIME PREVENTION: RECONSIDERING THE PROSPECT OF SANCTION 11 (2009) (explaining how individuals measure the risk associated with committing a crime and how the estimation decreases the longer they are not sanctioned for committing a certain crime).

44. *See id.* (establishing that individuals' underestimation of punishment undermines the deterrent objective of punishment).

discounting and diminished deterrence. For example, the Flash Crash occurred in 2010, but it was not until 2015 that the CFTC and the Department of Justice ("DOJ") identified Navinder Singh Sarao as the perpetrator, and it took another three years to successfully prosecute Sarao.[45]

Given sanctions discounting, many deterrence scholars focus on making changes to liability frameworks in ways that increase the certainty of punishment rather than the severity of sanctions.[46] Enhancing certainty can reduce the time delays that result in sanctions discounting, thereby making sanctions more effective.[47] And emphasizing certainty is likely to have a greater deterrent effect on risk-seeking or overconfident criminals than would harsher sanctions.[48]

Further, beyond sanctions discounting and risk evaluation, in comparing the relative effectiveness of severity versus certainty on achieving deterrence, certainty has been found to have a stronger deterrent effect.[49] This is true not only because there is a greater objective likelihood of getting caught, but also because of its impact on

---

45. *See* Matt Levine, *Guy Trading at Home Caused the Flash Crash*, BLOOMBERG OP. (Apr. 21, 2015, 5:37 PM CDT), https://www.bloomberg.com/opinion/articles/2015-04-21/guy-trading-at-home-caused-the-flash-crash [https://perma.cc/UL2Q-EHCU] (explaining how Navinder Sarao's spoofing strategy caused the Flash Crash); Margot Patrick, *'Flash Crash' Trader Navinder Sarao Worked with Fund Network Now Under Investigation*, WALL ST. J. (Jun. 17, 2015, 3:54 AM ET), https://www.wsj.com/articles/flash-crash-trader-navinder-sarao-worked-with-fund-network-now-under-investigation-1434527646 [https://perma.cc/SQ8K-RY8H] (explaining the strategy Sarao used that led to the Flash Crash); CFTC v. Sarao Futures Ltd., No. 15-cv-3398, 2016 WL 8257513 (N.D. Ill. Nov. 14, 2016) (discussing Sarao's manipulating scheme and holding Sarao liable for engaging in spoofing).

46. *See, e.g.*, Samuel Cameron, *The Economics of Crime Deterrence: A Survey of Theory and Evidence*, 41 KYKLOS 301, 306 (1988) (explaining that the degree of certainty of punishment is essential to deter crime and arguing that severity of punishment is ineffective if the individual believes he will not be punished); *see also* KENNEDY, *supra* note 43, at 16 ("The higher the chance of getting caught, and the higher the associated costs, the less likely that crime will be committed.").

47. *See* Mark A. Cohen, *The Economics of Crime and Punishment: Implications for Sentencing of Economic Crimes and New Technology Offenses*, 9 GEO. MASON L. REV. 503, 514–15 (2000) (providing empirical evidence that criminals are more deterred by certain punishment than severe sanctions).

48. A. Mitchell Polinsky & Steven Shavell, *On the Disutility and Discounting of Imprisonment and the Theory of Deterrence*, 28 J. LEGAL STUD. 1, 5 (1999) ("For risk-preferring individuals, the severity of imprisonment sanctions has a lesser effect on deterrence than the probability of sanctions . . . .").

49. *See* Nagin & Pogarsky, *supra* note 29, at 865 ("[P]unishment certainty is far more consistently found to deter crime than is punishment severity, and the extralegal consequences of crime seem at least as great a deterrent as do the legal consequences."); VALERIE WRIGHT, SENT'G PROJECT, DETERRENCE IN CRIMINAL JUSTICE: EVALUATING CERTAINTY VS. SEVERITY OF PUNISHMENT 4 (2010), https://www.sentencingproject.org/wp-content/uploads/2016/01/Deterrence-in-Criminal-Justice.pdf [https://perma.cc/QLG3-KF5M] ("Criminological research over several decades and in various nations generally concludes that enhancing the certainty of punishment produces a stronger deterrent effect than increasing the severity of punishment.").

public perception with respect to certainty of punishment.[50] As an individual either (1) breaks the law and successfully avoids detection or punishment, or (2) witnesses others being successful in their criminal activities, she may perceive a decrease in the probability that she will be caught and punished for her misdeeds.[51] But if she witnesses others being caught, a would-be perpetrator may evaluate that there is a strong likelihood that she will be detected and, therefore, refrain from engaging in misconduct.

While not all forms of crime can be meaningfully analyzed under deterrence theory, monetary crimes, such as market manipulation, are amenable to the theory.[52] Manipulation involves planning, reasoning, and having an awareness of how the markets work. Indeed, in discussing manipulation, regulators often frame their efforts in terms that presume a defendant calculates the profitability of her schemes, crafting regulatory responses aimed at altering that calculus.[53]

1. Deterrence & Uncertainty

To fully appreciate the role certainty plays in deterrence, it is necessary to unpack how uncertainty may arise in a legal framework. There are two primary forms of uncertainty that may diminish the deterrent effect of a liability framework. First, there may be legal uncertainty as to whether the perpetrator's conduct is illegal.[54] Imprecise and unwieldly laws that claim to proscribe everything ultimately deter very little or, in some cases, nothing at all.[55] Further, to the extent similar conduct may result in dissimilar penalties, legal uncertainty hampers deterrence. Deterrence theory presumes that a

50. *See* Paternoster, *supra* note 27, at 785 (explaining how "perceptual properties of punishment" affect deterrence).

51. KENNEDY, *supra* note 43, at 11 (describing this as the "experiential effect," where, "as time passes, many people come to lower their estimates of the risks of offending ," and "as offenders commit crimes and escape sanction, or see others do so, they adjust their risk estimates downward").

52. Baer, *supra* note 31, at 1309.

53. *See Anti-manipulation and Anti-fraud Final Rules Fact Sheet*, COMMODITY FUTURES TRADING COMM'N, https://www.cftc.gov/sites/default/files/idc/groups/public/@newsroom/documents/file/amaf_factsheet_final.pdf (last visited Sept. 18, 2020) [https://perma.cc/W64F-QKH4]. When filing complaints against market manipulation, the SEC will request both civil fines and disgorgement of any gains from market manipulation, including prejudgement interest. *See, e.g.*, Final Judgement as to Defendant Howard M. Appel at 4, SEC v. Appel, No. 18-cv-3200-PD (E.D. Pa. May 10, 2019), ECF No. 11 ("Defendant is liable for disgorgement . . . together with prejudgment interest . . . .").

54. *See* Baer, *supra* note 31, at 1313 ("[C]ritics of deterrence theory contend that most individuals are unaware of, or lack the ability to understand, complex legal rules.").

55. *See* Geraldine Szott Moohr, *On the Prospects of Deterring Corporate Crime*, 2 J. BUS. & TECH. L. 25, 28–30 (2007) ("In prohibiting everything, vague and broad criminal laws prohibit nothing.").

criminal knows her conduct is illegal;[56] if she does not know that her conduct violates the law, she lacks the knowledge necessary to assess the costs and benefits stemming from her conduct.

The problematic effect of this form of uncertainty on deterrence is one of overdeterrence of honest actors but underdeterrence of criminals. For honest, risk-averse individuals who fear being punished, legal uncertainty presents too great a risk to warrant continued participation in the markets and, as such, they prefer to exit to minimize the probability of punishment.[57] On the other hand, under an uncertain legal regime, bad actors may proliferate as they rely on the existing ambiguities to defend their conduct and evade punishment.

Many have written about the confusion and ambiguities that plague securities and commodities anti-manipulation laws.[58] Neither the Exchange Act nor the CEA defines manipulation,[59] and in some instances, the laws diverge in how to treat manipulative conduct.[60] As

---

56. Baer, *supra* note 31, at 1310 ("Deterrence theory presumes that criminals know they are violating the law.").

57. *See* Calfee & Craswell, *supra* note 34, at 995 ("Even when the probability of punishment is less than one, if that probability declines as defendants take more care, then defendants may tend to overcomply."); Rose, *supra* note 33, at 2190:

> The bottom line is that lawmakers face a clear tradeoff in setting sanctions: set sanctions high in an effort to deter more fraud, but risk increasing overdeterrence costs, or set them low to minimize overdeterrence costs, but risk increasing the incidence of fraud. If we assume, as seems reasonable, that those inclined to commit fraud are more likely to be risk seeking, whereas those inclined to obey the law are more likely to be risk averse, the tradeoff in sanction setting becomes even starker.

58. *See e.g.*, Joseph A. Grundfest & A.C. Pritchard, *Statutes with Multiple Personality Disorders: The Value of Ambiguity in Statutory Design and Interpretation*, 54 STAN. L. REV. 627, 653 (2002) (taking issue with the "strong inference" pleading standard to prove scienter under the Private Securities Litigation Reform Act as there is no "precise definition" of the standard and it had at "least three different articulations"); Craig Pirrong, *Commodity Market Manipulation Law: A (Very) Critical Analysis and a Proposed Alternative*, 51 WASH. & LEE L. REV. 945, 1013 (1994) (describing the state of commodity market manipulation law as "extraordinarily misguided" due to its confusing and contradictory nature and thus creating "[a] law [that] is less a deterrent to manipulators than [it is] an invitation to them").

59. Fischel & Ross, *supra* note 23, at 506 (highlighting that despite having "the prevention of manipulation as [their] primary goal . . . neither the Securities Exchange Act nor the Commodity Exchange Act attempts to define [manipulation]"); Jerry W. Markham, *Manipulation of Commodity Futures Prices—The Unprosecutable Crime*, 8 YALE J. ON REGUL. 281, 313 (1991) (stating that the "Commodity Exchange Act did not define manipulation," and so "the task of interpretation was left to the courts and to another small agency within the Department of Agriculture"); Wendy Collins Perdue, *Manipulation of Futures Markets: Redefining the Offense*, 56 FORDHAM L. REV. 345, 346–48 (1987) (criticizing federal laws for prohibiting manipulation for over sixty-five years while simultaneously failing to provide a proper definition, before exploring a different perspective to determining manipulation based on "conduct that would be uneconomical or irrational, absent an effect on market price").

60. *See* Fletcher, *supra* note 8, at 484–86 (underscoring the difference between the Commissions' treatment of open-market manipulation as requiring only manipulative intent and the courts' treatment of open-market manipulation as requiring both intent *and* "something more").

the schemes underlying market manipulation evolve, especially with the increased utilization of algorithms and AI straddling the line between legal and illegal conduct, the ambiguities in the anti-manipulation framework challenge its effectiveness at deterring manipulation. This is especially true for new, less understood forms of market manipulation, such as algorithm-related distortion or manipulation. Thus, in assessing the deterrent effect of the anti-manipulation liability regime, one must consider whether and to what extent the framework creates uncertainty as to the legality of the conduct in question.

Second, there may be legal uncertainty with respect to the capacity of the state to successfully prosecute a criminal. This uncertainty differs from legal ambiguity in that its focus is on the government's capabilities to prosecute, which would include its resources, the burdens of proof it faces, and any evidentiary hurdles the legal regime requires prior to imposing liability. In considering the certainty of punishment, deterrence theory places emphasis on identification of wrongdoing and government willingness to prosecute perpetrators.[61] Per this line of reasoning, if the government can identify and is willing to prosecute wrongdoing, then there is certainty of punishment. Even if the two criteria are met, however, there may be uncertainty of punishment if the state is unable to prosecute.[62] For example, the state may be ill-equipped to bring charges due to limited resources. Similarly, if the legal regime renders the misconduct effectively beyond prosecution because of near-impossible standards of proof and evidentiary burdens, then the deterrent effect of the liability framework will be muted.[63]

There is intense legal debate as to whether the anti-manipulation legal regime needlessly hampers the ability of regulators to prosecute market manipulation. Indeed, one scholar has described manipulation in the commodities market as an "unprosecutable" crime because of the significant burdens imposed on the state to hold traders liable.[64] For example, as traders outmaneuver and outspend regulators

61. *See* Baer, *supra* note 31, at 1344–45 (discussing how the government's increased efforts to prosecute crime has a deterrent effect on wrongdoers).

62. *See id.* at 1343 (explaining that an increase in allocation of resources is necessary for an increased probability of detection).

63. *See* J. KELLY STRADER, UNDERSTANDING WHITE COLLAR CRIME 111–17 (4th ed. 2017) (explaining how courts have not established clear standards for certain elements for crimes under the Securities Laws, thus resulting in highly contested cases).

64. *See* Markham, *supra* note 59, at 357 ("[W]here a gross manipulation occurs, the government is still faced with the imposing burden of proving that the price was artificial and that the trader was attempting to create an artificial price rather than exploiting a market situation based upon natural forces.").

on trading technology, a public sense of uncertainty may develop as to whether the state can effectively restrict manipulative and disruptive practices that exploit technological innovations. In turn, this contributes to an overall perception that both the regulators are weak and that manipulation is rampant is the markets.[65] Thus, the limited resources of regulators become a source of uncertainty that impedes deterrence of market manipulation. In sum, the efficacy of the liability regime in deterring misconduct depends on the tools and resources that the state has at its disposal to prosecute. A legal enforcer weakened by burdensome standards of proof and limited resources does not serve as an effective deterrent to misconduct.

2. The Limits of Emphasizing Severity

Deterrence theory seeks to increase the cost of misconduct to potential perpetrators by increasing the certainty of punishment and the severity of sanctions. In keeping with the broader trend in the U.S. criminal justice system of preferring severity over certainty in deterring criminal conduct,[66] lawmakers and the Commissions have focused their efforts to deter market manipulation on increasingly harsher penalties.[67] Specifically, the Commissions have consistently increased the size of monetary penalties levied against wrongdoers each year. For example, in 2018, the SEC levied penalties totaling $1.439 billion, almost doubling its 2017 penalties of $832 million.[68] Similarly, the size of the CFTC's penalties has increased significantly in the past few years. During 2016 and 2017, the CFTC had three judgments each year

65. *See, e.g.*, Fletcher, *supra* note 8, at 493 (discussing the Enron and WorldCom corporate frauds and their effect on market perception); Ana Carvajal & Jennifer Elliot, *The Challenge of Enforcement in Securities Markets: Mission Impossible?* (Int'l Monetary Fund, Working Paper No. 09/168, 2009), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1457591 [https://perma.cc/UH22-FHPY] (analyzing the effectiveness of market enforcement and its subsequent effects on investors' confidence in the market).

66. *See, e.g.*, Kelli D. Tomlinson, *An Examination of Deterrence Theory: Where Do We Stand?*, FED. PROB., Dec. 2016, at 33, 34 ("The United States has experienced an incarceration binge over the last several decades; in 1980 there were approximately 501,886 incarcerated persons in prisons and jails, and at year-end 2009 there were 2,284,913.").

67. David M. Becker, *What More Can Be Done to Deter Violations of the Federal Securities Laws?*, 90 TEX. L. REV. 1849, 1852 (2012).

68. SEC. & EXCH. COMM'N, DIVISION OF ENFORCEMENT ANNUAL REPORT 11 (2018), https://www.sec.gov/files/enforcement-annual-report-2018.pdf [https://perma.cc/3R92-T76J]. To be clear, this number represents penalties for all violations of the securities laws, not only market manipulation cases.

that totaled $10 million or more; in contrast, in 2018, the agency had three times as many monetary judgments of that size.[69]

The focus on severity is also evident in the enactment of legislation granting the Commissions access to more severe sanctions for market manipulation. The Dodd-Frank Act, for example, granted the SEC the authority to impose civil money penalties in administrative proceedings.[70] Prior to this amendment, the SEC was required to seek civil money penalties from a federal district court and, thus, was limited in the sanctions it could seek in administrative proceedings.[71] Further, the Dodd-Frank Act increased the penalty amounts that the SEC could impose in these proceedings by fifty percent.[72] With respect to the CFTC, the Dodd-Frank Act authorized the agency to impose civil penalties equal to the greater of one million dollars or treble damages for violations of its anti-manipulation provisions.[73] In adjudicating market manipulation cases, the courts likewise focus on severity of sanctions to deter future misconduct. In their sentencing, courts favor stricter, harsher punishments for market manipulators, altering the costs of the crime relative to its benefits, and thereby promoting deterrence.[74] As one court stated, market manipulation "when detected, must be heavily punished if deterrence is to be achieved."[75]

---

69. COMMODITY FUTURES TRADING COMM'N, ANNUAL REPORT ON THE DIVISION OF ENFORCEMENT 9 (2018), https://www.cftc.gov/sites/default/files/2018-11/ENFAnnualReport111418_0.pdf [https://perma.cc/BZ9Q-BWDM]. Again, this number represents all penalties for violations of commodities laws, not only market manipulation cases.

70. 15 U.S.C. § 78u-2(a)(1).

71. Gideon Mark, *SEC and CFTC Administrative Proceedings*, 19 U. PA. J. CONST. L. 45, 46 (2016):

> Prior to Dodd-Frank, the SEC's authority to impose civil penalties in an administrative proceeding ("AP") was limited to registered entities and persons associated with registered entities . . . . For all other defendants the SEC was required to file a civil enforcement action in federal court. One consequence of this limitation was that the SEC historically commenced only 60% of its new cases as APs.

72. *Compare* Securities Enforcement Remedies and Penny Stock Reform Act of 1990, Pub. L. No. 101-429, § 101(d)(2)(a), 104 Stat. 931, 932 (1990) (amending section 20 of the Securities Act of 1933, 15 U.S.C. § 77t, to include a $5,000 maximum penalty for individuals), *with* Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, § 929P(g)(2)(A), 124 Stat. 1376, 1862 (2010) (increasing the penalty against individuals to $7,500).

73. *See* Dodd-Frank Wall Street Reform and Consumer Protection Act, § 753(a) (amending the Commodity Exchange Act § 6(c), 7 U.S.C. §§ 9, 15, to expand the CFTC's authority to pursue anti-manipulation violations); *id.* (outlining the range of penalties for anti-manipulation violations).

74. *See*, *e.g.*, United States v. Castaldi, 743 F.3d 589, 594 (7th Cir. 2014) ("The judge addressed deterrence, both specific and general, and said that a Guideline sentence would not be adequate as a deterrent to this crime. . . . As noted, the sentence was the longest possible under the plea agreement: maximum consecutive sentences for a total of 276 months (twenty-three years) in prison").

75. Reddy v. CFTC, 191 F.3d 109, 127 (2d Cir. 1999).

This focus on severity, however, is misplaced and ineffective against misconduct such as market manipulation. Empirical research supports this, finding that there is little to no deterrent effect resulting from harsher penalties.[76] Indeed, according to research, harsher penalties may erode the deterrent effect of a liability regime by making sanctions less stigmatizing;[77] reducing conviction rates;[78] and, even, increasing crime.[79] In the financial markets, the emphasis on severity has likely done little to deter manipulation.

Public perception of the Commissions is that they are weak and ineffective, especially in safeguarding the markets against manipulation.[80] Indeed, despite the steady increase in monetary sanctions for market manipulation, some have accused the Commissions of being too lenient against defendants. For example, the SEC often allows defendants to pay a fine while neither admitting nor denying wrongdoing.[81] Similarly, in one of its first spoofing cases, the CFTC banned Michael Coscia from trading for only one year, which some saw as too lenient given the severity of the crime.[82] Thus, even with increased sanctions against defendants, the Commissions are not

---

76. *See, e.g.*, Anthony N. Doob & Cheryl Marie Webster, *Sentence Severity and Crime: Accepting the Null Hypothesis*, 30 CRIME & JUST. 143 (2003) (explaining that more severe sentences are not more effective than less severe sentences in reducing crime).

77. Daniel S. Nagin, *Criminal Deterrence Research at the Outset of the Twenty-First Century*, 23 CRIME & JUST. 1, 22 (1998) ("For an event to be stigmatizing it must be relatively uncommon.").

78. Tracey L. Meares, Neal Katyal & Dan M. Kahan, *Updating the Study of Punishment*, 56 STAN. L. REV. 1171, 1185 (2004) ("High penalties, instead of increasing conviction rates, may decrease them. As penalties increase, people may not be as willing to enforce them because of the disproportionate impact on those caught.").

79. Tomislav V. Kovandzic, John J. Sloan, III & Lynne M. Vieraitis, *"Striking out" as Crime Reduction Policy: The Impact of "Three Strikes" Laws on Crime Rates in U.S. Cities*, 21 JUST. Q. 207, 207, 234 (2004).

80. *See, e.g.*, Dennis Kelleher, *How the SEC Let Wall Street Run Wild*, POLITICO (Dec. 12, 2015, 7:23 AM EST), https://www.politico.com/agenda/how-the-sec-let-wall-street-run-wild-000004 [https://perma.cc/N83S-TT75] ("Today, the SEC is failing to enforce the law and write regulations to deal with the profound flaws in our markets that create dangerous instability and harm everyday investors. . . . Enforcement of delinquent-filing actions does not deter market manipulation, major fraud and other serious misconduct at our largest financial institutions."); *see also* MICHAEL LEWIS, FLASH BOYS: A WALL STREET REVOLT 200–01 (2014) (attributing the drop in stock ownership to the notion that the market is unfair).

81. *See, e.g.*, Edward Wyatt, *Responding to Critics, S.E.C. Defends 'No Wrongdoing' Settlements*, N.Y. TIMES: DEALBOOK (Feb. 23, 2012, 5:17 PM), https://dealbook.nytimes.com/2012/02/22/s-e-c-chairwoman-defends-settlement-practices/ [https://perma.cc/9AC6-FWBN] ("The [SEC] frequently settles cases . . . by allowing a Wall Street firm to pay a fine . . . . The settlements usually do not require the defendants to admit any wrongful conduct. . . . Some people have questioned [the] deterrent effect and the value of relying on the "neither admit nor deny" clause.").

82. Press Release, Bart Chilton, Comm'r, CFTC, Concurring Statement of Comm'r Bart Chilton in the Matter of Panther Energy Trading LLC and Michael J. Coscia (July 22, 2013), https://www.cftc.gov/PressRoom/SpeechesTestimony/chiltonstatement072213 [https://perma.cc/7AHL-YG2F].

viewed as effective regulators, thereby minimizing the deterrence of the regulatory regime.

While these critiques of the Commissions appear to be debates over the severity or leniency of sanctions, the undercurrent in the conversation is one of certainty. Although the Commissions are increasing their sanctions, these higher sanctions are less impactful given the lack of certainty of punishment for manipulation. Ensuring certainty of punishment, therefore, ought to be the Commissions' principal focus to enhance deterrence of manipulation in the markets.

B. The Benefits of Deterrence for Financial Markets

Manipulation undermines the fundamental purpose of the financial markets—efficient capital allocation.[83] Manipulation weakens market efficiency by injecting inaccurate information into the markets and undermines investor protection, causing investors to exit the markets. Deterrence is key to limiting the pernicious effects of manipulation on the financial markets. An effective deterrence framework minimizes the consequences of manipulation, resulting in two overarching benefits for the market: enhanced market efficiency and greater investor protection. Deterrence, therefore, is at the core of financial regulators' goals in overseeing and regulating the markets.

1. Enhanced Market Efficiency

Markets are efficient when they quickly incorporate available information into prices.[84] The two primary market characteristics that contribute to market efficiency are price accuracy and liquidity.[85] Price accuracy refers to the reliability of a price as a reflection of the fundamental value of an asset.[86] Liquidity refers to the ready availability of other traders with whom to trade.[87] The more liquid a market is, the easier it is for a trader to execute transactions without

83. *See* Yesha Yadav, *How Algorithmic Trading Undermines Efficiency in Capital Markets*, 68 VAND. L. REV. 1607, 1631 (2015) ("Efficiency in processing information can, in theory at least, also help foster better allocation of capital in securities markets, so-called allocative efficiency.").

84. Lynn A. Stout, *The Mechanisms of Market Inefficiency: An Introduction to the New Finance*, 28 J. CORP. L. 635, 639 (2003) ("[A] market is 'efficient' when prices always fully reflect available information.").

85. Fletcher, *supra* note 8, at 490.

86. *Id.* at 490–91.

87. Douglas J. Elliott, *Market Liquidity: A Primer*, BROOKINGS INST. 3 (2015), https://www.brookings.edu/wp-content/uploads/2016/07/Market-Liquidity.pdf [https://perma.cc/QVA9-J6QT] (explaining that liquidity emerges from ease of transactions based on time restraints, minimal transaction costs, and potential buyers willing to pay theoretical market value).

significant market movement.[88] Greater market liquidity increases price accuracy and market efficiency as it allows traders to more easily reveal information through their transactions. Decreased liquidity reduces market efficiency because traders that cannot readily transact are likely to discount the value of an asset to account for this reality.

Manipulation undercuts these two pillars of market efficiency by distorting informational efficiency of the markets. As to price accuracy, manipulation corrupts the information reflected in the price of an asset, thereby making the price less accurate. Manipulation schemes inject inaccurate information into the markets, which causes asset prices to deviate from their fundamental value.[89] Thus, a trader's ability to alter pricing data on which the market relies negatively impacts market efficiency and contributes to capital misallocation within the markets.

Relatedly, in the face of manipulation, market liquidity also diminishes. As traders realize that asset prices are inaccurate, they may withdraw from the market to protect themselves from being on the losing end of a manipulative trade.[90] The resulting illiquidity is akin to a tax on the markets that discourages honest traders from participating, further divorcing the market price of the asset from its fundamental value. Effective deterrence of manipulation, therefore, improves market efficiency by reducing the impact of market misconduct on the accuracy of asset pricing and the liquidity of the markets.

2. Greater Investor Protection

A familiar mechanism associated with investor protection is the mandatory disclosure system, which undergirds much of the financial regulatory system.[91] Along with required disclosures, investor

88. *See id.* (discussing how liquid markets allow for assets to be sold quickly before a significant price movement can occur).

89. Zohar Goshen & Gideon Parchomovsky, *The Essential Role of Securities Regulation*, 55 DUKE L.J. 711, 730 (2006) ("The larger the deviation between price and value and the longer it takes for prices to revert to value, the less efficient the market is."); Steve Thel, *Regulation of Manipulation Under Section 10(b): Security Prices and the Text of the Securities Exchange Act of 1934*, 1988 COLUM. BUS. L. REV. 359, 398 ("Prices may change in response to false or misleading communications since security prices reflect what investors believe, even if those beliefs are wrong.").

90. *See* Gina-Gail S. Fletcher, *Engineered Credit Default Swaps: Innovative or Manipulative?*, 94 N.Y.U. L. REV. 1073, 1113 (2019) ("Engineered CDS transactions decrease the liquidity of the CDS market because traders are likely to withdraw from the markets owing to the decreased utility of CDS as risk mitigation tools.").

91. *See* 15 U.S.C. § 78m(j) (requiring a publicly traded company to give annual disclosures of the firm's "financial condition, changes in financial condition, [and] results of operations"). The SEC has created other rules that require disclosures on a quarterly basis and after any material changes in the firm's financial condition or operations. *See* 17 C.F.R. § 249.308a (2019) (requiring

protection also extends to safeguarding market participants from abuses, such as fraud, misstatements, and manipulation.[92] Ensuring that dishonest or unscrupulous traders do not exploit other market participants for profit is paramount to the market's viability. To the extent investors doubt the integrity of the market or doubt that regulators cannot protect them from abuses, they are unlikely to invest their capital in the markets.[93] Or, should they choose to invest, they will discount the price of assets being sold to account for the possibility of market abuses.[94] Thus, investor protection through the deterrence of market distortion is a central goal of the anti-manipulation framework.

II. MODERN MARKETS, MODERN MANIPULATION

The financial markets have evolved significantly in recent years with the rise of technology and innovation. The result is not only a change in how the financial markets operate, but also the development of trading techniques and strategies that exploit technological advances to the detriment of the markets. Yet, despite these technological advances, the law of market manipulation is largely unchanged since it was enacted in the 1930s. The twofold consequences of the law's failure to evolve are that the regulatory framework is ill-equipped to address novel developments in the financial markets and the law fails to effectively deter misconduct.

This Part examines the contours of the existing legal and regulatory framework of market manipulation, highlighting the standards of proof necessary to hold someone liable for manipulation. Next, it examines the different ways in which technology is used in trading, specifically discussing algorithmic trading, high-frequency trading, and artificial intelligence in the financial markets. Lastly, this

---

quarterly transition reports, called Form 10-Qs); 17 CFR § 249.308 (2019) (requiring reports of any material changes, called Form 8-Ks). Additionally, when first going public, a company is required to give detailed disclosures in its registration statement. *See* 15 U.S.C. § 78l(a)–(b) (outlining registration requirements); 17 CFR § 239.11 (2020) (providing Form S-1 as the form for registration statements).

92. 1 LOUIS LOSS, JOEL SELIGMAN & TROY PAREDES, FUNDAMENTALS OF SECURITIES REGULATION 4 (7th ed. 2018).

93. This is a classic "lemons market," as first described by George Akerlof. According to Akerlof, in a market in which buyers do not know which cars are worth their asking price and which are not (that is, the lemons), the buyer will simply treat all cars like lemons. The result will be that worthy car sellers will leave the markets, unable to get an accurate price for their products, and lemon sellers will remain in the market. *See* George A. Akerlof, *The Market for "Lemons": Quality Uncertainty and the Market Mechanism*, 48 Q.J. ECON. 488, 489–90 (1970).

94. *See* Dionigi Gerace, Charles Chew, Christopher Whittaker & Paul Mazzola, *Stock Market Manipulation on the Hong Kong Stock Exchange*, 8 AUSTRALASIAN ACCT. BUS. & FIN. J. 105, 136 (2014) ("Manipulation is . . . associated with . . . reduced volume as investors exit the market rationally in fear of trading with a manipulator.").

Part examines possible examples of algorithmic manipulation as a precursor to later analysis of the limitations of the anti-manipulation framework.

A. The Existing Anti-Manipulation Framework

Jurisdiction over market manipulation is principally divided between the SEC and the Exchange Act on the one hand, and the CFTC and the CEA on the other. Owing to markets being traditionally human-dominated, anti-manipulation provisions in the Exchange Act and the CEA primarily center liability on the mental state of the actor. This Part examines four anti-manipulation provisions most applicable to algorithmic trading, highlighting the mental state required for each.

1. Price Manipulation

Price manipulation is proscribed under both Exchange Act section 9(a)(2) and CEA sections 6(c)(3) and 9(a)(2). Under the Acts, to prove price manipulation, the plaintiff must demonstrate that (1) the defendant had the ability to influence prices, (2) an artificial price existed, (3) the defendant caused the artificial price, and (4) the defendant specifically intended to cause the artificial price.[95] Courts have indicated that, under the Exchange Act, evidence that the defendant specifically intended to manipulate the price is unnecessary; instead, a defendant may be liable if it can be proven that she willfully engaged in the misconduct underlying the violation.[96] But to hold a defendant liable for price manipulation under the CEA, the CFTC must prove that the accused acted with the specific intent to create an

95. *In re* Amaranth Nat. Gas Commodities Litig., 730 F.3d 170, 173 (2d Cir. 2013); CFTC v. Wilson, 27 F. Supp. 3d 517, 531 (S.D.N.Y. 2014); *see also* Fletcher, *supra* note 8, at 500–01 (discussing the elements of the price manipulation standard).

96. "Manipulative purpose" is a required element to prove manipulative practice under section 9(a)(2) of the Exchange Act. 15 U.S.C. § 78i. Under the penalty provisions of the Exchange Act, liability attaches when a person "willfully violates [the statute]." 15 U.S.C. § 78ff(a). The United States Court of Appeals for the Second Circuit has interpreted this language not to necessitate proof of intent to specifically violate the Exchange Act, but rather the intent to willfully commit the act constituting the violation, and other courts have followed suit. United States v. Schwartz, 464 F.2d 499, 509 (2d. Cir. 1972); *see, e.g.*, United States v. Koenig, 388 F. Supp. 670, 711 (S.D.N.Y. 1974) (applying the Second Circuit's interpretation to not require proof of intent to violate the Exchange Act); United States v. Erikson, 601 F.2d 296, 304 n.12 (7th Cir. 1979) ("No proof of specific intent to violate the securities laws is necessary." (citing *Schwartz*, 464 F.2d at 509)). See *infra* Section II.A.2 for a discussion of the challenges of the recklessness standard.

artificial price that does not reflect legitimate forces of supply and demand.[97]

The specific intent standard is a particularly high standard to meet and has resulted in the CFTC not litigating many price manipulation cases. Indeed, because of the exacting burden of proof imposed on the plaintiff to prove price manipulation, the CFTC, in its forty-year history, has managed to successfully prosecute only one price manipulation case.[98] In an algorithmic world, it is questionable whether the price manipulation provision can meaningfully capture anything other than the most egregious misconduct in the markets given the high mental state requirement.

2. Fraud-Based Manipulation

The most widely used anti-manipulation provision is Exchange Act section 10(b) and its accompanying Rule 10b-5.[99] Together, they provide the SEC with a broad basis to regulate most forms of abusive market behavior. A successful section 10(b) and Rule 10b-5 action requires the plaintiff to show that (1) the defendant made a material misstatement or defrauded another party, (2) she committed these actions intentionally, (3) her actions were related to a securities sale or purchase, (4) the plaintiff or the markets in general relied on the misstatement or fraudulent conduct, and (5) the plaintiff was harmed.[100] In 2010, the CFTC was granted similar anti-fraud authority under CEA section 6(c)(1), which mirrors Exchange Act section 10(b). Per CEA section 6(c)(1), the CFTC enacted Rule 180.1, which is identical to Rule 10b-5 in all material respects, signaling the incorporation of decades of Rule 10b-5 jurisprudence and interpretation.[101]

Under Rules 10b-5 and 180.1, to hold a defendant liable, the Commissions or private plaintiffs must show that the defendant acted

---

97. Prohibition on the Employment, or Attempted Employment, of Manipulative and Deceptive Devices and Prohibition on Price Manipulation, 76 Fed. Reg. 41,398, 41,408 (July 14, 2011) (to be codified at 17 C.F.R. pt. 180).

98. Shaun D. Ledgerwood & Paul R. Carpenter, *A Framework for the Analysis of Market Manipulation*, 8 REV. L. & ECON. 253, 254 (2012) (noting that Bart Chilton, commissioner of the CFTC, admitted that "in 35 years, there has been only one successful prosecution [DiPlacido v. CFTC] for manipulation").

99. 15 U.S.C. § 78j(b); 17 C.F.R. § 240.10b-5 (2019).

100. *See, e.g.*, ATSI Commc'n, Inc. v. Shaar Fund, Ltd., 493 F.3d 87, 105 (2d Cir. 2007).

101. The CFTC's incorporation of Rule 10b-5 jurisprudence has been explicit:

> Given the similarities between CEA section 6(c)(1) and Exchange Act section 10(b), the [CFTC] deems it appropriate and in the public interest to model final Rule 180.1 on SEC Rule 10b-5. To account for the differences between the securities markets and

either intentionally or recklessly.[102] While the Supreme Court has never decided whether the scienter requirement encompasses recklessness, every federal appellate court has held that recklessness is sufficient, although the level of recklessness varies across the circuits.[103] Courts have defined recklessness to be conduct that "departs so far from the standards of ordinary care that it is very difficult to believe the [actor] was not aware of what he was doing."[104] To meet the recklessness standard, the Commissions or private plaintiffs must demonstrate a strong inference of scienter, either by showing that the defendant had the motive and opportunity to manipulate or through strong circumstantial evidence of conscious misbehavior.[105]

Rule 10b-5 is the workhorse of the anti-manipulation framework, providing the basis for the majority of the anti-manipulation cases brought by the Commissions and private plaintiffs. Despite its recency, the same is expected of Rule 180.1 given that it greatly expands the CFTC's manipulation authority and is closely modeled on Rule 10b-5.[106] Although the scienter requirement for Rules

---

> derivatives markets, the [CFTC] will be guided, but not controlled, by the substantial body of judicial precedent applying the comparable language of SEC Rule 10b-5.

Prohibition on the Employment, or Attempted Employment, of Manipulative and Deceptive Devices and Prohibition on Price Manipulation, 76 Fed. Reg. at 41,399 (citation omitted).

102. Tellabs, Inc. v. Makor Issues & Rts., Ltd., 551 U.S. 308, 319 n.3 (2007):

> We have previously reserved the question whether reckless behavior is sufficient for civil liability under § 10(b) and Rule 10b-5. Every Court of Appeals that has considered the issue has held that a plaintiff may meet the scienter requirement by showing that the defendant acted intentionally or recklessly, though the Circuits differ on the degree of recklessness required.

(citation omitted); Aaron v. SEC, 446 U.S. 680, 701–02 (1980) ("[W]e hold that the Commission is required to establish scienter as an element of a civil enforcement action to enjoin violations of § 17(a)(1) of the 1933 Act, § 10(b) of the 1934 Act, and Rule 10b-5 promulgated under that section of the 1934 Act.").

103. *See, e.g.*, Drexel Burnham Lambert, Inc. v. CFTC, 850 F.2d 742, 748 (D.C. Cir. 1988) (quoting First Commodity Corp. v. CFTC, 676 F.2d 1, 7 (1st Cir. 1982)); City of Dearborn Heights Act 345 Police & Fire Ret. Sys. v. Waters Corp., 632 F.3d 751, 757 (1st Cir. 2011) (quoting the definition of recklessness from Sundstrand Corp v. Sun Chem. Corp., 553 F.2d 1033, 1045 (7th Cir. 1977)); Gebhart v. SEC, 595 F.3d 1034, 1041–43 (9th Cir. 2010) (holding that reckless conduct that constitutes scienter is an extreme departure from the standard of ordinary care, and it presents a danger of misleading buyers or sellers that the defendant knew or must have known about); S. Cherry St., LLC v. Hennessee Grp. LLC, 573 F.3d 98, 109 (2d Cir. 2009) (same); Flaherty & Crumrine Preferred Income Fund, Inc. v. TXU Corp., 565 F.3d 200, 207 (5th Cir. 2009) (same); Institutional Invs. Grp. v. Avaya, Inc., 564 F.3d 242, 267 n.42 (3d Cir. 2009) (same).

104. *Drexel Burnham Lambert, Inc.*, 850 F.2d at 748 (alteration in original) (quoting *First Commodity Corp.*, 676 F.2d at 7). *See also supra* note 103 and accompanying text.

105. Sharette v. Credit Suisse Int'l, 127 F. Supp. 3d. 60, 79 (S.D.N.Y. 2015).

106. *Compare* Commodity Exchange Act § 6(c)(1), 7 U.S.C. § 9(1), *and* 17 C.F.R. § 180.1 (2020), *with* Securities Exchange Act § 10(b), 15 U.S.C. § 78j, *and* 17 C.F.R. § 240.10b-5 (2019) (17 C.F.R. § 180.1 augments 7 U.S.C. § 9(1) and clearly imitates 17 C.F.R. § 240.10b-5). *See also* Prohibition on the Employment, or Attempted Employment, of Manipulative and Deceptive Devices and Prohibition on Price Manipulation, 76 Fed. Reg. at 41,405 (explaining that the rule's enforcement

10b-5 and 180.1 is lower than that of price manipulation, recklessness is not an easy standard to meet.[107] With algorithmic trading, outside of clear cases in which a programmer deliberately or carelessly programs the algorithm to manipulate, it may be difficult to decipher from the algorithm's code whether the programmer had manipulative intent (scienter) when she coded the algorithm. Thus, even with a lower scienter requirement, Rules 10b-5 and 180.1 may still pose challenges for regulators in proscribing some forms of algorithmic manipulation.

3. Open-Market Manipulation

Rules 10b-5 and 180.1 are also utilized in sanctioning open-market manipulation. Open-market manipulation refers to manipulation accomplished through facially legitimate transactions.[108] Given that there is no per se fraud or misconduct in this form of market manipulation, courts have historically looked to the intent of the trader to determine whether the underlying conduct ought to be deemed manipulative. For example, short selling or heavy trading at the end of the trading day (marking the close) can be used to improperly distort prices but may also constitute a legitimate investment strategy depending on the goals of the investor. For most courts, liability for open-market manipulation turns on proof of the defendant's intent to manipulate the markets even with legitimate transactions.[109]

Part of the difficulty with open-market manipulation is that although liability arises from a violation of Rule 10b-5, courts have traditionally required proof that the defendant acted intentionally to manipulate the markets; recklessness is insufficient in these cases.[110]

---

would "be guided, but not controlled by, judicial precedent interpreting and applying scienter under Exchange Act section 10(b) and SEC Rule 10b–5").

107. *See* Gregory Scopino, *Do Automated Trading Systems Dream of Manipulating the Price of Futures Contracts? Policing Markets for Improper Trading Practices by Algorithmic Robots*, 67 FLA. L. REV. 221, 252 (2015) ("[T]he mental state requirements of many causes of actions could pose an insurmountable obstacle for plaintiffs in private lawsuits and the CFTC in civil enforcement actions.").

108. Fletcher, *supra* note 8, at 484.

109. *See, e.g.*, Koch v. SEC, 793 F.3d 147, 155 (D.C. Cir. 2015) (citing Santa Fe Indus., Inc. v. Green, 430 U.S. 462, 476 (1977)) (finding that there is no requirement for "the SEC to prove actual market impact, as opposed to intent to affect the market, before finding liability for manipulative trading practices").

110. *See, e.g.*, Sullivan & Long, Inc. v. Scattered Corp., 47 F.3d 857, 865 (7th Cir. 1995) (stating that liability for open-market manipulation required a showing of specific intent); *see also* David Yeres, Robert Houck & Brendan Stuart, *A Bridge Too Far*, LAW360 (Jan. 4, 2019, 5:20 PM), https://www.law360.com/articles/1113505/a-bridge-too-far-cftc-s-reckless-manipulation-theory [https://perma.cc/72WH-WESK] (analyzing cases applying Rule 10b-5 to open-market manipulation to argue that more than recklessness is needed to hold a defendant liable). But it should be noted that in adopting Rule 180.1, the CFTC asserted that intentional or reckless conduct is sufficient to create liability for open-market manipulation. Response and Incorporated

This raises the evidentiary burden for the Commissions and private plaintiffs who must demonstrate that the defendant had manipulative intent when she engaged in her facially legitimate trades. For example, to be liable for open-market manipulation in the United States Court of Appeals for the Second Circuit, the plaintiff must prove that the intent to manipulate was the *sole intent* underlying the transactions.[111] Indeed, according to the court in *SEC v. Masri*, if the defendant had both legitimate and manipulative motives for her trades, she would not be liable for open-market manipulation if her trades were facially legitimate.[112]

The high evidentiary requirement of open-market manipulation limits the availability of this theory of manipulation as a basis of liability for algorithmic manipulation in all but the most obvious cases. To the extent algorithms employ facially legitimate transactions that distort the markets, holding someone accountable in these instances may prove difficult. This is particularly true in light of the difficulty the Commissions have had in holding human traders liable for open-market manipulation in the past.[113]

4. Spoofing

The most recent addition to the anti-manipulation framework is the CFTC's anti-spoofing authority. The Dodd-Frank Act amended the CEA to prohibit "any trading, practice, or conduct . . . [that] is, is of the character of, or is commonly known to the trade as, spoofing[,]" which it defines as "bidding or offering with the *intent* to cancel the bid or offer before execution."[114] To aid the markets in understanding how the newly enacted spoofing provision would apply, the CFTC issued interpretative guidance to delineate the scope of the prohibition.[115] In the guidance, the CFTC identified four nonexhaustive examples of behavior that it would classify as spoofing: (1) submitting or cancelling orders to overload the quotation system, (2) submitting or cancelling bids to impede another's execution of trades, (3) submitting or

Memorandum of Law in Opposition to Defendants' Motion to Dismiss at 18–22, CFTC v. Kraft Foods Grp., Inc., No. 1:15-cv-02881 (N.D. Ill. Mar. 5, 2020), ECF No. 64; *see also* Prohibition on the Employment, or Attempted Employment, of Manipulative and Deceptive Devices and Prohibition on Price Manipulation, 76 Fed. Reg. at 41,399 (stating that Rule 180.1 can be violated by a showing of reckless or intentional conduct).

111. SEC v. Masri, 523 F. Supp. 2d 361, 370–75 (S.D.N.Y. 2007).

112. *Id.* at 372.

113. *See* CFTC v. Wilson, 27 F. Supp. 3d 517 (S.D.N.Y. 2014); Markowski v. SEC, 274 F.3d 525 (D.C. Cir. 2001).

114. Commodity Exchange Act § 4c(a)(5), 7 U.S.C. § 6c(a)(5), *amended by* Dodd-Frank Act, Pub. L. No. 111-203, § 747, 124 Stat. 1376, 1739 (2010) (emphasis added).

115. Antidisruptive Practices Authority, 78 Fed. Reg. 31,890 (May 28, 2013).

cancelling orders to create a false appearance of market depth, and (4) submitting or cancelling bids with the intent to create an artificial price.[116]

Liability for spoofing attaches if the trader acted intentionally to cancel the bid or offer—that is, the actor must have been more than reckless for her actions to constitute spoofing.[117] Notably, by tying liability to the intent of the trader, the anti-spoofing prohibition adheres to the intent-focused model of prior anti-manipulation provisions, despite being directed towards a modern, algorithm-dominated marketplace. In remaining tethered to an intent-centric framework, the newly enacted spoofing laws may also be less effective at deterring the very conduct they are aimed at proscribing.

* * *

As the above discussion demonstrates, the existing anti-manipulation framework's liability provisions are centered firmly around the intent of the actor. In human-dominated markets, this focus on intent was understandable. Modern financial markets, however, are not human-centric. Computers and algorithms dominate the markets, thereby challenging the efficacy of an intent-focused liability regime in deterring manipulation in the modern marketplace. The following Section discusses the involvement of algorithms in modern-day trading and its impact on how the market functions.

B. Modern Trading

Algorithmic trading dominates the securities and commodities markets, accounting for nearly sixty percent of all transactions in each market.[118] The development of technology has impacted the financial markets significantly, allowing for faster transaction execution, lowered costs, and greater efficiency in the markets overall. In analyzing the consequences and implications of technology in the markets, legal scholars have focused on algorithmic trading and high-

116. *Id.* at 31,896.

117. *Id.*

118. Chris Isidore, *Machines Are Driving Wall Street's Wild Ride, Not Humans*, CNN: BUS. (Feb. 6, 2018, 4:02 PM ET), https://money.cnn.com/2018/02/06/investing/wall-street-computers-program-trading/index.html [https://perma.cc/ZQP3-BCK6] ("On a typical trading day, computers account for 50% to 60% of market trades."); Gregory Meyer, Nicole Bullock & Joe Rennison, *How High Frequency Trading Hit a Speed Bump*, FIN. TIMES (Jan. 1, 2018), https://www.ft.com/content/d81f96ea-d43c-11e7-a303-9060cb1e5f44 [https://perma.cc/XUE3-6DPE] (graph depicting high frequency trading constituting between approximately thirty and fifty-five percent of U.S. equities volume from 2007 to 2017, respectively).

frequency trading ("HF trading"). Although these are important developments in the market, the next frontier in technology lies in the integration of AI and machine learning in trading algorithms. This Section examines early iterations of algorithmic trading, including HF trading, and then assesses how AI and machine learning continue to revolutionize trading.

1. Algorithmic Trading and HF Trading

Algorithmic trading refers to the use of preprogrammed electronic instructions in trading securities or commodities.[119] Trading algorithms are programmed to execute specific trading strategies based on preset rules that inform the algorithm when and how to act. For example, a simple trading algorithm could be programmed to buy five thousand shares of Widget, Inc. if and when the shares are $150 per share. Once the shares reach the desired price, the algorithm initiates a purchase order for Widget shares, sending its order to an exchange or electronic communication network for the desired purchase volume. Yet, trading algorithms can also be much more complex—disseminating upper and lower limits for transactions or changing trading strategies based on newly released information.[120]

Notwithstanding this complexity, programmers are still required to code these investment decisions into rules-based instructions that the algorithm can follow as it trades in the markets.[121] Programmers code trading algorithms to evaluate collected data, attach value to the data, and decide how to trade to accomplish the overarching trading strategy.[122] Within the scope of their rules-based set of instructions, algorithmic trading programs make decisions, such as when to initiate buy and sell orders, the volume of the transaction, and

---

119. Johannes Prix, Otto Loistl & Michael Huetl, *Algorithmic Trading Patterns in Xetra Orders*, 13 EUR. J. FIN. 717, 717 (2007).

120. TECH. COMM. OF THE INT'L ORG. OF SEC. COMM'NS, REGULATORY ISSUES RAISED BY THE IMPACT OF TECHNOLOGICAL CHANGES ON MARKET INTEGRITY AND EFFICIENCY 10 (July 2011), https://www.iosco.org/library/pubdocs/pdf/IOSCOPD361.pdf [https://perma.cc/758K-2YG3]:

> In its simplest guise, algorithmic trading may just involve the use of a basic algorithm . . . to feed portions of an order into the market at pre-set intervals to minimise market impact cost. At its most complex, it may entail many algorithms that are able to assimilate information from multiple markets . . . in fractions of a second.

121. RISHI K. NARANG, INSIDE THE BLACK BOX: A SIMPLE GUIDE TO QUANTITATIVE AND HIGH-FREQUENCY TRADING 8–9, 24–62 (2d ed. 2013).

122. Yesha Yadav, *The Failure of Liability in Modern Markets*, 102 VA. L. REV. 1031, 1064 (2016) (showing that programmers institute trading strategies in particularized ways by: "(1) collecting data for trading; (2) submitting orders/canceling orders; (3) establishing the price, amount, and type of trades to make; (4) anticipating the impact of trading on future price changes; (5) responding to unplanned events; and (6) determining when to stop trading").

the transaction's timing. Further, these programs do so in response to their analysis of the markets and expectations of market movements.[123] Algorithms can internalize, assess, and respond to large quantities of data faster than any human can, quickening the pace at which transactions occur in the markets, but with little to no human intervention *after* the algorithm has been deployed in the markets.

The speed at which algorithms execute transactions is a hallmark feature of a subset of algorithmic trading programs, known as HF trading. HF trading broadly refers to the rapid, high-volume placement and cancellation of bids and offers to realize short-term arbitrage profits.[124] While there is no agreed-upon definition, common features of HF trading include heavy reliance on algorithms and a focus on speed.[125] HF traders leverage technology, algorithms, and speed to gain an advantage over other traders in the market. Indeed, the success and profitability of HF traders is directly influenced by speed, that is, the ability to execute transactions faster than others in the market.[126] The importance of speed to HF trading means that traders expend considerable capital and expertise to reduce the time it takes to trade and maximize available information for profitability.[127]

---

123. Alain Chaboud, Benjamin Chiquoine, Erik Hjalmarsson & Clara Vega, *Rise of the Machines: Algorithmic Trading in the Foreign Exchange Market* 1 (Bd. of Governors for the Fed. Rsrv. Sys., Int'l Fin. Discussion Paper No. 980, Oct. 2009), http://www.federalreserve.gov/pubs/ifdp/2009/980/ifdp980.pdf [https://perma.cc/F69R-Z3XS] ("In algorithmic trading (AT), [traders'] computers directly interface with trading platforms, placing orders without immediate human intervention. The computers observe market data and possibly other information at very high frequency, and, based on a built-in algorithm, send back trading instructions, often within milliseconds.").

124. There is no agreed-upon definition of HF trading. In a 2010 concept release, the SEC identified five general characteristics that can be used to identify HF trading:

> (1) The use of extraordinarily high-speed and sophisticated computer programs for generating, routing, and executing orders; (2) use of co-location services and individual data feeds offered by exchanges and others to minimize network and other types of latencies; (3) very short time-frames for establishing and liquidating positions; (4) the submission of numerous orders that are cancelled shortly after submission; and (5) ending the trading day in as close to a flat position as possible (that is, not carrying significant, unhedged positions overnight).

Concept Release on Equity Market Structure, 75 Fed. Reg. 3594, 3606 (2010).

125. McGowan, *supra* note 2, ¶¶ 2–3 (finding that, at its core, HF trading uses an "algorithm [to] make[ ] important decisions such as timing, price, or in many cases, executing the entire order without human interaction" while "being smarter and faster than everyone else").

126. *Id.* ¶ 16 ("The speed factor in trading is known as 'latency', and is an important component of all high-frequency trading strategies.").

127. *See id.*:

> In order to turn a profit, HF traders have to flow information into their algorithms microseconds faster than their competitors. Therefore, to remain competitive, HF traders must constantly upgrade their computer systems to stay ahead of the pack. . . . In the HF trading world, speed and the most innovative technology separate the winners from the losers. The current trend in employee recruiting is to hire traders with

HF trading strategies rely on algorithms to submit and route trades to find and exploit arbitrage opportunities in the markets.[128] The predefined rules that govern an HF trading algorithm allow traders to execute complex trades in response to newly disclosed information ahead of slower traders in the market.[129] HF trading relies on algorithms to "analyze market data, organize trades based on pre-programmed instructions, access . . . trading center servers, and trade execution benefits."[130] HF algorithm programming, therefore, must be precise and detailed to effectively accomplish its trading goals. Once deployed in the market, the profitability of HF trading algorithms depends on being able to operate and make decisions in furtherance of the underlying goal without human intervention. Thus, the rules on which an HF trading algorithm is based at the outset are of paramount importance, and deciphering the underlying motivations of the programmer from these rules is essential to any liability for market manipulation.

2. Artificial Intelligence & Machine Learning

Although HF trading algorithms currently dominate the discourse on computerized trading, the very near future of algorithmic trading lies with AI and machine-learning algorithms.[131] The development of sophisticated learning algorithms is occurring at an accelerated speed throughout society. From speech recognition, to self-driving cars, to smart home speakers like Alexa, artificially intelligent, machine-learning algorithms are becoming more prevalent in everyday life.[132] And the financial markets are no different.

Algorithmic trading is evolving to incorporate sophisticated AI and machine-learning tools and techniques that allow algorithms to

---

degrees in math and computer science from the top schools, many traders even with PhD's, in order to stay competitive.

128. *Id.* ¶ 3.

129. *Id.* ¶ 16.

130. Kristin N. Johnson, *Regulating Innovations: High Frequency Trading in Dark Pools*, 42 J. CORP. L. 833, 857 (2017).

131. GOV'T OFF. FOR SCI., THE FUTURE OF COMPUTER TRADING IN FINANCIAL MARKETS: AN INTERNATIONAL PERSPECTIVE 36 (2012), http://www.bis.gov.uk/foresight [https://perma.cc/5UND-R894] (scroll down to and click on "Future of computer trading in financial markets: an international perspective") ("Since the late 1990s, researchers have also studied the use of automated optimisation methods to design and improve [autonomous] adaptive trading algorithms. . . . The use of these techniques in the finance industry looks likely to grow over the next decade.").

132. Bill Kleyman, *Smart Things Everywhere: The Connected Future of 2025*, DATA CTR. FRONTIER (Aug. 21, 2018), https://datacenterfrontier.com/smart-things-everywhere-the-connected-future-of-2025 [https://perma.cc/RU93-GAQN]:

dynamically learn from data, assess inputs, and incorporate new information into their decisionmaking. As discussed above, traditional trading algorithms, whether HF or not, are preprogrammed to operate within set parameters to fulfill a predetermined trading trajectory or strategy. Unlike traditional algorithmic trading programs, AI machine-learning algorithms have the capacity to learn from data and prior decisions, truly minimizing human involvement in trading.[133]

With AI machine-learning algorithms, coders specify a goal or a set of goals for the algorithm to achieve when solving a problem.[134] The algorithm is not given any rules for how to solve the problem at hand. Rather, it may be given rules on how to learn or it may be left to figure out how to solve the problem on its own through trial and error of similar problems. In learning from the available data, AI machine-learning algorithms are able to fine-tune their own decisionmaking through repeated practice on the provided data.[135] Thus, these algorithms are not merely executing preprogrammed instructions but, instead, are dynamically learning and solving problems based on the data available, eliminating the need for human involvement in their processes.

Importantly, the solutions that AI machine-learning algorithms provide may be beyond any results the coder considered or expected when she programmed the algorithm. Because the algorithm learns by making inferences, connections, and classifications from the data, the output from the algorithm may not be evident even to the programmer because of *how* the AI machine-learning algorithm learns. One popular technique used in AI machine-learning algorithms is the implementation of a neural network. Neural networks, particularly deep learning models, utilize virtual neurons to identify patterns in the data or make logical inferences and connections between data points.[136]

> By 2025, "smart" will become the new normal. . . . [Much of our technological experience] will involve cognitive systems that interact with the data that we generate, creating new layers of data analysis across a range of industries, applications, and scenarios. [International Data Corporation] estimates that the volume of analyzed data that is "touched" by cognitive systems will grow by a factor of 100 to 1.4 zettabytes in 2025.

133. Sonia K. Katyal, *Private Accountability in the Age of Artificial Intelligence*, 66 UCLA L. REV. 54, 68–69 (2019):

> [T]oday, machine learning algorithms are trained on a body of data that is selected by designers or by past human practices. This process is the "learning" element in machine learning; the algorithm learns, for example, how to pair queries and results based on a body of data that produced satisfactory pairs in the past.

134. *Id.* at 62–63.

135. *Id.* at 68–69.

136. For an overview of neural networks, see Victor Zhou, *Machine Learning for Beginners: An Introduction to Neural Networks*, TOWARDS DATA SCI. (Mar. 5, 2019),

Deep networks of neurons work together to arrive at a solution or decision based on an algorithm's analysis and internalization of the data. Oftentimes, it is not easy to discern why a deep neural network produced a given output or solution because the algorithm's decisionmaking process is "intuitive."[137] To illustrate, the outputs of preset algorithms can be retraced by walking backwards through the preprogrammed rules. But neural networks significantly complicate this retracing process as there are no clear steps or discernible reasons for each decision in its "thinking."[138]

The complexity underlying the operation of these AI machine-learning algorithms creates a "black box" problem, that is, "an inability to fully understand an AI's decision-making process and the inability to predict the AI's decisions or outputs."[139] Being unable to explain the outputs of the algorithm ex post limits the ability of humans to understand how they operate or supervise their use. Further, with a "strong black box," ex post analysis and reverse engineering to understand how and why the AI machine-learning algorithm came to its decision is not possible.[140] This renders the AI machine-learning algorithm's functioning opaque to human oversight and supervision. As AI machine-learning algorithms are introduced into the financial markets, questions arise as to the capacity of the regulatory framework to prevent and deter market manipulation. Unlike the rules-based criteria of HF algorithms, AI machine-learning algorithms learn and make dynamic, intuitive decisions that challenge the scienter-focused anti-manipulation regime.

C. Algorithmic Manipulation: Assessing the Possibilities

With the dominance of algorithmic trading, the concerns with respect to manipulation have moved away from focusing on the misconduct of human traders and instead towards detecting and deterring algorithmic manipulation. As one academic has stated, algorithmic manipulation schemes "can be undertaken much more effectively with the aid of algorithmic precision" than traditional

---

https://towardsdatascience.com/machine-learning-for-beginners-an-introduction-to-neural-networks-d49f22d238f9 [https://perma.cc/H5RT-D99H].

137. Yavar Bathaee, *The Artificial Intelligence Black Box and the Failure of Intent and Causation*, 31 HARV. J.L. & TECH. 889, 902 (2018) ("Because a neural network is learning from experience, its decision-making process is likewise intuitive.").

138. *Id.* at 902–03 ("No single neuron in these networks encodes a distinct part of the decision-making process. The thousands or hundreds of thousands of neurons work together to arrive at a decision . . . [and] often what is encoded will not be intelligible to human beings.").

139. *Id.* at 905.

140. *Id.* at 906.

market manipulation schemes.[141] This precision, coupled with the automated and increasingly AI-nature of algorithmic trading, makes algorithmic manipulation a particularly pernicious problem, both in the market and for regulators. This Section analyzes potential examples of how algorithmic manipulation may manifest in the markets.

1. The Easy Case: Deliberate Misuse of Algorithms

Programmers can code algorithms to deliberately distort and disrupt the markets. For example, a trader can deliberately program an algorithm to "spoof" the market. Spoofing captured the attention of regulators and the public because of its role in the Flash Crash—the almost one-thousand point fall and rebound of the Dow Jones Index that destabilized the U.S. securities markets in May 2010.[142] Since then, regulators have brought numerous enforcement actions against traders for spoofing in equities, precious metals, and other commodities.[143]

Statutorily, spoofing is defined as placing an order with the intent to cancel prior to execution.[144] Practically, spoofing is a distortive trading strategy with a few steps. First, a trader places a large, non-bona fide order on one side of the market causing the market to move in response to the trade. Second, after the market has moved, the trader places a small bona fide order on the other side of the market. The smaller bona fide order is filled at the artificial price, earning the trader a profit. Third, the trader cancels the large order, ending the scheme.[145] To use a concrete example: Shares of Widget Co. are trading at $5.25/share. Sarah Spoofer enters a buy order for one thousand shares of Widget Co. at $5.45/share. In response to the large buy order, the price of Widget Co. increases to $5.40/share, at which point Sarah

141. Yadav, *supra* note 122, at 1069.

142. Owen Davis, *Navinder Singh Sarao and the Flash Crash*, INT'L BUS. TIMES (Apr. 28, 2015, 12:39 PM), https://www.ibtimes.com/navinder-singh-sarao-flash-crash-why-financial-market-spoofing-so-hard-catch-even-1898716 [https://perma.cc/QPR3-267G] ("On the day of the crash—May 6, 2010—Sarao allegedly entered more than 32,000 orders to sell futures contracts, then canceled the vast majority of them. The technique, known as spoofing, allegedly allowed Sarao to profit from artificial price movements."); *see also* Treanor, *supra* note 5 ("[D]espite the turbulent start to the trading day, no one had expected the near 1,000-point dive in share prices.").

143. *See, e.g.*, CFTC v. Oystacher, 203 F. Supp. 3d 934, 938 (N.D. Ill. 2016) (the CFTC alleged that defendants were engaged in spoofing by placing large orders in the future contracts market, with the intent to cancel before execution); CFTC v. Khara, No. 15 CV 03497, 2015 WL 2066257 (S.D.N.Y. May 5, 2015) (the CFTC alleged that defendants engaged in unlawful conduct in the gold and silver futures markets by "bidding or offering with the intent to cancel the bid or offer before execution").

144. Commodity Exchange Act, 7 U.S.C. § 6c(a)(5)(C).

145. *See* Lin, *supra* note 24, at 1289 ("Spoofing allows the initiating party to distort the ordinary price discovery in the marketplace by placing orders with no intention of ever executing them and merely for the purpose of manipulating honest participants in the marketplace.").

enters a second order to sell one hundred shares of Widget at $5.40/share, earning her a profit of $0.15/share.

The above-described scheme nets Sarah $15 if done manually, slowly, and only once. But if Sarah deploys HF trading algorithms to execute the same scheme—repeatedly, at a high volume, and across numerous asset classes—she increases the profitability of the trading strategy exponentially.[146] HF trading algorithms can be coded to place, then cancel, large market-moving orders on one side of the market and also submit orders on the other side of the market to benefit from the subsequent price movement. In 2013, the CFTC and the DOJ brought their first criminal spoofing case against Michael Coscia and his firm Panther Energy Trading LLC (collectively, "Coscia").[147] Coscia deployed two algorithmic trading programs across approximately twelve different commodities markets to create an illusion of demand, thereby enabling him to earn profits on smaller trades on the opposite side of the market.[148] According to prosecutors, with the aid of algorithmic trading programs, Coscia netted $1.4 million in illegal profits in less than three months.[149]

Similarly, but with more devastating consequences, Navinder Sarao used algorithmic trading programs to flood the Chicago Mercantile Exchange with orders to sell millions of dollars' worth of securities as part of his spoofing strategy.[150] Sarao's algorithms, however, did more than just earn him illicit profits through depressing the price of the security: the algorithm's large sell order sent the markets into a twenty-minute state of extreme volatility.[151] In that brief

---

146. *Id.* at 1289.

147. Press Release, Commodity Futures Trading Comm'n, CFTC Orders Panther Energy Trading LLC and Its Principal Michael J. Coscia to Pay $2.8 Million and Bans Them from Trading for One Year, for Spoofing in Numerous Commodity Futures Contracts (July 22, 2013), https://www.cftc.gov/PressRoom/PressReleases/6649-13 [https://perma.cc/6MPS-A8S7] [hereinafter CFTC Press Release on Coscia]; Michael M. Philipp & Dina R. Kaufman, *Prosecutors Record First-Ever Conviction for 'Spoofing': A New Era of Trading Enforcement*, MORGAN LEWIS: LAWFLASH (Nov. 9, 2015), https://www.morganlewis.com/pubs/2015/11/prosecutors-record-first-ever-conviction-for-spoofing [https://perma.cc/9GWM-E48H].

148. Philipp & Kaufman, *supra* note 147 (detailing Coscia's spoofing method).

149. *Id.* ("The CFTC Order requires Panther and Coscia to . . . disgorge $1.4 million in trading profits . . . .").

150. *See* Davis, *supra* note 142 ("The technique, known as spoofing, allegedly allowed Sarao to profit from artificial price movements.").

151. *Id.* ("The criminal complaint says that Sarao's offers to sell Standard & Poor's 500 E-Minis, a commonly traded stock index future, eventually totaled 29 percent of the market."); COMMODITY FUTURES TRADING COMM'N & SEC. & EXCH. COMM'N, FINDINGS REGARDING THE MARKET EVENTS OF MAY 6, 2010, at 2, 5 (2010), http://www.sec.gov/news/studies/2010/marketevents-report.pdf [https://perma.cc/WEV5-3F68]:

> However, on May 6, when markets were already under stress, the Sell Algorithm chosen by the large trader to only target trading volume, and neither price nor time, executed the sell program extremely rapidly in just 20 minutes. . . . Between 2:40 p.m. and 3:00

window of time, prices of various financial products plummeted to pennies, while other prices increased to incredulous highs.[152] Owing to the volatility, traders exited the market, thereby reducing liquidity and exacerbating the crisis.[153] When the dust settled, the market had suffered approximately one trillion dollars in losses.[154]

In both examples, the traders programmed their trading algorithms to deliberately distort the markets. The trading algorithms were instructed to flood the markets, which created artificial prices and allowed each defendant to profit.[155] Although it took authorities months to piece together what occurred in the market each time, the trading algorithms left a paper trail that allowed regulators to decipher what happened and how.[156] The design of these rules-based algorithms also demonstrated the true, underlying intent of the traders. Notably, both Coscia and Sarao defended their actions by claiming that the algorithms' actions did not reflect their intentions as the programmer. Once regulators gained access to the trading algorithms, however, the traders' manipulative intent was evident from the programming language.[157] In similarly "easy" cases involving the deliberate misuse of algorithms for manipulation, regulators should be able to meet the

---

> p.m., approximately 2 billion shares traded with a total volume exceeding $56 billion. Over 98% of all shares were executed at prices within 10% of their 2:40 p.m. value. However, as liquidity completely evaporated in a number of individual securities and ETFs, participants instructed to sell (or buy) at the market found no immediately available buy interest (or sell interest) resulting in trades being executed at irrational prices as low as one penny . . . .

152. Johnson, *supra* note 130, at 835 (explaining the Flash Crash in 2010 and detailing some of the price fluctuations that occurred during the crash).

153. COMMODITY FUTURES TRADING COMM'N & SEC. & EXCH. COMM'N, *supra* note 151, at 1, 35–37 (discussing the exodus of traders due to volatility and ensuing reduction in liquidity); *see also* Matt Phillips, *Nasdaq: Here's Our Timeline of the Flash Crash*, WALL ST. J. (May 11, 2010, 12:34 PM ET), https://blogs.wsj.com/marketbeat/2010/05/11/nasdaq-heres-our-timeline-of-the-flash-crash [https://perma.cc/52YA-XGCG] (reporting on and analyzing the statements of executives from NASDAQ and NYSE outlining the timeline of the flash crashes during a related congressional hearing).

154. COMMODITY FUTURES TRADING COMM'N & SEC. & EXCH. COMM'N, *supra* note 151; Phillips, *supra* note 153; *see also* Edgar Ortega Barrales, *Lessons from the Flash Crash for the Regulation of High-Frequency Traders*, 17 FORDHAM J. CORP. & FIN. L. 1195, 1196 (2012) ("In twenty minutes on May 6, 2010, stock market investors lost about $862 billion.").

155. CFTC Press Release on Coscia, *supra* note 147; Davis, *supra* note 142.

156. COMMODITY FUTURES TRADING COMM'N & SEC. & EXCH. COMM'N, *supra* note 151; Davis, *supra* note 142.

157. *See* Press Release, Dep't of Just., Futures Trader Charged with Illegally Manipulating Stock Market, Contributing to the May 2010 Market 'Flash Crash' (Apr. 21, 2015), https://www.justice.gov/opa/pr/futures-trader-charged-illegally-manipulating-stock-market-contributing-may-2010-market-flash [https://perma.cc/PU4B-L8T2] (explaining that Sarao's algorithm used a " 'dynamic layering' scheme . . . [to] create[ ] the appearance of substantial supply in the market"); CFTC Press Release on Coscia, *supra* note 147 ("While forms of algorithmic trading are of course lawful, using a computer program that is written to spoof the market is illegal and will not be tolerated.").

evidentiary burden of scienter through the paper trail left in the rules of the algorithm's source code. To the extent there are obvious or plausible signs of manipulative intent, it ought to be straightforward enough to hold defendants liable for violating Rule 10b-5, Rule 180.1, or the spoofing provision.

Yet, Coscia and Sarao's claims that the algorithms' actions did not reflect their intentions as the programmer are noteworthy. Their claims demonstrate that perpetrators of algorithmic manipulation are likely to point to the innate layer of abstraction between themselves and the algorithm as a defense. Simply put, traders accused of algorithmic manipulation will likely raise as a defense differences between what they *intended* the algorithm to do and what the algorithm *actually* did. Such defenses are not likely to hold in deliberate manipulation cases, especially those involving rules-based algorithms that can be reverse engineered. With access to a trading program's design and rules, regulators should be able to ferret out the true intent of traders. It remains to be seen, however, whether regulators have the time and resources to effectively assign liability for such manipulative conduct.

2. The Medium Case: Open-Market Manipulation & Unintended but Harmful Distortion

A stronger challenge to the anti-manipulation framework arises when the intent of the programmer may not be evident from the programming code. While this may be possible in numerous instances, two are highlighted here.

First, the manipulative intent of the programmer may not be evident if the algorithm is designed to use facially legitimate transactions to distort the markets (that is, to engage in open-market manipulation).[158] A trader could program her trading algorithm to short sell stocks aggressively or to engage in heavy trading at the end of the day, a strategy known as marking the close.[159] Either strategy can cause a significant impact on the price of the stock because of the timing and volume of the transactions. Neither practice, however, is per se illegal. As previously discussed, to determine whether such practices are manipulative, courts have traditionally looked to the intent of the

158. Fletcher, *supra* note 8 (defining open-market manipulation).

159. *See id.* at 506–07 (identifying the practice of short selling as a common manipulative trading strategy, especially when it is "aggressive," and the practice of marking the close); *In re* Kocherhans, Exchange Act Release No. 36556, 60 SEC Docket 2210, 2212 (Dec. 6, 1995) (defining "marking the close" as a manipulative practice that is employed in an attempt to "influence the closing price of a stock by executing purchase or sale orders at or near the close of the market").

trader.[160] But with trading algorithms, even those that operate on preprogrammed instructions, making such determinations regarding manipulative intent can be quite difficult. In this instance, despite the paper trail the algorithm leaves behind, it may not be enough to decipher a clear intent to manipulate to meet the scienter requirement for open-market manipulation.

Second, the algorithm may operate in a way that is unexpected and truly does not reflect the intent of the programmer. Here, the algorithm's unexpected behavior does not arise from the algorithm's "intuitive" neural response to data. Rather, the unexpected distortion is the result of a failure to properly design and test the algorithm before installation, a failure to properly monitor and respond to warning signs of potential, or a mistake in the algorithm's code. If one defines manipulation based on the intent of the actor, as many scholars and jurists do,[161] such conduct may not rise to the level of illegal manipulation. Instead, this conduct may be classified as negligent or reckless. Even if one does not deem the unintended consequences to be illegal manipulation, such algorithms can nonetheless wreak havoc and have dire consequences for the market. Under the current anti-manipulation framework, it is highly doubtful that liability would attach for such unintended distortion, unless the Commissions are able to prove that the defendant's conduct rose to the level of recklessness necessary to violate Rule 10b-5 or Rule 180.1.[162]

3. The Hard Case: Rational Distortion & Independent Misconduct

The most significant challenge to the anti-manipulation framework stems from AI machine-learning algorithms that may distort the markets as part of their dynamic learning and

160. *See supra* notes 95–98 and accompanying text.

161. Manipulative purpose is a required element to prove manipulative practice under section 9(a)(2) of the Exchange Act. 15 U.S.C. § 78i(a)(2). Courts and scholars repeatedly analyze manipulative purpose by utilizing circumstantial evidence to extrapolate intent. *See, e.g.*, United States v. Dardi, 330 F.2d 316, 331–32 (2d Cir. 1964) (describing the criteria that should inform analysis of circumstantial evidence to discern intent); *In re* The Federal Corp., Exchange Act Release No. 3909, 25 S.E.C. 227, 230 (Jan. 19, 1947) ("Since it is impossible to probe into the depths of [an actor]'s mind [to prove manipulative purpose], it is [usually] necessary . . . that the finding of manipulative purpose be based on inferences drawn from circumstantial evidence."); Fischel & Ross, *supra* note 23, at 510 ("The only definition [of manipulation] that makes any sense is subjective—it focuses entirely on the intent of the [actor]."); *see also supra* Section II.A (discussing the scienter element of the Acts).

162. This analysis is limited to liability under the anti-manipulation framework specifically and does not address potential liability under FINRA or NFA rules or other Commission regulations that may capture this form of misconduct. *See, e.g.*, Yadav, *supra* note 122, at 1039, 1057–58 (discussing how the negligence standard and the market access rule addressed similar unintended distortions in the securities markets).

decisionmaking process. To the extent algorithmic trading programs are capable of learning and making independent (that is, not merely rules-based) decisions to meet set goals, then there is possibility that an algorithm may manipulate the market in unforeseen and even unforeseeable ways. Although there is a wealth of potential hypothetical scenarios in which trading algorithms could unexpectedly manipulate the markets, this Article explores the possibility of (1) "rational distortion" and (2) "independent misconduct," particularly by an AI-based trading algorithm.

First, an algorithm may be programmed to accomplish a legitimate goal but may engage in rationally disruptive or distortive conduct to achieve that goal. For example, the algorithm may place and cancel a large number of orders repeatedly to gain valuable information it then uses to accomplish its programmed goals.[163] The underlying conduct—placing and cancelling orders repeatedly—is not per se illegal and, without more, does not rise to the level of illegal manipulation. Yet, such conduct is disruptive to the markets—it can distort the asset's price, which now incorporates noise trading rather than reflecting the asset's inherent value,[164] and it can create a false appearance of liquidity in the market. Traditionally, liability for such conduct required a showing that the defendant acted with scienter, but, as discussed above, this may be difficult to prove, especially with AI machine-learning algorithms.

Further, if the algorithm has adopted AI machine-learning techniques, it could have rationally decided to engage in this conduct as the most efficient means to accomplish its trading goals. Importantly, the programmer may not have expected the algorithm to engage in rational distortion, and she may not be able to explain why the AI machine-learning algorithm decided that distortion was appropriate. To the extent the algorithm's distortion creates an artificial price, liability under the CEA would require evidence that the programmer had the specific intent to manipulate the commodity[165]—a difficult task even when there is no AI machine-learning trading algorithm involved. Holding the programmer liable under the lower scienter requirements

163. This example draws on the trading strategy known as "pinging" whereby algorithms place and cancel orders repeatedly to determine the lowest or highest price a trader is willing to pay for an asset. *See* FINRA Staff, *Getting Up to Speed on High-Frequency Trading*, FINRA (Nov. 25, 2015), https://www.finra.org/investors/insights/getting-speed-high-frequency-trading [https://perma.cc/4ERT-7R2F].

164. Yadav, *supra* note 122, at 1075 ("More problematically, the market suffers if prices reflect noise created by such evasions or a degree of discounting on the part of traders internalizing higher transaction costs.").

165. *See* Commodity Exchange Act § 6(c)(3), 7 U.S.C. § 9(1)–(3)*; see also supra* notes 97–98 and accompanying text.

of Rules 10b-5 and 180.1 may still prove difficult if the programmer and the regulators are unable to reverse engineer the algorithm's decisionmaking to see why it engaged in distortion.

Second, an AI machine-learning algorithmic program may "discover" the profitability of manipulative conduct and decide to engage in such conduct independent of its intended design. For example, an AI trading algorithm may independently "learn" that if it engages in certain types of trading strategies it can earn greater profits. The algorithm's programmers never intended for these trading strategies to be executed, and, to take it one step further, the programmer specifically instructed the AI algorithm to not engage in illegal manipulation. Yet, the AI algorithm may nonetheless discover strategies currently unknown to human traders that manipulate prices and increase the algorithm's profitability.

Alternately, suppose "two or more [AI algorithms] independently discover that they can profit from cooperating in a pattern of trading activity."[166] Additionally, the AI algorithms have learned how to better cloak their conduct from surveillance by working together, thereby strengthening their ability to manipulate the markets. Again, as with the previous hypothetical, this misconduct is independent of the intended goals of the algorithm.

Although at first blush this seems like a far-fetched hypothetical, it is not. In 2017, it was reported that AI algorithms on Facebook that were tasked with bartering created their own language for the bartering exercise.[167] In light of AI algorithms' ability to discover ways to cooperate and communicate, it is not unbelievable that they may discover ways to engage in manipulation. Because AI machine-learning decisions cannot be reverse engineered, regulators are in the dark as to whether the programmer intended the AI algorithm's manipulative behavior. And, even if the programmer did intend such behavior, she may be able to shield herself from liability through the complexity of the algorithm. The essentiality of scienter to assigning liability becomes more problematic when dealing with AI machine-learning algorithms, whose conduct remains a black box ex post. It is questionable, therefore, whether the scienter-focused anti-

166. Collin Starkweather & Izzy Nelken, *Artificial Intent: AI on the Trading Floor*, LAW360 (Jan. 23, 2019, 1:21 PM), https://www.law360.com/articles/1119871/artificial-intent-ai-on-the-trading-floor [https://perma.cc/SEW7-SCBK].

167. Andrew Griffin, *Facebook's Artificial Intelligence Robots Shut Down After They Start Talking to Each Other in Their Own Language*, INDEPENDENT (July 31, 2017, 5:10 PM), https://www.independent.co.uk/life-style/gadgets-and-tech/news/facebook-artificial-intelligence-ai-chatbot-new-language-research-openai-google-a7869706.html [https://perma.cc/PR3M-238A].

manipulation framework can credibly deter algorithm-related market manipulation.

III. THE FAILURE TO DETER ALGORITHMIC MANIPULATION

The rise of algorithmic trading strains one of the fundamental goals of the anti-manipulation framework—deterrence. To the extent the legal framework does not clearly identify what constitutes impermissible conduct and fails to effectively punish those who violate the law, it is ineffective in achieving deterrence. Liability for the most common market manipulation offenses requires a showing that, at a minimum, the defendant acted recklessly.[168] Historically, the legal regime has posed problems for regulators in punishing manipulation in human-dominated markets; these issues are further amplified with algorithmic trading. The scienter-focused liability framework creates a vague, overbroad standard with limited application to algorithms and algorithmic manipulation.[169] Further, with the involvement of algorithms, both preprogrammed and AI machine-learning types, identifying scienter to hold a human responsible for the manipulative conduct of an algorithm is a difficult feat. In sum, the outsized role of intent in the regulatory framework restricts the ability of regulators to hold traders liable for algorithmic manipulation. This renders punishment uncertain, even in the face of significant market harm, and weakens the deterrent effect of the anti-manipulation legal regime.

One important point to note here: algorithms qua algorithms cannot be deterred. Regardless of the capacity of algorithms to learn, assess, and adjust their decisions, algorithms cannot appreciate the legal liability for their decisions, and holding an algorithm liable for its misdeeds is futile.[170] Therefore, the focus of deterrence has to be on whether and to what extent we can deter humans from misusing algorithms to manipulate the markets or, alternately, how to incentivize programmers to take greater care in designing their algorithms.

At present, the legal regime does not credibly deter algorithm-related market manipulation because there is significant uncertainty of punishment. Part II analyzed the gaps created by the scienter-focused legal regime, which directly diminish deterrence of algorithm-based

168. *See supra* notes 99–102 and accompanying text.

169. *See* Scopino, *supra* note 107, at 252 (explaining the gap between crimes requiring scienter and AI).

170. At a minimum, it seems futile at this juncture. Future developments in AI may result in conscious robots and algorithms that can appreciate the consequences of their actions, but it is safe to say that we are not there yet.

manipulation. This Part aims to demonstrate that by grounding liability in scienter, the legal framework fails to adequately punish many forms of algorithm-related manipulation and other forms may evade punishment altogether. Thus, current laws and regulations fail to effectively deter manipulation in the markets, undermining regulators' authority and efficient capital allocation.

A. Algorithms & Scienter

One of the primary obstacles to application of anti-manipulation laws to algorithms is the basic principle that algorithms cannot form intent. Only humans and business entities constitute "persons" under the law;[171] thus, unsurprisingly, computers, algorithms, and AI programs do not have legal personhood.[172] When algorithms cause market disruptions or distortions, it is necessary to identify which legal person ought to be held responsible. But this inquiry is not as straightforward as it initially appears. With preprogrammed algorithms, trading is a matter of following preset electronic instructions—if X occurs, then do Y. Market harm that results from these types of algorithms can often be traced back to human programmers; even if the process is time consuming and costly, it is, nonetheless, possible.[173] Presuming intent is visible through the code, the programmer is liable for the manipulative conduct of the algorithm, even if it goes beyond the scope of her initial plans. The manipulative intent of the programmer, therefore, allows us to hold her accountable for any resulting algorithmic misconduct.

But the issue is murkier when dealing with AI algorithms employing machine-learning techniques. As discussed above, AI machine-learning algorithms learn and modify their behavior in response to continuous analysis of the markets, available information, and expected market movements, without human guidance.[174] In these

171. *See* Amanda D. Johnson, Comment, *Originalism and* Citizens United*: The Struggle of Corporate Personhood*, 7 RUTGERS BUS. L.J. 187, 187 (2010) (indicating that *Citizens United* stands for the proposition that business entities and individuals have equal identity as "persons" under the law).

172. Shawn Bayern, *The Implications of Modern Business-Entity Law for the Regulation of Autonomous Systems*, 19 STAN. TECH. L. REV. 93, 95 (2015) ("(1) [N]onhuman forms of life, including other animals; (2) natural systems; and (3) algorithmic processes implemented in software or hardware, including those that underlie modern computer systems—are not traditionally conceived as legal persons.").

173. *See* Davis, *supra* note 142 (explaining that to catch Sarao, regulators had to "pick through mountains of trading data" and seek "the assistance of a consulting firm and a high-priced professor").

174. *See* Ryan Calo, *Artificial Intelligence Policy: A Primer and Roadmap*, 51 U.C. DAVIS L. REV. 399, 405 (2017) (describing machine learning); *Machine Learning Algorithms for Trading*,

instances, the most direct "decisionmaker," whose intent ought to matter for assigning liability, is the algorithm. Given that algorithms cannot legally form the requisite intent, even when their actions are independent, imposing liability on the algorithms for the consequences of their harmful conduct is beyond the scope of the legal framework.[175] Further, unless it can be demonstrated that the programmer had manipulative intent when she designed the AI algorithm, it is unlikely that the Commissions could hold her liable for the algorithm's conduct. In sum, given the difficulties in deciphering why an AI algorithm utilizing machine learning makes the decisions it does, finding clear evidence of intent is highly unlikely.

It is arguable, therefore, that algorithm-based manipulation is less likely to result in legal liability because the law does not capture algorithmic decisionmaking. The available loophole for algorithmic manipulation would encourage potential wrongdoers to use algorithms (the more complex the better) to manipulate the market, expecting that the algorithm would mask their intentions. In the end, the low likelihood of punishment for manipulation effectuated through algorithms would decrease the deterrent effect of the legal regime, as deterrence theory predicts.

B. The Problem of Abstraction

Given the limitations of directly applying anti-manipulation liability to algorithms, deterrence of algorithmic manipulation lies in altering the cost-benefit analysis of humans responsible for trading algorithms. But there is an inherent layer of abstraction between the programmer's conduct and the algorithm's operation that complicates questions of scienter and, by extension, liability for manipulation. In designing a preprogrammed algorithm, the programmer manifests her goals for the algorithm through the programming code;[176] with AI machine-learning algorithms, the programmer sets a goal for the algorithm to achieve in solving a problem.[177] Translating expectations from natural language into computer code for an algorithm can be quite

---

TRADING TUITIONS (Feb. 9, 2017), http://tradingtuitions.com/machine-learning-algorithms-trading [https://perma.cc/M9ND-NH7S] ("Machine learning algorithms for trading continuously monitor the price charts, patterns, or any fundamental factors and adjust the rules accordingly.").

175. *See supra* Section II.C for discussion on holding the programmer liable in attenuated cases.

176. Yadav, *supra* note 83, at 1620 (explaining that after traders decide on a trading strategy, "[p]rogrammers then build the computerized algorithm or series of algorithms to execute the strategy in the market").

177. Mark A. Lemley & Bryan Casey, *Remedies for Robots*, 86 U. CHI. L. REV. 1311, 1324 (2019).

challenging[178] and, importantly, attenuates the causal connection between the programmer's intention and the algorithm's ultimate actions. This "layer of abstraction" between what the programmer expects and what the algorithm does is possible with all trading algorithms and is particularly acute with AI machine-learning algorithms.

Recall that the processes by which machine-learning AI algorithms make decisions, namely neural networks, are a black box to the programmer and to anyone investigating ex post.[179] Abstraction coupled with the black box problem undercuts the likelihood of liability because it is difficult to identify the programmer's intent in most cases, except for instances of deliberate manipulation. The further removed the programmer is from the algorithm's ultimate decisionmaking, the less likely it is that regulators can successfully hold the programmer responsible for market manipulation. Altogether, this creates legal uncertainty because it is unclear at what point the programmer's intent is too remote to reasonably constitute the basis for liability; this uncertainty encourages, rather than deters, algorithmic manipulation. The layers of abstraction innate to preprogrammed and AI machine-learning algorithms, albeit to different degrees, diminish the relevance and applicability of scienter as a basis of liability for manipulation.

Another way in which abstraction challenges the anti-manipulation framework occurs when the link between the programmer's goals and the algorithm's conduct is severed. This may manifest in two ways. First, as discussed above, a programmer may code a trading algorithm to accomplish a permissible trading strategy, but the algorithm may engage in "rational distortion" to more efficiently accomplish its goals.[180] Although the trader did not intend for the algorithm to distort the market, the AI algorithm's machine-learning techniques may have found a way to accomplish its goals using impermissible means.

In such a case, some may argue that the algorithm's ability to engage in rational distortion is indicative of the programmer's underlying manipulative intent.[181] Imputing liability to the

178. *See* David Auerbach, *The Programs That Become the Programmers*, SLATE (Sept. 25, 2015, 1:34 PM), https://slate.com/technology/2015/09/pedro-domingos-master-algorithm-how-machine-learning-is-reshaping-how-we-live.html [https://perma.cc/WS36-LT4E] (explaining how algorithms struggle in situations that do not have clear boundaries or defined terms).

179. *See* Bathaee, *supra* note 137, at 901–02 (explaining why humans are unable to process the decisions made by neural networks).

180. *See supra* Section II.C.3.

181. *See, e.g.*, Kim A. Kamin & Jeffrey J. Rachlinski, *Ex Post ≠ Ex Ante: Determining Liability in Hindsight*, 19 L. & HUM. BEHAV. 89, 91, 101 (1995) (examining the problematic phenomenon that a person is more likely to find blame when she has the benefit of ex post review).

programmer on the basis of the ultimate conduct of the algorithm would, however, be contrary to the anti-manipulation framework, which grounds liability on ex ante intentions, not ex post harms.[182] Indeed, under the intent-based liability framework, the absence of the programmer's intent to manipulate the market ought to be sufficient to protect her from liability. Scienter, therefore, does not provide a satisfying basis on which to hold a programmer liable for the harm resulting from the manipulative conduct of her algorithm when the link between the two is severed.

Second, and notably, the law may provide a basis for liability in the reverse scenario—that is, a situation in which the programmer intended to manipulate the market, but the algorithm failed to do so. In accordance with the Commissions' intent-centric approach to "open-market manipulation," a trader can be liable for market manipulation on the basis of her manipulative intent alone.[183] Open-market manipulation refers to market manipulation that is accomplished entirely through facially legitimate transactions.[184] In prosecuting traders for open-market manipulation, the Commissions have adopted the theory of liability that manipulative intent alone is sufficient to hold a trader liable for market manipulation.[185] The example of intended-but-failed algorithmic manipulation differs somewhat from open-market manipulation in that no manipulation occurred; yet, the Commissions' theory of liability would impose liability on the programmer based on her manipulative intent.[186] This example, particularly in contrast to the prior examples, demonstrates the scienter standard's overbroad nature when applied to algorithms, which increases uncertainty and decreases deterrence.

---

182. *See supra* Section II.A.

183. *See* Fischel & Ross, *supra* note 23, at 510 ("[T]here is no objective definition of manipulation. The only definition that makes any sense is subjective—it focuses entirely on the intent of the trader.").

184. Fletcher, *supra* note 8, at 484.

185. *See* Fischel & Ross, *supra* note 23, at 510.

186. *See, e.g.*, Markowski v. SEC, 274 F.3d 525, 528 (D.C. Cir. 2001) ("Legality would thus depend entirely on whether the investor's intent was 'an investment purpose' or 'solely to affect the price of [the] security.' " (quoting United States v. Mulheren, 938 F.2d 364, 368 (2d Cir. 1991))). In holding that the CFTC's complaint in *CFTC v. Kraft Foods Group., Inc.*, 153 F. Supp. 3d 996, 1014 (N.D. Ill. 2015), sufficiently pled manipulation, the court relied on the Commission's finding that:

> (1) Kraft took a huge wheat futures position; (2) that it did not intend to use in production; (3) but instead intended that the position would signal Kraft's demand for wheat in the relevant time period; (4) in a way that would mislead others in the market into thinking that Kraft would take delivery of its futures position and not buy cash wheat; (5) which was intended to, and in fact did, cause cash wheat prices to decrease and the price for futures to increase.

In sum, the anti-manipulation framework does not effectively deter algorithmic manipulation because the level of abstraction between the programmer and the algorithm undermines the applicability of intent to the relevant conduct. The real and potential gap between the aims of the programmer and the operation of the trading algorithm attenuates liability for algorithmic manipulation, especially in an intent-based framework, thereby rendering the liability regime's deterrence ineffective.

C. Uncertain Enforcement

Detecting algorithmic market manipulation is, on the one hand, easier than detecting non-computer-based forms of manipulation. But it can also be more difficult, particularly in algorithm-dominated markets. Algorithmic trading leaves behind evidence of executed transactions that regulators can follow to identify manipulative and disruptive conduct.[187] Computerized trades provide a tangible record of who did what and when that regulators can utilize to detect wrongdoers. Once such misconduct is identified, regulators can seek access to a trader's programming code, which may indicate the programmer's manipulative intent and result in liability.[188] In this regard, algorithmic manipulation may be more easily detected than traditional (i.e., non-computer-based) forms of market manipulation that depended on undisclosed and, oftentimes, untraceable agreements among parties.[189]

Yet, the availability of swaths of trading data, although a blessing for regulators, can also be a burden to proving algorithmic manipulation.[190] To identify manipulative algorithms, regulators must

187. *See* Yadav note 83, at 1620 ("[A]utomated trading requires investment in constructing a detailed plan before any trading can take place. Traders devise a strategy to buy and sell securities.").

188. *See id.* ("[T]raders set parameters within which their algorithms trade. . . . [A]lgorithms comprise pre-set mathematical instructions that detail their exact terms of operation.").

189. Yadav, *supra* note 122, at 1074 ("From an enforcer's standpoint, this state of affairs is a far cry from the back-room dealings and the nudges and winks that might have characterized attempts at manipulation in nonautomated markets.").

190. Koosha Golmohammadi, Osmar R. Zaïane & David Díaz, *Detecting Stock Market Manipulation Using Supervised Learning Algorithms*, 2014 IEEE INT'L CONF. ON DATA SCI. & ADVANCED ANALYTICS 435, 435, https://www.researchgate.net/publication/282950245_Detecting_stock_market_manipulation_using_supervised_learning_algorithms [https://perma.cc/C287-9DRD]:

> The existing approach in industry for detecting market manipulation is a top-down approach that is based on a set of known patterns and predefined thresholds. . . . These methods are based on expert knowledge but suffer from . . . issues[,] [including] adapting to the changing market conditions whilst the amount of transactional data is exponentially increasing . . . .

sift through and interpret mountains of data to deduce problematic trading patterns within a sea of legitimate ones. Even with deliberately manipulative algorithms, this endeavor would require a significant outlay of time, costs, and resources from regulators. Algorithmic trading may leave a paper trail, but the effort required to interpret the data and detect manipulative conduct could be a significant barrier in detection, further weakening deterrence.[191] Regulators would need the expertise to decipher algorithmic code and trading programs to determine whether the algorithm evidences the trader's intent to manipulate. The Commissions, however, lack the technology needed to effectively oversee the markets, thereby leaving the markets unprotected against the harms of algorithmic manipulation (a reality acknowledged by regulators themselves).[192] Thus, to the extent regulators cannot successfully punish manipulation because of a lack of resources or expertise, deterrence is less credible.

Importantly, regulatory oversight of algorithmic traders is uneven, with half the market subject to regulatory oversight and the other half not, which places the market in a precarious condition. On the one hand, the SEC has some oversight of algorithmic traders. Regulation Systems Compliance and Integrity ("Reg SCI") requires firms that employ algorithmic trading strategies to implement practices to reduce the likelihood of harms from algorithmic trading programs and mitigate their impact should they occur.[193] These practices include rules on general risk assessment and response, software development and implementation, software testing, and compliance, among others.[194] Additionally, persons responsible for design, development, or modification of an algorithmic trading program must be registered as a "Securities Trader" with the Financial Industry Regulatory Authority and pass a qualifying exam.[195] Reg SCI was proposed in response to

191. *See id.* (describing the challenges of analyzing vast amounts of data to detect market manipulation).

192. *See* Silla Brush, *High-Speed Trades Outpace CFTC's Oversight, O'Malia Says*, BLOOMBERG (May 6, 2014, 11:01 PM CDT), https://www.bloomberg.com/news/articles/2014-05-06/high-speed-trades-outpace-cftc-s-oversight-o-malia-says [https://perma.cc/7BFU-K5U9] ("The CFTC lacks the technology necessary to routinely oversee the millions of messages traders send every day to futures exchanges . . . .").

193. *See Spotlight on Regulation SCI*, SEC, https://www.sec.gov/spotlight/regulation-sci.shtml (last visited Oct. 2, 2020) [https://perma.cc/LB64-3V8H] (broadly describing Reg SCI's requirements).

194. *See* Yesha Yadav, *Algorithmic Trading and Market Regulation*, *in* GLOBAL ALGORITHMIC CAPITAL MARKETS: HIGH FREQUENCY TRADING, DARK POOLS, AND REGULATORY CHALLENGES 232, 232–33, 241 (Walter Mattli ed., 2019).

195. Michael T. Foley, Janet M. Angstadt, Ross Pazzol & James D. Van De Graaff, *FINRA Rule Amendment Requires Registration of Associated Persons Who Develop Algorithmic Trading Strategies*, 17 J. INV. COMPLIANCE 39, 39 (2016).

numerous high-profile technological failures, not least of which was the Flash Crash.[196] The regulations aim to strengthen the securities markets, reduce errors, improve market resiliency in the face of errors, and enhance the SEC's oversight of the market's technological infrastructure.[197] As an initial, albeit imperfect, step towards algorithmic trading oversight, Reg SCI is useful in providing the SEC with data about how algorithmic traders operate in the markets and what impact algorithmic trading strategies' have on the market.

On the other hand, the CFTC has no specific regulatory oversight of algorithmic trading in the commodities markets. In 2015, the CFTC proposed Regulation Automated Trading ("Reg AT") to address the agency's concerns with the risks that arise from algorithmic trading strategies, including market illiquidity and disruption.[198] Under Reg AT, persons who trade using algorithmic programs would be required to register with the CFTC and, consequently, be subject to additional compliance requirements under Reg AT.[199] Also, Reg AT set forth a multipart risk control structure that would enable the CFTC to more closely monitor algorithmic trading at different stages in the trading process.[200] Lastly, and most controversially, Reg AT would require the source code of algorithmic trading programs be preserved according to specified provisions and accessible to the CFTC via subpoena.[201] Notably, the proposed regulations also would have granted the CFTC access to records tracking any changes to the source code and to log files recording the algorithm's market activity.[202] Reg AT received considerable pushback from the industry, especially with regards to

196. Samuel Wolff & Amy Thayer, *Cybersecurity and the SEC: Part 2*, 38 SEC. & FED. CORP. L. REP., no. 1, 2016, at 1, 3.

197. Regulations Systems Compliance and Integrity, 78 Fed. Reg. 18,084, 18,092 (proposed Mar. 25, 2013) (to be codified at 17 C.F.R. pt. 242, 249).

198. Regulation Automated Trading, 80 Fed. Reg. 78,824 (proposed Dec. 17, 2015) (to be codified at 17 C.F.R. pt. 1, 38, 40, 170). The Proposed Rule was opened for a second round of commenting in January 2017, but ultimately was not promulgated. Regulation Automated Trading, 82 Fed. Reg. 8,502 (comment period extended Jan. 26, 2017) (to be codified at 17 C.F.R. pt. 1, 38, 40, 170); Regulation Automated Trading; Withdrawal, 85 Fed. Reg. 42,755 (July 15, 2020) (to be codified at 17 C.F.R. pt. 1, 38, 40, 170).

199. Regulation Automated Trading, 80 Fed. Reg. at 78,914.

200. *Id.* at 78,838.

201. Regulation Automated Trading, 81 Fed. Reg. 85,334, 85,337 (proposed Nov. 25, 2016) (to be codified at 17 C.F.R. pt. 1, 38, 40, 170). Reg AT and the Supplemental Proposal also require periodic review of compliance with Reg AT and offer options to facilitate the compliance of third-party systems. *Fact Sheet – Supplemental Notice of Proposed Rulemaking on Regulation Automated Trading*, COMMODITY FUTURES TRADING COMM'N 2–3 (2016), https://www.cftc.gov/sites/default/files/idc/groups/public/@newsroom/documents/file/regat_factsheet110316.pdf [https://perma.cc/6U7F-DRTB] [hereinafter *CFTC Fact Sheet*].

202. *CFTC Fact Sheet*, *supra* note 201, at 2.

source code access and preservation.[203] After reproposing the rules and a change from the Obama to Trump Administration, Reg AT was never finalized.[204]

The discrepancy between the level of regulatory oversight each agency has over algorithmic trading in its respective markets creates a significant gap in the anti-manipulation legal regime. With the SEC having more meaningful oversight over algorithmic trading, it is in a better position to identify manipulation and possibly minimize its impact on the markets. The CFTC, on the other hand, has limited ex ante market information, thereby diminishing the agency's efficacy in detecting potentially manipulative behavior.

The absence of algorithmic trading surveillance in the commodities markets decreases the likelihood of would-be manipulators being caught and punished, weakening the deterrent effect of the anti-manipulation framework. Further, the lopsided market oversight encourages regulatory arbitrage, as algorithmic traders preferring less regulation are likely to gravitate to the commodities market. Given the interconnected nature of the markets, however, whatever risks that accumulate in the commodities markets are likely to spill over into the securities markets.[205] Thus, the uneven likelihood of detection diminishes deterrence in the markets overall, as wrongdoers gravitate to markets in which their misdeeds are likely undetected.

D. Dissimilar Liability

Uncertainty also arises when similar conduct receives dissimilar treatment under the legal framework. To the extent would-be manipulators receive different liability for conduct that is similar in

---

203. *See* Regulation Automated Trading, 80 Fed. Reg. at 78,947 ("Regulation AT dramatically lowers the bar for the federal government to obtain [a source code repository for algorithms]."); *see also* Gregory Meyer & Phillip Stafford, *US Regulators Propose Powers to Scrutinise Algo Traders' Source Code*, FIN. TIMES (Dec. 1, 2015), https://www.ft.com/content/137f81bc-944f-11e5-b190-291e94b77c8f [https://perma.cc/HV62-J4TZ] (explaining concerns of HF trading firms in response to the new regulation).

204. Nicholas A.J. Wendland, *CFTC Withdraws Regulation AT and Proposes New Electronic Trading Risk Principles*, NAT'L L. REV. (July 8, 2020), https://www.natlawreview.com/article/cftc-withdraws-regulation-and-proposes-new-electronic-trading-risk-principles [https://perma.cc/H23J-MXVT]. As of February 2021, algorithmic trading remains unregulated in the commodities market. The recently elected Biden Administration has not yet made any indication whether it will attempt to revive the proposal.

205. *See* COMMODITY FUTURES TRADING COMM'N & SEC. & EXCH. COMM'N, PRELIMINARY FINDINGS REGARDING THE MARKET EVENTS OF MAY 6, 2010, app. A, at 15 (2010), https://www.sec.gov/sec-cftc-prelimreport.pdf [https://perma.cc/BXL8-4DXY] ("Because the markets today are increasingly fast, automated, and interconnected, an erroneous trade on one market can very rapidly trigger a wave of similarly erroneous trades on other markets.").

function but not in form, the legal regime's deterrent effect is weakened. The problem of dissimilar treatment for similar conduct is not unique to algorithmic versus human manipulation. Rather, it is a deeper problem associated with the scienter focus of anti-manipulation laws and regulations, especially as applied to open-market manipulation. As discussed above, under the current theory of open-market manipulation, a trader can be liable for manipulation even if her transactions are legitimate if she had the intent to manipulate the market at the time of trading.[206] Practically, this means that two traders may engage in the same conduct, but one may be liable for open-market manipulation because of her intent and the other not liable because she lacked the requisite intent. The Commissions' approach has been criticized for creating significant legal uncertainty regarding how anti-manipulation laws are applied to legitimate transactions because of the equivocal and circumstantial evidence typically relied on to prove the trader's manipulative intent.[207] This issue is all the more pronounced with algorithm-related manipulation.

Algorithms can more effectively implement legitimate trading strategies that can distort or manipulate the market, but they will always lack the requisite mental state to be held accountable. More to the point, if a programmer uses an algorithm to engage in open-market manipulation, the likelihood of liability is further decreased. The legitimacy of the transactions would hinge liability on deciphering whether the programmer had manipulative intent, and the evidentiary burden is the same, if not heavier, with the involvement of a trading algorithm. Again, without a smoking gun or convincing evidence of the programmer's manipulative intent, the use of an algorithm would likely place the harm from open-market manipulation beyond the legal framework's scope.

Similarly, if an AI machine-learning algorithm independently decides to engage in disruptive but not illegal conduct, such as marking

---

206. *See supra* note 109 and accompanying text; *see, e.g.*, SEC v. Masri, 523 F. Supp. 2d 361, 372 (S.D.N.Y. 2007):

> [I]f an investor conducts an open-market transaction with the intent of artificially affecting the price of the security, and not for any legitimate economic reason, it can constitute market manipulation. Indeed, "the only definition [of market manipulation] that makes any sense is subjective—it focuses entirely on the intent of the trader."

(alteration in original) (quoting Fischel & Ross, *supra* note 23, at 510).

207. *See* Fletcher, *supra* note 8, at 553 (explaining that, under the Commissions' approach, "intent plays an outsized role that does not increase market safety"); *see also* John Crabb, *CFTC's Market Manipulation Enforcement Position Under Fire*, INT'L FIN. L. REV. (May 2, 2019), https://www.iflr.com/article/b1lmx9r4l5vwbv/cftcs-market-manipulation-enforcement-position-under-fire [https://perma.cc/SQG2-KHAT] (describing the CFTC's "weakened" position in exerting its anti-manipulation authority due to a recent loss at trial).

the close,[208] it is unclear whether the programmer would face liability. And, for the reasons enumerated above, proving that the programmer intended the algorithm's behavior may be particularly difficult when dealing with AI machine-learning algorithms.[209] The current legal regime makes it easier for algorithm-related open-market manipulation to escape liability, despite being punishable when done by a human. Imposing liability differently for similar conduct undermines the deterrent effect of the regulatory regime, creating a loophole that decreases the certainty of punishment for algorithmic manipulation.[210]

* * *

The existing liability framework fails to effectively deter manipulation in financial markets increasingly dominated by algorithmic trading. The mismatch between anti-manipulation laws and the realities of algorithmic trading increases legal uncertainty, making punishment, detection, and enforcement of algorithm-related manipulation less likely. The law's inability to fulfill one of its fundamental goals leaves the markets vulnerable to increased manipulative conduct and the attendant harms that accompany such distortion. In sum, the law fails to force wrongdoers to internalize the costs of their manipulative conduct, causing the markets to bear the negative externalities of algorithm-related manipulation.

E. Market Implications of Failed Deterrence

The law's shortcomings in achieving credible deterrence of manipulative behavior are particularly salient as algorithmic trading becomes the norm in the financial markets.[211] The mismatch between the requirements of the law and the realities of algorithmic trading

208. "Marking the close" (also known as "banging the close") is the practice of aggressively trading at the end of the trading day. Fletcher, *supra* note 8, at 507. The practice is not illegal, but it is not looked on favorably by the Commissions; however, there are legitimate, nonmanipulative reasons a trader may execute several transactions close to the end of the trading day. *Id.*; *see also CFTC Glossary*, CFTC, https://www.cftc.gov/ConsumerProtection/EducationCenter/CFTCGlossary/glossary_b.html (last visited Oct. 2, 2020) [https://perma.cc/EK4H-JLYV] (defining "banging the close" as "[a] manipulative or disruptive trading practice").

209. *See supra* Section III.A.

210. *See* COMMODITY FUTURES TRADING COMM'N, TRANSCRIPT OF TECHNOLOGY ADVISORY COMMITTEE MEETING 158–59 (2014), http://www.cftc.gov/ucm/groups/public/@newsroom/documents/file/tac_021014_transcript.pdf [https://perma.cc/BXL8-4DXY] ("[P]ractices that are illegal when performed by humans, should be equally illegal when done by computers," and if current law does not account for this, "then there is an urgent need to adapt the rulebook to match the playing field.").

211. *See* Lin, *supra* note 24, at 1270–71 (highlighting the "new financial reality" for regulators brought about by the increasing use of "advanced technology" in finance).

facilitates greater opportunities for market manipulation, with deleterious consequences for the financial markets' health and stability. Indeed, algorithmic-based manipulation has significant implications for the markets that heighten the shortcomings of the existing legal regime in effectively deterring this form of market abuse.

Specifically, failed deterrence of algorithm-related manipulation exacerbates systemic risk in the markets.[212] Typically, market manipulation schemes are not considered to be a concern for financial stability because of the limited scope and impact of manipulation schemes. Manipulation schemes usually (1) target small, illiquid assets, (2) one at a time, and (3) on a short-term horizon, which altogether decreases the likelihood that such schemes would threaten market stability.[213] These limitations, however, are not applicable to algorithm-related market manipulation because it may have deep and lasting consequences on the financial markets. As seen with the 2010 Flash Crash, algorithm-related manipulation can cause widespread volatility, threatening the entire financial market's stability.

First, algorithmic trading is used mostly in liquid assets because the strategies employed depend on deep pools of liquidity to be successful. Finding and profiting from arbitrage opportunities in the markets in a fraction of a second, thousands of times per day, requires access to highly liquid markets. The same is true of algorithm-related market manipulation. Spoofing, for example, is most successful in heavily traded assets because this allows the manipulator to profit from her fake orders over thousands of trades. The focus of algorithm-related manipulation on larger, more liquid assets increases the likelihood that the fallout from such schemes will have systemic reverberations. This was evident with the 2010 Flash Crash, in which Navinder Sarao flooded the Chicago Mercantile Exchange with sell orders for the S&P 500 E-Minis.[214] As a result of Sarao's efforts to manipulate one of the most commonly traded stock index futures, the financial market went

212. Steven L. Schwarcz provides an oft-quoted and useful definition of systemic risk:

> [T]he risk that (i) an economic shock such as market or institutional failure triggers (through a panic or otherwise) either (X) the failure of a chain of markets or institutions or (Y) a chain of significant losses to financial institutions, (ii) resulting in increases in the cost of capital or decreases in its availability, often evidenced by substantial financial-market price volatility.

Steven L. Schwarcz, *Systemic Risk*, 97 GEO. L.J. 193, 204 (2008).

213. Gina-Gail S. Fletcher, *Macroeconomic Consequences of Market Manipulation*, 83 LAW & CONTEMP. PROBS. 123, 125–27 (2020).

214. Complaint for Injunctive Relief, Civil Monetary Penalties & Other Equitable Relief at 3, CFTC v. Nav Sarao Futures Ltd. PLC, No. 1:15-cv-03398, 2015 WL 1843321 (N.D. Ill. Apr. 17, 2015), ECF No. 1.

into a twenty-two-minute rollercoaster ride of volatility.[215] And, in the end, the market suffered a trillion dollars in losses.[216]

Second, algorithms allow traders to buy and sell different asset types at once, increasing the profitability of their trading strategies and diversifying their investment risk. The same is also true of a manipulator's capacity. Rather than focusing her efforts on a single asset, a would-be manipulator can focus on numerous assets, which may exacerbate volatility and systemic harm in the markets. The DOJ and CFTC's criminal spoofing prosecution against Michael Coscia is a salient example. In 2013, Coscia was charged with using one algorithmic trading program across approximately twelve different commodities markets to create an illusion of demand, thereby enabling him to earn profits on smaller trades on the opposite side of the market.[217] According to prosecutors, with the aid of algorithmic trading programs, Coscia netted $1.4 million in illegal profits in less than three months.[218] Although Coscia's scheme did not destabilize the markets, it is not far-fetched to think that it could have. Significant volatility in numerous asset classes in a short span of time could have a similar effect as seen in the 2010 Flash Crash, lending further support to concerns that algorithm-related manipulation increases systemic risk in the markets.

Third, notwithstanding the short-term horizon of manipulative schemes, including algorithm-related ones, the interconnected nature of the markets and the prevalence of algorithmic trading enhance the risk that manipulation may cause financial instability. In algorithm-dominated markets, the linkages between different market segments, types of assets, and market actors may become fragile during times of stress, such as extreme volatility owing to manipulation. Further, when these networks are coupled with the high volume and high speed of many algorithmic traders, there is a strong likelihood that a manipulative scheme can destabilize the financial markets. In the absence of manipulation, these market networks increase efficiency within the markets. These connections, however, can also facilitate the spread of contagion throughout the market. The prevalence of algorithmic trading in the markets also contributes to the spread of

215. *Id.* at 3; COMMODITY FUTURES TRADING COMM'N & SEC. & EXCH. COMM'N, *supra* note 151, at 1–3.

216. *CFTC Fact Sheet*, *supra* note 201; *see also* Barrales, *supra* note 154, at 1195–97 (noting that, in addition to causing momentary losses of nearly $1 trillion, the Flash Crash "rattled investor confidence" and precipitated withdrawals of $90 billion from U.S. stock mutual funds).

217. CFTC Press Release on Coscia, *supra* note 147 (detailing Coscia's spoofing method).

218. *Id.* ("The CFTC Order requires Panther and Coscia to . . . disgorge $1.4 million in trading profits . . . .").

instability across these networks. Many algorithms make similar assumptions about the markets and tend to react similarly to market movements, especially in times of stress.[219] The correlated responses of algorithms and the networks that link the markets all contribute to the likelihood that algorithm-related manipulation will cause systemic harm.

Although the 2010 Flash Crash is one of the most significant examples to date, there are numerous additional examples of other flash crashes in the markets. For example, one day in 2015, the Dow fell 1,100 points in the first five minutes of trading, owing to fears of a slowing Chinese economy and market illiquidity.[220] During this crash, HF and other algorithmic traders withdrew en masse from the market, further exacerbating illiquidity and pricing anomalies.[221] Similarly, in 2016 the British pound fell by six percent against the U.S. dollar, which some believe was as a result of algorithms reacting to commentary on Brexit.[222] Despite the fact that neither example is specifically tied to algorithmic manipulation, they demonstrate the ease with which volatility and instability can spread through algorithm-dominated markets, affecting a wide range of stocks, indices, and traders.[223] One can fairly assume that these effects would be worse if a manipulative scheme or a rogue algorithm were behind the markets' deterioration. The interconnections between markets, the prevalence of high-volume algorithmic traders, and the herding tendencies of algorithmic programs increase the systemic risks arising from manipulative

---

219. *See* GOV'T OFF. FOR SCI., *supra* note 131, at 61–87 (explaining that algorithmic trading "can lead to significant instability in financial markets . . . [due to] self-reinforcing feedback loops . . . [that] can amplify internal risks and lead to undesired interactions and outcomes").

220. Bob Pisani, *What Happened During the Aug 24 'Flash Crash,'* CNBC: TRADER TALK (Sept. 25, 2015, 3:59 PM EDT), https://www.cnbc.com/2015/09/25/what-happened-during-the-aug-24-flash-crash.html [https://perma.cc/2YGA-DRRU].

221. *Id.*

222. Jethro Mullen, *U.K. Pound Plunges More Than 6% in Mysterious Flash Crash*, CNN (Oct. 7, 2016, 11:30 AM ET), https://money.cnn.com/2016/10/06/investing/pound-flash-crash-currency-brexit/index.html [https://perma.cc/7294-8UWE]; Jamie Condliffe, *Algorithms Probably Caused a Flash Crash of the British Pound*, MIT TECH. REV. (Oct. 7, 2016), https://www.technologyreview.com/2016/10/07/244656/algorithms-probably-caused-a-flash-crash-of-the-british-pound [https://perma.cc/LYB2-RRD3].

223. *See, e.g.*, Mullen, *supra* note 222; Pisani, *supra* note 220; Fred Imbert, *'Flash Crash' Hits the Currency Markets as Financial Volatility Intensifies*, CNBC (Jan. 3, 2019, 8:17 AM EST), https://www.cnbc.com/2019/01/03/yen-surges-against-global-currencies-after-flash-crash.html [https://perma.cc/76E4-WXMV] (explaining the surge in value of the Japanese Yen as the result of an eight percent flash crash in Apple stock stoking economic fears); Fitz Tepper, *Coinbase Is Reimbursing Losses Caused by the Ethereum Flash Crash*, TECHCRUNCH (June 24, 2017, 11:32 AM CDT), https://techcrunch.com/2017/06/24/coinbase-is-reimbursing-losses-caused-by-the-ethereum-flash-crash [https://perma.cc/WC5D-ZWVC] (attributing Ethereum's flash crash from approximately $320.00 to $0.10 to a large sell order triggering eight hundred stop loss orders and margin liquidations).

schemes, propagating their impact beyond their original sphere. The legal framework's failure to credibly deter algorithm-related manipulation exposes the financial markets to a significant source of systemic risk. Therefore, it becomes increasingly important to consider how to create an effective system of deterrence in algorithm-dominated financial markets.

IV. PATHWAYS FORWARD: ACHIEVING CREDIBLE DETERRENCE

As algorithms, especially AI algorithms, become more ubiquitous in the financial markets, it is increasingly important to address the gaps that arise from the application of the law to evolving technologies. The challenge facing lawmakers is how to foster technological innovation in the markets without allowing modern-day manipulation techniques that exploit the technology to thrive. The anti-manipulation framework's failure to effectively detect, punish, and ultimately deter algorithm-related manipulation has significant repercussions for the markets, as discussed above.

This Part considers potential pathways forward in algorithm-dominated markets to create a credible deterrence regime for manipulation and, potentially, other financial regulation violations tethered to scienter. This Part analyzes the promises and shortcomings of an oft-proposed solution to the problems of algorithms and AI in various domains: transparency. This Part also assesses a range of legal and policy responses that can emphasize certainty of punishment, thereby enhancing the legal regime's deterrence of manipulation.

A. Transparent & Explainable Algorithms

With preset algorithms, review of the code and the programmer's work ought to provide insight into the operations and decisions of the algorithm. With AI machine-learning algorithms, however, examining the work of the programmer is not likely to make the algorithm's decisionmaking any clearer. A recurring proposed solution to the black box problem that is innate to AI algorithms is to make them more transparent and explainable.[224] The inability to understand the rationale behind an algorithm's decisionmaking raises concerns regarding the trustworthiness of the algorithm's operations in the markets, especially when it distorts or otherwise harms the markets. Demands for greater explainability and transparency are particularly

224. *See, e.g.*, Amina Adadi & Mohammed Berrada, *Peeking Inside the Black-Box: A Survey on Explainable Artificial Intelligence (XAI)*, 6 IEEE ACCESS 52138, 52138 (2018), https://ieeexplore.ieee.org/document/8466590 [https://perma.cc/8WXG-T2A5].

strong in instances when individual liberty is at stake, such as in criminal sentencing and determinations of recidivism risk.[225] But concerns regarding the opacity of AI algorithms' decisionmaking permeate a range of fields—from health care, to consumer finance, to hiring.[226]

In response to these concerns, there has been a growing push for the development and deployment of "explainable AI." Explainable AI refers to the range of efforts to assist humans in understanding how or why a machine-learning algorithm arrived at its decision or solution.[227] The emphasis is on providing insight into how the algorithm operates or an approximation of its processes in reaching its final conclusion. In addition to machine-learning models that are designed to be explainable and transparent, explainable AI has two broad approaches.

One approach is the "exogenous approach," which aims to explain how the entire model works or, alternately, how the model works in a specific case.[228] The exogenous approach provides information on how the AI algorithm works by explaining the programmer's intentions, the parameters and data used to train the algorithm, and the means by which the algorithm was tested to prevent or minimize the occurrence of unwanted behavior, among other things.[229]

The second approach to explainable AI attempts to replicate the AI algorithm's decisionmaking.[230] Revealing the course code underlying the algorithm is one way to accomplish this, but, as described above, this may prove unsatisfactory because of the machine-learning techniques used.[231] Another alternative would be to create a "surrogate

---

225. *See, e.g.*, Jessica M. Eaglin, *Population-Based Sentencing*, 106 CORNELL L. REV. 353; Jessica M. Eaglin, *Constructing Recidivism Risk*, 67 EMORY L.J. 59 (2017) (explaining the need for accountability measures for developers who create tools used to evaluate recidivism risk for purposes of criminal sentencing).

226. *See, e.g.*, W. Nicholson Price II, M*edical Malpractice and Black-Box Medicine*, *in* BIG DATA, HEALTH LAW, AND BIOETHICS 295 (I. Glenn Cohen, Holly Fernandez Lynch, Effy Vayena & Urs Gasser eds., 2018) (assessing the black box problems that stem from the use of AI in medicine and healthcare); Kristin Johnson, Frank Pasquale & Jennifer Chapman, *Artificial Intelligence, Machine Learning, and Bias in Finance: Toward Responsible Innovation*, 88 FORDHAM L. REV. 499 (2019) (discussing the problems of AI in consumer finance); McKenzie Raub, *Bots, Bias and Big Data: Artificial Intelligence, Algorithmic Bias and Disparate Impact Liability in Hiring Practices*, 71 ARK. L. REV. 529 (2018) (addressing the systemic and legal problems posed by introducing AI algorithms into hiring systems).

227. Ashley Deeks, *The Judicial Demand for Explainable Artificial Intelligence*, 119 COLUM. L. REV. 1829, 1834 (defining explainable AI).

228. *Id.* at 1835–37 (defining and describing the exogenous approach to explainable AI).

229. *Id.* at 1835.

230. *Id.* at 1837.

231. *See supra* Section II.B.2 (explaining the difficulty in fully understanding AI's decisionmaking process in producing outputs through machine learning).

model," which assesses the inputs and outputs the machine-learning algorithm uses, thereby providing insight into how the algorithm may weigh certain factors in its decisionmaking.[232]

Explainable AI undoubtedly has significant promise for increasing the transparency of algorithms, both preset and AI machine learning, that are utilized in the financial markets. The benefits of making AI algorithms more explainable and transparent are many—greater trust in algorithms' operations, greater accountability for harms resulting from algorithms' defect or misconduct, and reduction of intentional (or unintentional) use of algorithms to distort or manipulate the markets, among others.[233] If regulators only permitted explainable algorithms to operate in the markets, this would likely reduce the ability of wrongdoers to hide behind complexity and transparency when an algorithm harmed the market through manipulation or rational distortion. Yet, there are real costs that accompany explainable AI—costs which reduce the expected benefits of requiring greater transparency and explainability of algorithms.

First, algorithms that are built to be explained are less complex than those that are black boxes. Notably, the reduced complexity that increases the algorithm's transparency and explainability also decreases its reliability.[234] The decreased accuracy of explainable AI is concerning and would be a significant tradeoff in the quest to increase the transparency of algorithmic decisionmaking. Indeed, an explainable, yet less precise, AI algorithm is likely to increase volatility and distortion in the market. While the algorithms' outputs are more interpretable, in this instance, the market is not better off with the use of explainable AI versus black box machine-learning algorithms. Further, the algorithm's reduced reliability means that it also becomes a new source of risk, thereby increasing the potential market harm that may arise from algorithms. The pursuit of transparency and explainability, therefore, cannot be at the expense of accuracy and reliability of the algorithm's decisionmaking.

---

232. Deeks, *supra* note 227, at 1837.

233. *See* Finale Doshi-Velez & Been Kim, Towards a Rigorous Science of Interpretable Machine Learning 1–3 (Mar. 2, 2017) (unpublished manuscript), https://arxiv.org/pdf/1702.08608.pdf [https://perma.cc/ALR4-DM7J] ("[I]f the system can *explain* its reasoning, we then can verify whether that reasoning is sound with respect to . . . other desiderata—such as fairness, privacy, reliability, robustness, causality, usability and trust . . . .").

234. *See* Finale Doshi-Velez, Mason Kortz, Ryan Budish, Chris Bavitz, Sam Gershman, David O'Brien, Kate Scott, Stuart Shieber, James Waldo, David Weinberger, Adrian Weller & Alexandra Wood, Accountability of AI Under the Law: The Role of Explanation 3 (Dec. 20, 2019) (unpublished manuscript), https://arxiv.org/pdf/1711.01134.pdf [https://perma.cc/45FM-DEJZ] ("[E]xplanation would come at the price of system accuracy or other performance objectives.").

Second, explainable AI is costly to design and build.[235] It would cost programmers more time and money to build an explainable AI algorithm as opposed to one that is not transparent. Indeed, the expenses associated with explainable AI may stifle innovation, as algorithm developers may be disincentivized to develop algorithms that may be more efficient but less transparent.[236] Further, explainable AI may compel programmers to reveal trade secrets to enhance the transparency and explainability of the algorithm. This would only further disincentivize investment in the development of better and more efficient AI algorithms. In addition, there are regulatory costs associated with effectively overseeing explainable AI. For example, there would need to be some authority that determines whether the algorithm is sufficiently explainable to be allowed to operate in the markets. Thus, there would be costs to regulators to review, understand, and approve the algorithms. But, given the chronic shortfall of regulatory expertise and resources to keep pace with technology, it is questionable whether regulators would truly be in the position to undertake these costs.[237]

Third, in generating more information about the algorithm's decisionmaking, explainable AI may also create new risks. The more data is produced about an algorithm—its inputs, outputs, and inner workings—the more vulnerable the algorithm becomes to hacking or misuse.[238] For example, an AI algorithm developer attempting to make her algorithm more transparent may reveal information about its operations. Another programmer can use the same information to replicate the algorithm but for more malicious ends, such as market manipulation. Developing explainable AI algorithms, therefore, may have the perverse effect of making it easier for potential manipulators

---

235. *See* Cynthia Rudin, *Stop Explaining Black Box Machine Learning Models for High Stakes Decisions and Use Interpretable Models Instead*, 1 NATURE MACH. INTEL. 206, 210 (2019) (noting that domain expertise is needed to construct explainable AI and "many organizations do not have analysts who have the training or expertise to construct interpretable models at all"); *see also* Q. Vera Liao, Daniel Gruen & Sarah Miller, Questioning the AI: Informing Design Practices for Explainable AI User Experiences 7 (Feb. 8, 2020) (unpublished manuscript), https://arxiv.org/pdf/2001.02478.pdf [https://perma.cc/VQH5-95VX] (explaining that "inherent tension often exists between explainability and other system and business goals," including costs and resources involved in working with "data scientists, developers and other stakeholders" to make AI explainable).

236. Doshi-Velez et al., *supra* note 234, at 21 ("Requiring every AI system to explain every decision could result in less efficient systems, forced design choices, and a bias towards explainable but suboptimal outcomes.").

237. *See* Mirjana Stankovic, Nikola Neftenov & Bratislav Stankovic, *Can Regulators Keep Up with Emerging Technologies?*, MEDIUM (Mar. 10, 2020), https://medium.com/swlh/can-regulators-keep-up-with-emerging-technologies-c53448bcbd64 [https://perma.cc/8Y9W-LK75].

238. Andrew Burt, *The AI Transparency Paradox*, HARV. BUS. REV. (Dec. 13, 2019), https://hbr.org/2019/12/the-ai-transparency-paradox [https://perma.cc/KG9Y-PGUL].

to gain access to effective source code that, with adjustments, could be used to distort and manipulate the markets.

Fourth and finally, recent studies have called into question the reliability of explainable AI. Specifically, researchers have shown that some of the most promising techniques for explaining and interpreting the outputs of black box algorithms can themselves be manipulated.[239] According to the study, explainable AI can be exploited to provide innocuous ex post explanations for insidiously discriminatory behavior.[240] The ability to trick an explainable AI system into generating explanations that fail to see the AI algorithm's misconduct significantly undermines the utility of explainable AI to deter manipulation. Indeed, the possibility of misusing explainable AI in this way would exacerbate the problem of algorithm-related manipulation. To the extent the explanation provided for the distortion provides a defense for the manipulator's misconduct, it would be all the more difficult to hold her accountable for the harms the algorithm causes.

Increasing transparency and explainability, therefore, is laudable but not a panacea. Providing more data about how algorithms work will increase trust and accountability in the markets. Transparency, however, is accompanied by a set of risks that may undercut the expected benefits of greater explainability. From a policy standpoint, therefore, it is important to consider the ramifications of increased transparency to the broader goals of market efficiency, investor protection, and, ultimately, credibly deterring manipulation in the markets. To the extent greater transparency is sought as a means of reducing algorithm-related manipulation, it must be balanced against competing policy concerns and coupled with other mechanisms to emphasize certainty of punishment, thereby increasing deterrence.

B. Emphasizing Certainty

Certainty of punishment is key to deterring algorithm-related manipulation. To emphasize certainty, the scope and substance of the legal regime matters, including the detection, conviction, and imposition of meaningful sanctions on wrongdoers. The existing anti-manipulation framework fails to provide certainty of punishment because the law's requirements—which depend on scienter to determine liability—do not reflect the practicalities of algorithmic trading, in which scienter is often indeterminable. This Section

239. Dylan Slack, Sophie Hilgard, Emily Jia, Sameer Singh & Himabindu Lakkaraju, *Fooling LIME and SHAP: Adversarial Attack on Post Hoc Explanation Methods*, AIES '20, at 180, 182–85 (Feb. 7–8, 2020), https://dl.acm.org/doi/10.1145/3375627.3375830 [https://perma.cc/9QK5-JQJK].

240. *Id.* at 181.

considers a range of potential responses to increase certainty of punishment for algorithm-related market manipulation.

1. Focus on Harm, Not Intent

The focus on scienter is outdated for the modern, algorithm-dominated markets that now exist. And, importantly, this emphasis on intent hampers effective application of the legal regime to algorithm-related manipulation. To increase certainty of punishment for algorithm-related manipulation, this Article proposes minimizing or eliminating the focus on scienter and, instead, emphasizing the harm of the algorithm on the markets. A harm-based approach to manipulation would de-emphasize scienter, allowing regulators and private plaintiffs to pursue instances of algorithmic manipulation regardless of the provable mental state of the human connected to the algorithm. A focus on harm, in short, would emphasize the certainty of punishment for manipulative conduct and deny wrongdoers the defense that the algorithm was not carrying out their intent.

In other scholarship, the Author has proposed a harm-based approach to manipulation to supplement the intent-only liability standard for open-market manipulation.[241] Here in the context of algorithmic manipulation, however, this Article proposes eliminating intent from the equation altogether, focusing exclusively on the harm of the transaction to determine liability because of the innate difficulty of identifying scienter when algorithms are involved in trading. In identifying "harm," this Article proposes referring to the purposes underlying the anti-manipulation framework to determine whether a human ought to be liable for the misconduct of an algorithm. Thus, algorithmic conduct that decreases market efficiency or undercuts investor protection goals may be the basis for liability for manipulation, regardless of the programmer's provable intent.

By focusing on harm, this Article aims to treat transactions that have the same market impact similarly, rather than making distinctions on the vague and hard-to-prove basis of mental state. Consider: If an algorithm's trades create an artificial stock price, its conduct is no less impactful because the algorithm (or its programmer) lacked manipulative intent. Rather, the price's artificiality harms the pricing efficiency of the markets and impairs investor trust and confidence in the market. A harm-based approach, therefore, emphasizes the negative impact of algorithmic misconduct on the

241. Fletcher, *supra* note 8, at 519.

market rather than the provable scienter of the programmer, which would increase the deterrent effect of the legal framework.

To balance the potential chilling effect of the proposed harm-based approach that eschews scienter as a basis of liability, this Article proposes that if the algorithm's conduct is proven to be harmful to the market, this creates a rebuttable presumption of liability. Specifically, to the extent the trading algorithm impairs market efficiency or undermines investor protection, there should be a presumption of liability for manipulation. Once regulators or private plaintiffs are able to demonstrate that the algorithm's conduct harmed the market, as discussed below, the burden shifts to the defendant to provide evidence rebutting her presumed liability. The presumption of liability may be rebutted with a showing, for example, that the algorithm has worked appropriately in the past and has not been improperly adjusted or that the factors that caused the algorithm to distort the markets were unforeseeable to the programmer.

Importantly, the burden shift in this instance is key to increasing deterrence for two reasons. First, it eliminates the need for regulators to provide notoriously difficult evidence of manipulative intent and, instead, allows them to rely on proof of market harm. Second, the rebuttable presumption places the burden on programmers to justify the conduct of their algorithms. In sum, by alleviating the evidentiary burden on regulators to prove scienter, which is notoriously difficult to prove, the harm-based approach places the burden on the defendants to demonstrate why they should not be held accountable for the actions of their algorithms. This makes it less likely that would-be manipulators can evade punishment by hiding behind their algorithms' complexity. Rather, programmers would be required to demonstrate that the algorithm's misconduct was the product of negligence or unforeseeable circumstances.

Although proving that transactions harmed the market may be difficult, it would be easier to establish than the programmer's manipulative intent. Harm can be proven using objective, market-based evidence, historical data, and deep econometric analysis, among other factors.[242] It is susceptible to proof beyond factors and information outside the defendant's control. Intent, on the other hand, is subjective and rarely is there direct evidence of a defendant's intent to manipulate.[243] In the absence of such direct proof, plaintiffs and

242. *See id.* at 521–23 (discussing methods for determining artificial pricing).

243. *See* Fischel & Ross, *supra* note 23, at 519 ("[T]he difficulty of reading people's minds and thus the need to infer manipulative intent from actions are explicitly recognized as a problem in the area.").

regulators must rely on circumstantial evidence, inferring manipulative intent from factors such as volume, size, and timing of transactions. Many of these factors, however, are open to multiple interpretations, particularly when ex post justification is needed.[244] Focusing on the harm that arises from algorithmic trading to determine liability for manipulation, therefore, provides more certain punishment for misconduct, enhancing the deterrent effect of the legal framework.

2. Adopt a Recklessness Standard

An alternative to the elimination of scienter from the liability framework is to reduce the standard when applied to algorithm-related misconduct. Recall, price manipulation, open-market manipulation, and spoofing all require the plaintiff to demonstrate that the defendant intentionally manipulated the market; the fraud-based standard is met with a showing of recklessness.[245]

Instead of these varying, hard to prove bases of liability, the recklessness standard ought to be the highest scienter standard applicable to algorithm-related manipulation, regardless of the form of manipulation alleged. While not an easy standard, recklessness is a better fit for liability in algorithmic markets. Recall, under the recklessness standard, the plaintiff must demonstrate that the defendant's conduct was so far outside the scope of ordinary care that it is difficult to believe that the defendant did not know that what she was doing was wrong.[246] Key to liability under the recklessness standard is the standard of ordinary care, which many courts apply objectively.[247]

---

244. Fletcher, *supra* note 8, at 515–16 ("Yet, given the permissibility of traders' actions in cases of open-market manipulation, these factors are all subject to interpretation.").

245. *See supra* Section II.A (discussing the various scienter standards under the existing anti-manipulation regime).

246. *See* note 104 and accompanying text.

247. *See* Sundstrand Corp. v. Sun Chem. Corp., 553 F.2d 1033, 1045 (7th Cir. 1977):

> [R]eckless conduct may be defined as . . . highly unreasonable [conduct], involving not merely simple, or even inexcusable negligence, but an extreme departure from the standards of ordinary care, and which presents a danger of misleading buyers or sellers that is either known to the defendant or is so obvious that the actor must have been aware of it.

(quoting Franke v. Midwestern Okla. Dev. Auth., 428 F. Supp. 719, 725 (W.D. Okla. 1976)); *see also* McConville v. SEC, 465 F.3d 780, 788 (7th Cir. 2006) (holding that the defendant's conduct was such an extreme departure from the standards of ordinary care that it posed a danger to buyers and sellers); SEC v. Fife, 311 F.3d 1, 9 (1st Cir. 2002) (defining recklessness as a highly unreasonable omission); *In re* Silicon Graphics Inc. Sec. Litig., 183 F.3d 970, 977 (9th Cir. 1999) ("[R]ecklessness only satisfies scienter under § 10(b) to the extent that it reflects some degree of intentional or conscious misconduct . . . recklessness in the § 10(b) context is, in the words of the Supreme Court, a form of intentional conduct.").

With a recklessness standard, holding programmers liable for the misbehavior of their algorithms would turn less on whether the programmer intended the algorithm's actions and more on whether the programmer's conduct in designing, building, and testing the algorithm comported with objective standards of ordinary care. For example, private plaintiffs and regulators could hold the programmers of preset algorithms liable for manipulation by showing that the programmer failed to comply with industry norms or regulatory standards in creating and implementing the algorithm.

AI algorithms that learn to engage in manipulation or rational distortion, however, may be more difficult for the recklessness standard to address. On the one hand, if the AI algorithm evolves to manipulate the markets, the programmer's liability for the algorithm's independent misconduct may rest on whether she followed industry norms and standards in designing the algorithm. Even with AI algorithms, programmers should build in guardrails and other mechanisms to prevent the algorithm from engaging in independent misconduct. If she failed to do so, then she ought to be liable for the algorithm's unanticipated actions. On the other hand, if the algorithm's learning is the result of negligence, the recklessness standard would not be sufficient to hold the programmer liable. This would be a shortcoming of the recklessness standard, but some may view it as a necessary limitation if one believes that liability for manipulation ought to be based on deliberate misconduct, even if an algorithm is involved.

Nonetheless, reducing the scienter standard to recklessness for all manipulation enforcement actions involving an algorithm would ease the burden of proof applicable to regulators, making it more likely that they can hold programmers accountable for their conduct. The recklessness standard is also more applicable to the realities of algorithm-dominated markets. A potential wrongdoer may be able to plausibly deny intentionality with her algorithm's manipulative behavior; but, based on objective market and industry standards, it may be more difficult to credibly deny that her algorithm was designed within the standards of ordinary care. Essential to the efficacy of recklessness as a more applicable standard is the objectivity of the standard itself, which removes the subjective intent of the programmer from the equation. An objective standard, such as recklessness, enables regulators to more easily bring enforcement actions based on factors less susceptible to subjectivity, such as intent. Thus, lowering the standard to recklessness increases deterrence by enhancing the likelihood of punishment for manipulation.

3. Meaningful, Harmonized Regulatory Oversight

A final proposal to improve deterrence of the anti-manipulation framework is to bolster and harmonize regulatory oversight of algorithmic trading in the securities and commodities markets. Increasing the resources and expertise of both agencies would, undoubtedly, emphasize certainty of punishment against algorithm-related manipulation. But more can and ought to be done to enhance the enforcement capabilities of the primary financial market regulators. As discussed above, the SEC and the CFTC have vastly divergent oversight of algorithmic trading in their respective jurisdictions, which undermines deterrence because detection is decreased and punishment is inconsistent across markets.[248] Meaningful, harmonized regulatory oversight of the financial markets as a whole, therefore, would undoubtedly increase the credibility of the regime's deterrence.

Most obviously, the CFTC needs to adopt, at a minimum, a registration framework similar to that of the SEC for programmers and traders that utilize algorithms in their trading.[249] Imposing affirmative obligations on programmers to implement practices that reduce the likelihood of harm arising from their algorithms would improve the CFTC's mostly nonexistent oversight of algorithmic trading. Further, the CFTC should also require programmers to pass qualifying exams required of humans who trade in the commodities and derivatives markets. At minimum, these requirements will bring the CFTC's oversight of algorithmic trading in line with the SEC's and also provide the agency with greater oversight of the market's technological infrastructure. On the one hand, given the CFTC's failure to pass Reg AT, the agency may be reluctant to adopt such a framework. But, on the other hand, the rising importance of algorithmic trading in the commodities markets may push the CFTC to adopt these regulations to safeguard the markets' integrity and stability.

In addition to making the Commissions' supervision of algorithmic trading more harmonized, the Commissions should bolster their oversight and regulation of the market to improve their capacity to detect algorithm-related manipulation and hold wrongdoers accountable. In this regard, this Article has two potential suggestions.

First, the Commissions should require attestations from algorithm designers and users that the algorithm is not designed to

248. *See* discussion *supra* Sections III.C, III.D.

249. *See* Foley et al., *supra* note 195 (providing an overview of FINRA rules requiring registration of persons who oversee algorithmic securities trading).

violate applicable laws and regulations. Such attestations would be comparable to the requirements that a company's Chief Executive Officer and Chief Financial Officer attest that the company's annual and quarterly reports are accurate and complete.[250] In so certifying, these officers assert that, based on their knowledge, the reports are not misleading, fairly represent the financial condition of the company, and that they have personally reviewed the reports.[251] Importantly, false attestations violate Rule 10b-5 (among other provisions) and can provide the basis for establishing intentionality or recklessness to hold the officers liable.[252]

This Article proposes a similar attestation requirement in which programmers and users of algorithms attest that, based on their knowledge and review of the algorithm, it complies with securities and commodities laws, especially (for the purposes of this Article) the anti-manipulation regime. The attestation requirement would provide regulators with an initial basis to allege violation of anti-manipulation laws if a defendant's attestations later prove to be false. Indeed, the attestations could be used to prove the defendant's knowing violation of the laws, since she would be required to assert that she reviewed the code and it complied with laws.

Relatedly, these attestations could serve as a basis for vicarious liability. If an accused certifies that she is responsible for an algorithm's design and operation, then she ought to likewise be liable for the algorithm's misconduct. The attestations here legally bind the programmer to the algorithm in such a manner that she can be held accountable for its actions, even without proof of manipulative intent. By imposing this prerequisite to deploy algorithms in the market, the legal regime would ease enforcement actions by providing regulators with a mechanism to assign liability without the burden of scienter.

Notably, these attestations could render programmers liable for an algorithm's unforeseen misconduct that manipulates the market. Such extensive liability could have a chilling effect on the development of trading algorithms. But it could also make the deterrence regime more effective by forcing programmers to internalize the potential risk of harm their algorithms pose. Although holding programmers liable for

250. *See* Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, § 302, 116 Stat. 745, 777 (codified as amended at 15 U.S.C. § 7241) (requiring an issuer's principal executive and financial officers each to certify the financial and other information contained in the issuer's quarterly and annual reports).

251. *Id.*; *see also* Certification of Disclosure in Companies' Quarterly and Annual Reports, 67 Fed. Reg. 57,276 (Aug. 29, 2002) (to be codified at 17 C.F.R. pt. 228, 229, 232, 240, 249, 270, 274) (establishing rules as required by the Sarbanes-Oxley Act of 2002).

252. 17 C.F.R. § 240.10b-5(b) (2020) (making it unlawful "[t]o make any untrue statement of a material fact . . . in connection with the purchase or sale of any security").

the conduct of their AI may be seen as reasonable by some, others may view this as a bridge too far. Should lawmakers decide to adopt a harm-based approach to algorithmic manipulation, then these attestations would provide a basis for liability even for independent algorithmic misconduct. But if a recklessness approach is adopted instead, regulators could decide to exclude such unforeseen misconduct from the scope of the attestations, if the misconduct is the result of negligence. In the end, the scope of liability that may arise from these attestations will depend on the extent to which regulators and lawmakers seek to emphasize the certainty of punishment for algorithmic manipulation, including independent algorithmic misconduct.

Second, the Commissions ought to consider how and to what extent they want to incentivize explainable AI in the markets. Despite the shortcomings of explainable AI, it holds great promise for reducing the opacity of black box AI algorithms. Working alongside academics and industry participants, the Commissions ought to contemplate how explainable AI can be used to both help provide ex post justifications for harmful market conduct and aid in identifying manipulative behavior in the market. The promise of algorithms and similar technological advances is not only for traders hoping to be more profitable. There is great potential for regulators to utilize algorithms to help identify market misconduct faster and more effectively than before.[253]

Here, the CFTC's actions are promising. In 2017, the agency launched LabCFTC to promote its efforts to engage with financial technology innovators and facilitate its understanding of new technologies in the market.[254] A primary goal of the office is to identify interactions between the regulatory framework that could be improved in order to promote "responsible innovation."[255] Thus, the CFTC is proactively engaging with new technologies to enhance its own understanding and to accomplish its regulatory goals more effectively and efficiently. This type of dual engagement with new technologies is necessary for regulators to develop more robust understanding and oversight of new technologies, such as algorithmic trading and AI algorithms with machine learning techniques.

Undeniably, there are other ways in which the Commissions can improve their regulation of algorithms in the markets. These preliminary proposals, however, serve as a positive first step towards

253. *See* Douglas W. Arner, Jànos Barberis & Ross P. Buckley, *FinTech, RegTech, and the Reconceptualization of Financial Regulation*, 37 NW. J. INT'L L. & BUS. 371, 374–75 (2017) (arguing that regulation technology could make market supervision more effective).

254. COMMODITY FUTURES TRADING COMM'N, LABCFTC OVERVIEW, https://www.cftc.gov/LabCFTC/Overview/index.htm (last visited Oct. 3, 2020) [https://perma.cc/9LYT-56JA].

255. *Id.*

expanding oversight of algorithmic trading in such a way to credibly deter algorithm-related manipulation and meaningfully reduce the systemic risks that accompany it.

CONCLUSION

Preset and AI algorithmic trading programs will continue to play a major role in the financial markets for the foreseeable future. Therefore, it is increasingly necessary to consider the law's effectiveness in punishing manipulative conduct effectuated with these evolving technologies. Applying the anti-manipulation framework to algorithmic trading reveals a serious gap that undermines one of the framework's fundamental purposes: deterring market manipulation. This Article demonstrates the pervasive shortcomings of the manipulation framework in deterring algorithmic manipulation by explaining how the scienter requirement decreases the likelihood of punishment. The law's focus on scienter limits its applicability to algorithmic manipulation both because algorithms cannot form intent and because the difficulty in proving the intent of the programmer renders any enforcement for market manipulation uncertain and ineffective.

Importantly, the law's failure to deter algorithmic manipulation undermines market stability, exposing the market to a significant source of systemic risk. To address the mismatch between the realities of algorithmic trading and the requirements of the anti-manipulation regime, this Article highlights the benefits to be gained from embracing explainable and transparent algorithms but cautions against this being the only solution in achieving a credible deterrent framework. As such, this Article also suggests ways to modernize the anti-manipulation framework as applied to algorithmic trading and improve regulatory oversight of the market. Together, these suggestions would emphasize certainty of punishment and increase the likelihood of programmers being held accountable for the harm resulting from their algorithmic trading programs. By emphasizing certainty, this Article presents options to achieve credible deterrence of algorithmic manipulation, thereby allowing the law to remain effective in the face of technological evolution and, importantly, to promote market efficiency and investor protection.