# ARTIFICIAL INTELLIGENCE, FINANCE, AND THE LAW

*Tom C.W. Lin**

*Artificial intelligence is an existential component of modern finance. The progress and promise realized and presented by artificial intelligence in finance has been thus far remarkable. It has made finance cheaper, faster, larger, more accessible, more profitable, and more efficient in many ways. Yet for all the significant progress and promise made possible by financial artificial intelligence, it also presents serious risks and limitations.*

*This Article offers a study of those risks and limitations—the ways artificial intelligence and misunderstandings of it can harm and hinder law, finance, and society. It provides a broad examination of inherent and structural risks and limitations present in financial artificial intelligence, explains the implications posed by such dangers, and offers some recommendations for the road ahead. Specifically, it highlights the perils and pitfalls of artificial codes, data bias, virtual threats, and systemic risks relating to financial artificial intelligence. It also raises larger issues about the implications of financial artificial intelligence on financial cybersecurity, competition, and society in the near future. Ultimately, this Article aspires to share an insightful perspective for thinking anew about the wide-ranging effects at the intersection of artificial intelligence, finance, and the law with the hopes of creating better financial artificial intelligence—one that is less artificial, more intelligent, and ultimately more humane, and more human.*

## INTRODUCTION

Artificial intelligence is coming for our money.[1] The rise of artificial intelligence in finance and beyond has understandably garnered a great deal

* Professor of Law, Temple University Beasley School of Law. Many thanks to Tom Baker, Jonah Crane, Deborah Denno, and Robert Seamans for helpful comments and exchanges. Additionally, I am grateful to Anjali Deshpande and Matthew Sherman for their extraordinary research assistance. This Article was prepared for the Symposium entitled *Rise of the Machines: Artificial Intelligence, Robotics, and the Reprogramming of Law*, hosted by the *Fordham Law Review* and the Neuroscience and Law Center on February 15, 2019, at Fordham University School of Law. For an overview of the Symposium, see Deborah W. Denno & Ryan Surujnath, *Foreword: Rise of the Machines: Artificial Intelligence, Robotics, and the Reprogramming of Law*, 88 FORDHAM L. REV. 381 (2019).

1. *See generally* ARTIFICIAL INTELLIGENCE IN FINANCIAL MARKETS (Christian L. Dunis et al. eds., 2016).



Electronic copy available at: https://ssrn.com/abstract=3480607

of attention in recent years.[2] The progress and promise presented by artificial intelligence and related new technologies in finance and elsewhere in the economy has been remarkable, though much is yet to be realized.[3] We are just at the beginning of the beginning of the age of artificial intelligence. That said, in just the last few decades alone, we have witnessed significant advances in financial technology made possible in part by artificial intelligence in various aspects of the financial sector.[4] Previously, human-dominated financial efforts and endeavors have been eliminated, supplemented, or supplanted by artificial intelligence and smart machines.[5] Trading, financial research, risk analysis, wealth management, investment banking, and other areas of the financial sector have been dramatically changed by the rise of artificial intelligence.[6] Many of these advances and innovations have been profit-enhancing and socially beneficial. They have lowered the costs of capital for businesses and entrepreneurs, expanded the types of financial resources to a broader and more diverse population of

2. This growing attention and interest in artificial intelligence has led to a growing catalogue of books on the subject. *See, e.g.*, AJAY AGRAWAL ET AL., PREDICTION MACHINES: THE SIMPLE ECONOMICS OF ARTIFICIAL INTELLIGENCE (2018); PAUL R. DAUGHERTY & H. JAMES WILSON, HUMAN + MACHINE: REIMAGINING WORK IN THE AGE OF AI (2018); AMIR HUSAIN, THE SENTIENT MACHINE: THE COMING AGE OF ARTIFICIAL INTELLIGENCE (2017); KAI-FU LEE, AI SUPERPOWERS: CHINA, SILICON VALLEY, AND THE NEW WORLD ORDER (2018); THOMAS W. MALONE, SUPERMINDS: THE SURPRISING POWER OF PEOPLE AND COMPUTERS THINKING TOGETHER (2018).

3. *See* William Magnuson, *Regulating Fintech*, 71 VAND. L. REV. 1167, 1169 (2018) ("[T]he fintech revolution promises to produce great benefits for the wider economy, including broader access to capital, fairer lending standards, better investment advice, and more secure transactions."). *See generally* Thomas H. Davenport & Rajeev Ronanki, *Artificial Intelligence for the Real World*, HARV. BUS. REV., Jan.–Feb. 2018, at 108.

4. Douglas W. Arner et al., *FinTech, RegTech, and the Reconceptualization of Financial Regulation*, 37 NW. J. INT'L L. & BUS. 371, 377–81 (2017).

5. *See* Tom C.W. Lin, *The New Investor*, 60 UCLA L. REV. 678, 681–82 (2013) (introducing the concept of cyborg finance).

6. *See, e.g.*, Concept Release on Risk Controls and System Safeguards for Automated Trading Environments, 78 Fed. Reg. 56,542, 56,573 app. 2 (Sept. 12, 2013) (to be codified at 17 C.F.R. ch. 1) [hereinafter Concept Release] ("We have witnessed a fundamental shift in markets from human-based trading to highly automated electronic trading."); SCOTT PATTERSON, DARK POOLS: HIGH-SPEED TRADERS, AI BANDITS, AND THE THREAT TO THE GLOBAL FINANCIAL SYSTEM 322–23 (2012); Bradley Hope, *How Computers Trawl a Sea of Data for Stock Picks*, WALL ST. J. (Apr. 1, 2015, 10:30 PM), http://www.wsj.com/articles/how-computers-trawl-a-sea-of-data-for-stock-picks-1427941801 [https://perma.cc/37XK-BZ3U]; Sheelah Kolhatkar & Sree Vidya Bhaktavatsalam, *The Colossus of Wall Street*, BLOOMBERG (Dec. 9, 2010, 5:00 PM), https://www.bloomberg.com/news/articles/2010-12-09/the-colossus-of-wall-street [https://perma.cc/5WTE-YHCB]; Andrew Ross Sorkin, *Fintech Firms Are Taking On the Big Banks, but Can They Win?*, N.Y. TIMES (Apr. 7, 2016), https:// www.nytimes.com/2016/04/07/business/dealbook/fintech-firms-are-taking-on-the-big-banks-but-can-they-win.html [https://perma.cc/KR2V-ET7L]; Seth Stevenson, *The Wolf of Wall Tweet*, SLATE (Apr. 20, 2015, 4:12 PM), http://www.slate.com/articles/business/moneybox/2015/04/bot_makes_2_4_million_reading_twitter_meet_the_guy_it_cost_a_fortune.html?wpsrc=fol_tw. [https://perma.cc/8FCV-4AZ6]; John F. Wasik, *Sites to Manage Personal Wealth Gaining Ground*, N.Y. TIMES (Feb. 11, 2014), https://www.nytimes.com/2014/02/11/your-money/sites-to-manage-personal-wealth-gaining-ground.html [https://perma.cc/3KLY-PUJG].

Electronic copy available at: https://ssrn.com/abstract=3480607

investors, and made it easier for consumers to bank and invest.[7] Yet, for all the significant progress and promise presented by artificial intelligence in finance, it also presents serious pitfalls and perils.

This Article is about those risks and limitations—the ways artificial intelligence and misunderstandings of it can harm and hinder law, finance, and society. It provides a broad examination of inherent and structural risks and limitations present in financial artificial intelligence, explains the implications posed by each identified danger, and offers some recommendations for the road ahead. This Article does not seek to pinpoint every peril posed by financial artificial intelligence, as such an attempt would necessarily be incomplete and dated given the rapid changes in financial technology and their evolving ramifications. Rather, this Article aims to explore the larger penumbras of risks and limitations latent in financial artificial intelligence and how we can better confront them. In pursuit of these objectives, this Article hopes to provide another perspective for thinking about artificial intelligence and its wide-ranging impact on law, finance, and society.

Drawing on the author's prior writings and building upon a rich and growing body of interdisciplinary literature on artificial intelligence that spans law, finance, technology, and sociology, this Article proceeds in two major parts.[8] Part I provides an overview of critical risks and limitations. It describes four inherent areas of intertwined risks and limitations relating to programming codes, data bias, virtual threats, and systemic risks. It explains why and how each of these innate areas can harm and hinder the positive potential of artificial intelligence in finance. Pivoting from the intrinsic to the extrinsic, Part II contends with emerging ramifications and possible responses. It explores the challenges posed by financial artificial intelligence. Specifically, it focuses on implications relating to financial

7. *See, e.g.*, Joel Hasbrouck & Gideon Saar, *Low-Latency Trading*, 16 J. FIN. MKTS. 646, 648 (2013) (suggesting that high-frequency, smart machine trading has positive market-stabilizing effects); Charles R. Korsmo, *High-Frequency Trading: A Regulatory Strategy*, 48 U. RICH. L. REV. 523, 549–50 (2014) (discussing the benefits of high-frequency trading powered by artificial intelligence); Donald C. Langevoort & Robert B. Thompson, *"Publicness" in Contemporary Securities Regulation After the JOBS Act*, 101 GEO. L.J. 337, 347 (2013) ("Today, liquidity is now much more possible outside of traditional exchanges. In the new millennium, cheap information and low communication costs have expanded markets."). *See generally* Tom C.W. Lin, *Reasonable Investor(s)*, 95 B.U. L. REV. 461 (2015) (cataloguing the diversity of investors in modern finance).

8. *See, e.g.*, BRIAN CHRISTIAN, THE MOST HUMAN HUMAN: WHAT ARTIFICIAL INTELLIGENCE TEACHES US ABOUT BEING ALIVE 5–10 (2011); CATHY O'NEIL, WEAPONS OF MATH DESTRUCTION: HOW BIG DATA INCREASES INEQUALITY AND THREATENS DEMOCRACY 3 (2016); Derek E. Bambauer, *Ghost in the Network*, 162 U. PA. L. REV. 1011, 1050 (2014); Stephanie Bornstein, *Antidiscriminatory Algorithms*, 70 ALA. L. REV. 519, 522–23 (2018); Henry T. C. Hu, *Too Complex to Depict?: Innovation, "Pure Information," and the SEC Disclosure Paradigm*, 90 TEX. L. REV. 1601, 1608–12 (2012); Tom C.W. Lin, *The New Market Manipulation*, 66 EMORY L.J. 1253, 1287–93 (2017); Andrew W. Lo & Mark T. Mueller, *Warning: Physics Envy May Be Hazardous to Your Wealth!*, 8 J. INV. MGMT., no. 2, 2010, at 13, 21; Gregory Scopino, *Preparing Financial Regulation for the Second Machine Age: The Need for Oversight of Digital Intermediaries in the Futures Market*, 2015 COLUM. BUS. L. REV. 439, 518–19.

Electronic copy available at: https://ssrn.com/abstract=3480607

cybersecurity, competition, and societal impact in connection with the rise of artificial intelligence in finance. Finally, the Article concludes by looking forward to an incredibly promising future offered by financial artificial intelligence, while cautioning of looming perils that may accompany that incredible promise.

## I. RISKS AND LIMITATIONS

Despite the incredible progress and promise made possible by advances in financial artificial intelligence, it nevertheless presents some serious, interconnected risks and limitations.[9] Four categories of risks and limitations relating to programming codes, data bias, virtual threats, and systemic risks are particularly noteworthy. Individually and collectively, these four perilous areas loom large as potential inherent and structural dangers in connection with the rise of financial artificial intelligence.

### *A. Uncertain Markets and Artificial Codes*

Artificial intelligence programs are limited by their underlying code and their ability to fully and properly capture all that is happening in the marketplace. There are simply too many complex, ineffable human and other elements of financial markets and our uncertain world that cannot be fully or properly captured by artificial lines of codes, no matter how comprehensive or smart. As such, computer codes and models frequently make simplifying and oversimplifying assumptions about the workings of the marketplace that can make it appear that it is more predictive and productive than in reality.[10] As a result of these simplifications, financial artificial intelligence tools have the capacity to make powerful predictions and to produce incredible value that helps move and grow markets, but on the other hand, they also operate with potentially dangerous blind spots to the workings of the marketplace because of their limitations.[11]

The fantastical powers and applications of financial artificial intelligence have convinced many within the financial industry to naively believe that these smart machines are the fix for most of our human-created financial problems.[12] While such admiration and acclamation is understandable, it

9. Bernhard Babel et al., *Derisking Machine Learning and Artificial Intelligence*, MCKINSEY ON RISK, June 2019, at 35, 36–37.

10. *See, e.g.*, ROBERT J. SCHILLER, FINANCE AND THE GOOD SOCIETY 132–133 (2012) (warning of the attractiveness of elegant financial models); David H. Bailey et al., *Pseudo-Mathematics and Financial Charlatanism: The Effects of Backtest Overfitting on Out-of-Sample Performance*, 61 NOTICES AM. MATHEMATICAL SOC'Y 458, 458–59 (2014).

11. *See, e.g.*, AGRAWAL ET AL., *supra* note 2, at 3–11; JAMES OWEN WEATHERALL, THE PHYSICS OF WALL STREET: A BRIEF HISTORY OF PREDICTING THE UNPREDICTABLE 36–39 (2013); Lo, *supra* note 8, at 21; Paul Krugman, *How Did Economists Get It So Wrong?*, N.Y. TIMES MAG. (Sept. 2, 2009), https://www.nytimes.com/2009/09/06/magazine/06Economic-t.html [https://perma.cc/Z3YB-3G4H] ("[E]conomists, as a group, mistook beauty, clad in impressive-looking mathematics, for truth.").

12. EMANUEL DERMAN, MODELS. BEHAVING. BADLY.: WHY CONFUSING ILLUSION WITH REALITY CAN LEAD TO DISASTER, ON WALL STREET AND IN LIFE 143–87 (2011).

Electronic copy available at: https://ssrn.com/abstract=3480607

must also be balanced with proper recognition of the limitations of artificial intelligence at their underlying codes to perfectly depict and encapsulate the complexities of the financial marketplace and the world at large.[13] The 2008 financial crisis was caused and exacerbated in part by too many in the financial industry placing too much faith in smart machines to properly account for the risks and repercussions of a booming—then bursting—real estate market.[14] Uncertainty, risk, repercussions, and animal spirits in finance can never be perfectly coded, modeled, mitigated, or eliminated because human unpredictability is beyond precise mathematical modeling and computer coding.[15]

Furthermore, deal negotiations, board presentations, regulatory actions, legal interpretations, and many other activities critical to finance are done largely among humans communicating using verbal and nonverbal language in ways that smart machines are thus far unable to do on a consistent basis.[16] Despite all of its amazing advances, artificial intelligence still does not possess all of the capabilities of the human brain, with its trillions of synaptic connections and billions of neurons.[17] Artificial intelligence cannot fully decipher a simple common human phrase like "it's fine," let alone the many nonverbal expressions that humans use among one another.[18]

In sum, financial artificial intelligence is limited by the incapability of its programming to fully capture the breadth, depth, and diversity of all that is happening in a marketplace. This is due in large part to the whimsical, flawed, and unpredictable role humans continue to play in finance and markets.[19] Therefore, as we grow more reliant and assured about the promise

13. Hu, *supra* note 8, at 1608–12.

14. *See, e.g.*, ANTHONY SAUNDERS & LINDA ALLEN, CREDIT RISK MANAGEMENT IN AND OUT OF THE FINANCIAL CRISES: NEW APPROACHES TO VALUE AT RISK AND OTHER PARADIGMS 31 (2010); Amir E. Khandani & Andrew W. Lo, *What Happened to the Quants in August 2007?*, J. INV. MGMT., 2007, at 5, 5–9; Krugman, *supra* note 11 ("There was nothing in the prevailing models suggesting the possibility of the kind of collapse that happened last year."); Joe Nocera, *Risk Management*, N.Y. TIMES MAG. (Jan. 4, 2009), https://www.nytimes.com/2009/01/04/magazine/04risk-t.html [https://perma.cc/A5VL-QFHE] (criticizing the flawed computer risk models in connection with the 2008 financial crisis).

15. *See, e.g.*, JEROME FRANK, LAW AND THE MODERN MIND 129 (2009) ("The law is not a machine and the judges not machine-tenders. There never was and there never will be a body of fixed and predetermined rules alike for all."); FRANK H. KNIGHT, RISK, UNCERTAINTY, AND PROFIT 347 (1921); Lo, *supra* note 8, at 14.

16. *See, e.g.*, CHRISTIAN, *supra* note 8, at 5–10.

17. *See* ELLEN E. PASTORINO & SUSANN M. DOYLE-PORTILLO, WHAT IS PSYCHOLOGY? 355 (2012); *see also* Cade Metz, *$1 Billion in Hand, A.I. Lab Wants to Mimic the Brain*, N.Y. TIMES (July 23, 2019), https://www.nytimes.com/2019/07/22/technology/open-ai-microsoft.html [https://perma.cc/9GCN-CVKD]; Cade Metz, *DeepMind Can Now Beat Us at Multiplayer Games, Too*, N.Y. TIMES (June 3, 2019), https://www.nytimes.com/2019/05/30/science/deep-mind-artificial-intelligence.html [https://perma.cc/6257-G3QD].

18. *See* HARRY T. REIS & SUSAN SPRECHER, ENCYCLOPEDIA OF HUMAN RELATIONSHIPS 249 (2009) (describing the importance of nonverbal communication in human interactions). To be fair to the machines, many humans have difficulties deciphering the meaning of the phrase, "it's fine," depending on the context.

19. *See* FRANK, *supra* note 15, at 129 ("The acts of human beings are not identical mathematical entities; the individual cannot be eliminated as, in algebraic equations, equal quantities on the two sides can be cancelled."); WEATHERALL, *supra* note 11, at 36–39; Lo,

Electronic copy available at: https://ssrn.com/abstract=3480607

of financial artificial intelligence, we should also grow more mindful of its limited capacity to fully comprehend the ineffable complexities of a still largely human-driven marketplace.

### *B. Discriminatory Data and Algorithmic Biases*

Discriminatory data and algorithmic bias represent a set of critical risks and limitations associated with financial artificial intelligence. They concern the integrity and utilization of the underlying informational inputs that are the fuel of artificial intelligence systems.[20] Most artificial intelligence systems initially need large quantities of data to teach the programs to recognize certain patterns and make certain predictions. At its best, artificial intelligence can uncover valuable new insights and observations from troves of big data, otherwise impossible without artificial intelligence's awesome processing powers.[21] At its worst, artificial intelligence can exacerbate misguided old practices and aggravate past social harms with its incredible processing powers and the veneer of novel objectivity since discriminatory humans are associated with the decisions.[22] While we should appreciate the incredible potential of financial artificial intelligence, we should also be cognizant of the potential risks inherent in systems built with data that may reflect harmful past biases against the marginalized and the poor that we do not want to replicate in the present or perpetuate in the future.[23] We should be particularly mindful of underlying data contexts and applications that are being selected and coded by flawed humans with all of our biases, prejudices, and fallacies.[24]

First, we should be mindful of the context of the data in order to properly account for potential latent biases. When, where, why, and how was this trove of data generated? Understanding the context of the data is critical to understanding the data, its utility, and its potential risks. Inputting data without properly understanding its context could lead to dangerous discriminatory implications.[25] As a crude example, if one obtusely inputs

*supra* note 8, at 21; Mark Whitehouse, *Economists' Grail: A Post-Crash Model*, WALL ST. J. (Nov. 30, 2010, 12:01 AM), https://www.wsj.com/articles/SB10001424052702303891804575576523458637864 [https://perma.cc/26HF-NTMZ] (reporting on the dangerous limitations of financial models).

20. O'NEIL, *supra* note 8, at 3.

21. *See* Sonia K. Katyal, *Private Accountability in the Age of Artificial Intelligence*, 66 UCLA L. REV. 54, 59 (2019) ("At first glance, because data collection has now become ubiquitous, the benefits of algorithmic decisionmaking often seem to outweigh their costs. And this is mostly right."); *see also* PEDRO DOMINGOS, THE MASTER ALGORITHM: HOW THE QUEST FOR THE ULTIMATE LEARNING MACHINE WILL REMAKE OUR WORLD 1–3 (2015) (discussing the benefits of algorithmic decision-making).

22. *See* O'NEIL, *supra* note 8, at 3.

23. VIRGINIA EUBANKS, AUTOMATING INEQUALITY: HOW HIGH-TECH TOOLS PROFILE, POLICE, AND PUNISH THE POOR 6–10 (2018).

24. *See* O'NEIL, *supra* note 8, at 3 ("The math-powered applications powering the data economy were based on choices made by fallible human beings.").

25. *See* Bornstein, *supra* note 8, at 522–23 ("If the underlying data on which an algorithm relies is itself biased, incomplete, or discriminatory, the decisions it makes have the potential to reproduce inequality on a massive scale.").

Electronic copy available at: https://ssrn.com/abstract=3480607

white-collar professional labor data from the 1940s to the 1970s into an artificial intelligence system to predict what demographics of individuals would be the most successful applicants for white-collar professions, the suggestion would likely be white males of a certain age. This is not because the algorithm or code is intentionally pernicious; rather, it is because the underlying data is reflective and reproductive of certain harmful discriminatory practices and (mis)understandings of a bygone era.[26] As such, if the context of the data is not properly accounted for, it can lead to innovative technologies that perpetuate old, harmful ways—directly or indirectly via proxy.[27] Given the long history of discriminatory practices in the financial industry, adopters of financial artificial intelligence must be particularly mindful of the historical context of the data that they input into their smart systems so as not to bring forth past biases into the present and the future.[28]

Second, in addition to being more mindful of the context of the data, we should also be more thoughtful about the application of the data by artificial intelligence so as to mitigate potential algorithmic biases.[29] Artificial intelligence, as well as its underlying data and code at their most basic level, is amoral, neither immoral nor virtuous. It lacks values and judgments. We imbue these smart machines with the values and judgments that we believe are important, however good or ill the intentions.[30] Humans, with all of their foibles and faults, design these systems.[31] As such, society cannot simply accept the outputs of artificially intelligent systems without due consideration and understanding of their implications. For example, financial artificial intelligence may recommend that veterans and certain minority populations should be charged higher interest rates on loans without ever considering the social and moral ramifications of such recommendations. Because of the importance of finance in the lives and livelihoods of people, it is critical that programmers, designers, architects, and consumers of financial artificial intelligence systems properly account

26. SAFIYA UMOJA NOBLE, ALGORITHMS OF OPPRESSION: HOW SEARCH ENGINES REINFORCE RACISM 151–52 (2018).

27. *See, e.g.*, Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 4–5 (2014); Katyal, *supra* note 21, at 68–77. *See generally* Pauline T. Kim, *Data-Driven Discrimination at Work*, 58 WM. & MARY L. REV. 857 (2017); Darcy Steeg Morris, Daniel Schwarcz & Joshua Teitelbaum, *Do Credit-Based Insurance Scores Proxy for Income in Predicting Auto Claim Risk?*, 14 J. EMPIRICAL LEGAL STUD. 397 (2017).

28. *See generally* MEHRSA BARADARAN, THE COLOR OF MONEY: BLACK BANKS AND THE RACIAL WEALTH GAP (2017); RICHARD ROTHSTEIN, THE COLOR OF LAW: A FORGOTTEN HISTORY OF HOW OUR GOVERNMENT SEGREGATED AMERICA (2017).

29. *See generally* Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 PROC. MACHINE LEARNING RES. 77 (2018).

30. *See* O'NEIL, *supra* note 8, at 3 ("[M]any of these models encoded human prejudice, misunderstanding, and bias into the software systems that increasingly manage our lives.").

31. *See* Katyal, *supra* note 21, at 59 ("While algorithmic decisionmaking may initially seem more reliable because it appears free from the irrational biases of human judgment and prejudice, algorithmic models are also the product of their fallible creators, who may miss evidence of systemic bias or structural discrimination in data or may simply make mistakes.").

Electronic copy available at: https://ssrn.com/abstract=3480607

for the pernicious ways that such systems can be used and misused and must include humans as safeguards in critical decision points.[32]

In sum, data and algorithmic bias represent one of the key categories of risks and limitations inherent in the rise of financial artificial intelligence. As the financial industry grows more reliant on artificial intelligence, policymakers, regulators, and other key stakeholders must also grow more vigilant about the potential harms that could arise out of data and algorithmic bias. In recent years, there have been significant and serious movements to combat algorithmic bias in finance and beyond.[33] Ultimately, it is important that new technology does not bring forth old discriminations into the present and the future under the blended gloss of innovation, neutrality, and objectivity.[34]

### *C. Virtual Threats and Cyber Conflicts*

Another key category of risks and limitations associated with the rise of financial artificial intelligence involves the rise of virtual threats and cyber conflicts in the financial system. The emergence of financial artificial intelligence is an extension of the growing reliance on technology in the financial industry, and this burgeoning reliance has made the financial industry ever more vulnerable to virtual threats. In 2019, IBM found that the finance and insurance industry was the most attacked industry in terms of cybersecurity threats.[35] As the financial industry evolves even more into a high-tech industry, it will surely face even more of the same types of cyber challenges confronted by most traditional technology companies.[36]

The virtual threats against the financial industry can be both external and internal. First, in terms of external virtual threats, financial firms and financial industry regulators must be particularly vigilant against foreign

32. MICHAEL CHUI ET AL., MCKINSEY GLOB. INST., NOTES FROM THE AI FRONTIER: APPLYING AI FOR THE SOCIAL GOOD 41 (2018), https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/Artificial%20Intelligence/Applying%20artificial%20intelligence%20for%20social%20good/MGI-Applying-AI-for-social-good-Discussion-paper-Dec-2018.ashx [https://perma.cc/KT3S-LXHT].

33. *See, e.g.*, ALGORITHMIC JUST. LEAGUE, https://www.ajlunited.org [https://perma.cc/W9XJ-LZT9] (last visited Oct. 6, 2019).

34. *See* Kim, *supra* note 27, at 877 ("Data models may also discriminate when neutral factors act as 'proxies' for sensitive characteristics like race or sex. Those neutral factors may be highly correlated with membership in a protected class, and also correlate with outcomes of interest. In such a situation, those neutral factors may produce results that systematically disadvantage protected groups, even though the model's creators have no discriminatory intent, and the sensitive characteristics have been removed from the data.").

35. IBM, X-FORCE THREAT INTELLIGENCE INDEX 4 (2019), https://www.securindex.com/downloads/8b9f94c46a70c60b229b04609c07acff.pdf [https://perma.cc/3MDS-4TJW].

36. *See* Duncan B. Hollis, *Why States Need an International Law for Information Operations*, 11 LEWIS & CLARK L. REV. 1023, 1042 (2007) (speculating about computer viruses that target stock markets); *see also* Scott Patterson, *CME Was the Victim of 'Cyberintrusion' in July*, WALL ST. J. (Nov. 15, 2013), https://www.wsj.com/articles/cme-says-it-was-victim-of-8216cyber-intrusion8217-in-july-1384543426 [https://perma.cc/3VSY-N7S7]; Michael Riley & Ashlee Vance, *Cyber Weapons: The New Arms Race*, BLOOMBERG BUSINESSWEEK (July 21, 2011), https://www.bloomberg.com/news/articles/2011-07-20/cyber-weapons-the-new-arms-race [https://perma.cc/6677-VTMM].

Electronic copy available at: https://ssrn.com/abstract=3480607

nation-states, competitors, terrorist organizations, cybercriminals, and cybermercenaries.[37] In the last decade alone, the financial industry has had to confront a diverse matrix of external threats from state and nonstate actors, some seeking profit while others seeking merely to sow chaos using sophisticated hacks designed to steal billions of dollars, acquire valuable information, and cause significant disruptions.[38]

Second, in addition to the external threats, financial firms and regulators also have to guard against internal threats, such as rogue employees, corporate spies, and misguided contractors.[39] IBM in recent years has

37. *See, e.g.*, MARK BOWDEN, WORM: THE FIRST DIGITAL WORLD WAR 48 (2011) ("Today the most serious computer predators are funded by rich criminal syndicates and even nation-states, and their goals are far more ambitious."); SHANE HARRIS, @WAR: THE RISE OF THE MILITARY-INTERNET COMPLEX 103–22 (2014) (discussing the market for cybermercenaries); INTELLIGENCE & NAT'L SEC. ALL., CYBER INTELLIGENCE: SETTING THE LANDSCAPE FOR AN EMERGING DISCIPLINE 7–9 (2011), https://www.insaonline.org/wp-content/uploads/2017/04/INSA_CyberIntel_WP.pdf [https://perma.cc/6PG4-WHW2]; SCOTT PATTERSON, THE QUANTS: HOW A NEW BREED OF MATH WHIZZES CONQUERED WALL STREET AND NEARLY DESTROYED IT 107–16 (2010) (discussing the theft of trade secrets from hedge funds); U.S. DEP'T OF DEF., THE DEPARTMENT OF DEFENSE CYBER STRATEGY 9 (2015), https://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf [https://perma.cc/N9F8-PXNM] ("Criminal actors pose a considerable threat in cyberspace, particularly to financial institutions, and ideological groups often use hackers to further their political objectives."); Eric Talbot Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense*, 38 STAN. J. INT'L L. 207, 232 (2002) (alluding to the difficulties of identifying a wide cast of potential cyber attackers); Matthew Goldstein, *Need Some Espionage Done?: Hackers Are for Hire Online*, N.Y. TIMES (Jan. 15, 2015), https://dealbook.nytimes.com/2015/01/15/need-some-espionage-done-hackers-are-for-hire-online [https://perma.cc/ST23-63N7]; Michael Joseph Gross, *Silent War*, VANITY FAIR (June 6, 2013), https://www.vanityfair.com/news/2013/07/new-cyberwar-victims-american-business [https://perma.cc/86RN-L6V7]; Nicole Perlroth, *Hunting for Syrian Hackers' Chain of Command*, N.Y. TIMES (May 17, 2013), https://www.nytimes.com/2013/05/18/technology/financial-times-site-is-hacked.html [https://perma.cc/3D2U-852F] (reporting on the difficulties of tracing hackers); Nathaniel Popper, *Wall Street's Exposure to Hacking Laid Bare*, N.Y. TIMES: DEALBOOK (July 25, 2013), https://dealbook.nytimes.com/2013/07/25/wall-streets-exposure-to-hacking-laid-bare [https://perma.cc/UL9C-JJYB].

38. *See, e.g.*, FIREEYE, APT28: A WINDOW INTO RUSSIA'S CYBER ESPIONAGE OPERATIONS? 3–6 (2014), https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf [https://perma.cc/X7BT-TCJB]; BARRY VENGERIK ET AL., FIREEYE, HACKING THE STREET?: FIN4 LIKELY PLAYING THE MARKET 3 (2014), https://www.fireeye.com/current-threats/threat-intelligence-reports/rpt-fin4.html [https://perma.cc/B5UV-WV33]; Megha Bahree, *Former Bangladesh Bank Chief Blames Global System for Theft*, N.Y. TIMES (June 22, 2016), https://www.nytimes.com/2016/06/23/business/dealbook/former-bangladesh-bank-chief-blames-others.html [https://perma.cc/C2N6-DBHZ]; Nicole Perlroth & Quentin Hardy, *Bank Hacking Was the Work of Iranians, Officials Say*, N.Y. TIMES (Jan. 8, 2013), https://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html [https://perma.cc/GE4L-SBMH]; Michael Riley, *How Russian Hackers Stole the Nasdaq*, BLOOMBERG BUSINESSWEEK (July 21, 2014), https://www.bloomberg.com/news/articles/2014-07-17/how-russian-hackers-stole-the-nasdaq [https://perma.cc/S6S9-SJ44]; Nelson D. Schwartz, *Facing Threat from WikiLeaks, Bank Plays Defense*, N.Y. TIMES (Jan. 2, 2011), https://www.nytimes.com/2011/01/03/business/03wikileaks-bank.html [https://perma.cc/N3U6-9WLH].

39. *See, e.g.*, Bambauer, *supra* note 8, at 1050 ("[I]t is not technologically possible to prevent those authorized to access data from misusing it . . . ."); Steven R. Chabinsky,

Electronic copy available at: https://ssrn.com/abstract=3480607

estimated that human errors account for a very significant percentage of all data and cybersecurity breaches.[40] While such internal threats have always existed within the financial industry, the industry's heavy reliance on technology like artificial intelligence has magnified the impact of such internal threats. In a financial marketplace where millions of dollars can automatically move in fractions of a second with or without a keystroke, the rogue internal threat may be one of the most dangerous menaces to the financial industry.[41]

Furthermore, both internal and external virtual threats have grown more sophisticated and complex to detect and thwart.[42] In the coming years, with the rise of financial artificial intelligence, market regulators and participants may have to confront unprecedented threats in the marketplace. Financial deepfakes, financial fake news, and many other previously unimagined ways to disrupt and manipulate the markets will persist and grow in a marketplace that becomes ever more reliant on technologies like artificial intelligence.[43] In 2016, then-Federal Reserve Chair Janet Yellen ominously testified before Congress that cyberattacks on the financial system present "one of the most significant risks our country faces."[44]

In the last few years alone, hackers injected false data into the U.S. Securities and Exchange Commission's EDGAR electronic filing system and hacked social media accounts to manipulate the stock market.[45] For instance, in 2013, cybercriminals hacked the Associated Press's Twitter account to falsely report an attack on the White House, which momentarily caused a $136 billion loss in market value when programs driven by artificial

*Cybersecurity Strategy: A Primer for Policy Makers and Those on the Front Line*, 4 J. NAT'L SECURITY L. & POL'Y 27, 34–35 (2010); Robin Sidel, *Banks Battle Staffers' Vulnerability to Hacks*, WALL ST. J. (Dec. 20, 2015, 5:30 AM), http://www.wsj.com/articles/the-weakest-link-in-banks-fight-against-hackers-1450607401 [https://perma.cc/C9A5-KZ5B].

40. *See* IBM, *supra* note 35, at 7–8; IBM GLOB. TECH. SERVS., IBM SECURITY SERVICES 2014 CYBER SECURITY INTELLIGENCE INDEX 3 (2014), http://media.scmagazine.com/documents/82/ibm_cyber_security_intelligenc_20450.pdf [https://perma.cc/6EKB-6R8G] (finding that 95 percent of data breaches are the result of human error).

41. Dune Lawrence, *Companies Are Tracking Employees to Nab Traitors*, BLOOMBERG BUSINESSWEEK (Mar. 16, 2015), https://www.bloomberg.com/news/articles/2015-03-12/companies-are-tracking-employees-to-nab-traitors [https://perma.cc/PQS8-LDQH].

42. *See, e.g.*, Sealed Indictment, United States v. Murgio, 15 Cr. 769 (S.D.N.Y. Nov. 5, 2015), ECF No. 14; Sealed Indictment, United States v. Shalon, 15 Cr. 333 (S.D.N.Y. June 2, 2015), ECF No. 3; Bahree, *supra* note 38; Matthew Goldstein & Alexandra Stevenson, *Nine Charged in Insider Trading Case Tied to Hackers*, N.Y. TIMES (Aug. 11, 2015), https://www.nytimes.com/2015/08/12/business/dealbook/insider-trading-sec-hacking-case.html [https://perma.cc/9ZEQ-R9A6].

43. Lin, *supra* note 8, at 1287–94.

44. Chiara Albanese, Daniele Lepido & Giles Turner, *"Anonymous" Joins Hacker Army Targeting Central Banks for Cash*, BLOOMBERG (Mar. 17, 2017, 4:33 AM), https://www.bloomberg.com/news/articles/2017-03-17/-anonymous-joins-hacker-army-targeting-central-banks-for-cash [https://perma.cc/42PE-3XTN].

45. *See, e.g.*, Amy Chozick & Nicole Perlroth, *Twitter Speaks, Markets Listen and Fears Rise*, N.Y. TIMES (Apr. 28, 2013), https://www.nytimes.com/2013/04/29/business/media/social-medias-effects-on-markets-concern-regulators.html [https://perma.cc/L8RP-YMZP]; Goldstein, *supra* note 37.

Electronic copy available at: https://ssrn.com/abstract=3480607

intelligence traded on the bogus news.[46] Such innovative, pernicious threats will continue to increase as finance becomes more reliant on automated systems powered by artificial intelligence that may be particularly susceptible to bad or false data as nation-states and nonstate actors try to weaponize technological tools like artificial intelligence that have made so much progress in the financial system possible against the system itself.[47]

In sum, as the financial industry becomes more like the technology industry, with its greater adoption of artificial intelligence, it will face growing and serious risks concerning virtual and other technology-oriented threats.

### *D. Systemic Risks and Financial Accidents*

The rise of financial artificial intelligence and related financial technology heightens the dangers of systemic risk and major financial accidents.[48] A growing reliance on artificial intelligence and other forms of technology in the financial industry can exacerbate intertwined systemic risks related to size, speed, and interconnectivity. Moreover, the growing complexity of technology increases the risks of serious financial accidents.

Wider adoption of financial artificial intelligence can amplify certain systemic risks for the financial system relating to size, speed, and linkage. First, in terms of size, there exists the well-known systemic risk of "too big to fail," whereby large financial institutions supposedly become too large and important to the welfare of the system to falter or fail.[49] As financial artificial intelligence gains more ground in the financial industry, institutions that are critical to the system because of their large data holdings for the purpose of financial artificial intelligence could also become too important to the system to fail. As such, in the future, the systemic risk of size may mean not only the size of a financial institution's balance sheet but also the size of its databases.

Second, in terms of speed, wider adoption of financial artificial intelligence would likely lead to even faster financial speeds, which would create a systemic risk of "too fast to save," whereby disruptions, bad acts, and other events could destabilize the financial system before any corrective

46. Chozick & Perlroth, *supra* note 45.

47. *See* LEE, *supra* note 2, at 82–86 (discussing the competition between the United States and China in the area of artificial intelligence); BRAD SMITH & CAROLE ANN BROWNE, TOOLS AND WEAPONS: THE PROMISE AND THE PERIL OF THE DIGITAL AGE 69–76 (2019).

48. *See* Magnuson, *supra* note 3, at 1199 (arguing that new financial technologies can create and complicate systemic risks).

49. *See* S. PERMANENT SUBCOMM. ON INVESTIGATIONS, COMM. ON HOMELAND SEC. & GOVERNMENTAL AFFAIRS, WALL STREET AND THE FINANCIAL CRISIS: ANATOMY OF A FINANCIAL COLLAPSE, S. HRG. 112-675, at 19–22 (1st Sess. 2011) (studying the regulatory challenges of "too big to fail"); ANDREW ROSS SORKIN, TOO BIG TO FAIL: THE INSIDE STORY OF HOW WALL STREET AND WASHINGTON FOUGHT TO SAVE THE FINANCIAL SYSTEM FROM CRISIS—AND THEMSELVES 538–39 (2009) (discussing the systemic risk associated with "too big to fail" institutions).

Electronic copy available at: https://ssrn.com/abstract=3480607

or preventive measure could be taken.[50] During times and trading periods of distress, panic, and confusion, high-speed automated programs running on artificial intelligence can sow greater volatility and calamity by rapidly increasing or decreasing liquidity.[51] In the last few decades alone, we have seen unprecedented volatility and flash crashes in the financial markets, made possible by new technology like artificial intelligence.[52]

Third, in terms of linkage, the prevalence of financial artificial intelligence could intensify the systemic risk of "too linked to fail," whereby actions, errors, and failings trigger destabilizing ripples across the financial system because of the interconnectivity of firms, regardless of their value or size.[53] This systemic risk is particularly troubling because of the highly intermediated and interconnected nature of modern finance and the use of similar and interdependent artificial intelligence programs by many firms within the financial industry.[54] As a consequence of these tight links and interoperative programs, one or a few firms can create dangerous cycles and cascades of volatility and spillover effects that destabilize the entire financial system.[55]

---

50. *See* Andrei A. Kirilenko & Andrew W. Lo, *Moore's Law Versus Murphy's Law: Algorithmic Trading and Its Discontents*, J. ECON. PERSP., Spring 2013, at 51, 60; Lin, *supra* note 5, at 711–14 ("[A]utomated trading systems provide enormous economies of scale and scope in managing large portfolios, but trading errors can now accumulate losses at the speed of light before they're discovered and corrected by human oversight.").

51. FRANK PARTNOY, WAIT: THE ART AND SCIENCE OF DELAY 43 (2012).

52. *See, e.g.*, CFTC & SEC, FINDINGS REGARDING THE MARKET EVENTS OF MAY 6, 2010, at 1 (2010), https://www.sec.gov/news/studies/2010/marketevents-report.pdf [https://perma.cc/34T5-VF5T]; Timothy Lavin, *Monsters in the Market*, ATLANTIC (July/Aug. 2010), https://www.theatlantic.com/magazine/archive/2010/07/monsters-in-the-market/308122 [https://perma.cc/EL84-ALZD]. *See generally* U.S. DEP'T OF TREASURY ET AL., JOINT STAFF REPORT: THE U.S. TREASURY MARKET ON OCTOBER 15, 2014 (2015), http://www.treasury.gov/press-center/press-releases/Documents/Joint_Staff_Report_Treasury_10-15-2015.pdf [https://perma.cc/FZ5Q-PQWE].

53. *See, e.g.*, Lin, *supra* note 5, at 714–16 (introducing the concept of "too linked to fail"); Steven L. Schwarcz, *Systemic Risk*, 97 GEO. L.J. 193, 200 (2008) (discussing the systemic risks associated with financial intermediation).

54. *See* Markus K. Brunnermeier, *Deciphering the Liquidity and Credit Crunch 2007–2008*, J. ECON. PERSP., Winter 2009, at 77, 96–97 (describing the financial system's "interwoven network of financial obligations"); Tom C.W. Lin, *Infinite Financial Intermediation*, 50 WAKE FOREST L. REV. 643, 661 (2015) (explicating on the highly intermediated nature of modern finance). *See generally* HAL S. SCOTT, COMM. ON CAPITAL MKTS. REGULATION, INTERCONNECTEDNESS AND CONTAGION (2012), http://www.capmktsreg.org/wp-content/uploads/2014/11/2012.11.20_Interconnectedness_and_Contagion.pdf [https://perma.cc/45V4-MGZL].

55. *See* BRIAN R. BROWN, CHASING THE SAME SIGNALS: HOW BLACK-BOX TRADING INFLUENCES STOCK MARKETS FROM WALL STREET TO SHANGHAI 7 (2010); PATTERSON, *supra* note 6, at 9–10 (discussing the financial dangers of "a vicious self-reinforcing feedback loop"); Louise Story & Graham Bowley, *Market Swings Are Becoming New Standard*, N.Y. TIMES (Sept. 11, 2011), https://www.nytimes.com/2011/09/12/business/economy/stock-markets-sharp-swings-grow-more-frequent.html [https://perma.cc/MVN8-ZC6U]; James Surowiecki, *New Ways to Crash the Market*, NEW YORKER (May 11, 2015), https://www.newyorker.com/magazine/2015/05/18/new-ways-to-crash-the-market [https://perma.cc/S4SS-FKJM] ("High-speed firms tend to mimic one another's trading strategies, and in times of crisis this can amplify price swings."). *See generally* Chris Brummer & Yesha Yadav, *Fintech and the Innovation Trilemma*, 107 GEO. L.J. 235 (2019).

Electronic copy available at: https://ssrn.com/abstract=3480607

In addition to the rise of financial artificial intelligence that exacerbates systemic risk, its ascent could also lead to financial accidents. Charles Perrow, in his landmark study on technological risks *Normal Accidents: Living with High-Risk Technologies*, theorized that complex technology systems, like the artificial intelligence–driven ones that are at the heart of our financial system, are inherently vulnerable to breakdowns and accidents.[56] As financial artificial intelligence grows more prevalent, "normal financial accidents" will likely also grow more frequent within the financial system.[57] In fact, both the New York Stock Exchange and the Nasdaq, the two most prominent American stock exchanges, suffered serious malfunctions that halted hundreds of billions of dollars worth of trading for hours during otherwise normal trading sessions in recent years.[58]

In sum, the proliferation of artificial intelligence in finance increases the dangers of systemic risks and major financial accidents. While we should appreciate the many new positive outgrowths of financial artificial intelligence for certain firms and institutions, we should also be mindful of the hazards and challenges that it may cause for the entire financial system going forward.[59]

## II. KEY IMPLICATIONS AND RECOMMENDATIONS

The proliferation of financial artificial intelligence will have many profound implications on finance, law, and society. While the specific and wider effects of financial artificial intelligence remain forthcoming, three particular areas are worthy of closer near-term consideration and action: financial cybersecurity, competition, and societal impact.

### *A. On Financial Cybersecurity*

One of the most significant issues and challenges arising from the wider adoption of financial artificial intelligence is financial cybersecurity. Today, many of the more sophisticated attempts to manipulate and disrupt financial

56. *See* CHARLES PERROW, NORMAL ACCIDENTS: LIVING WITH HIGH-RISK TECHNOLOGIES 4–5 (1999).

57. Marc Schneiberg & Tim Bartley, *Regulating or Redesigning Finance?: Market Architectures, Normal Accidents, and Dilemmas of Regulatory Reform*, *in* MARKETS ON TRIAL: THE ECONOMIC SOCIOLOGY OF THE FINANCIAL CRISIS 279, 284–89 (Michael Lounsbury & Paul M. Hirsch eds., 2010).

58. *See* E. S. Browning & Scott Patterson, *Market Size + Complex Systems = More Glitches*, WALL ST. J. (Aug. 22, 2013, 10:49 PM), https://www.wsj.com/articles/SB10001424127887323980604579029342001534148 [https://perma.cc/5W6H-Y4Z7]; Nathaniel Popper, *Pricing Problem Suspends Nasdaq for Three Hours*, N.Y. TIMES: DEALBOOK (Aug. 22, 2013), https://dealbook.nytimes.com/2013/08/22/nasdaq-market-halts-trading [https:// perma.cc/9U9Q-KW3Z]; Nathaniel Popper, *The Stock Market Bell Rings, Computers Fail, Wall Street Cringes*, N.Y. TIMES (July 8, 2015), https://www.nytimes.com/2015/07/09/business/dealbook/new-york-stock-exchange-suspends-trading.html [https://perma.cc/76TB-XCTN].

59. *See, e.g.*, Korsmo, *supra* note 7, at 549–50 (listing the benefits relating to algorithmic trading); Langevoort & Thompson, *supra* note 7, at 347 (discussing how new financial technologies have increased liquidity and lowered transactional costs for many in the marketplace).

Electronic copy available at: https://ssrn.com/abstract=3480607

markets take place exclusively in cyberspace and are aimed at artificial intelligence systems.[60] Because financial artificial intelligence relies on interconnected, complex technological systems, being able to safeguard those systems from threats and attacks is critical to preserving the integrity of the financial system.[61]

One of the critical challenges concerning financial cybersecurity is that disparate private parties, who may have misaligned and competing interests, control much of the global cyberinfrastructure.[62] As such, private firms motivated by higher profits, competitive advantage, expense reductions, and other understandable considerations may not always act with systemic financial cybersecurity as a top priority in their decision-making.[63] For instance, many financial firms already spend substantial sums of money annually on regulatory compliance and cybersecurity efforts and may be reluctant to spend more on a timely basis going forward.[64] That said, sound systemic financial cybersecurity requires all or most firms to have strong cybersecurity capabilities. It is not nearly enough for just a few firms to have strong cybersecurity safeguards while their counterparties and vendors are vulnerable, given the interconnected nature of the modern financial system. As such, public policymakers need to think creatively to incentivize private firms around the world to innovate faster and cooperate better with other firms and public regulators as the specter of cybersecurity attacks grows larger with advances in financial artificial intelligence.[65]

---

60. Lin, *supra* note 8, at 1287–93.

61. *See, e.g.*, PATTERSON, *supra* note 6, at 8–10; Tom C.W. Lin, *Financial Weapons of War*, 100 MINN. L. REV. 1377, 1405–08 (2016) (discussing the threats of "cyber financial weapons").

62. *See* Kristen E. Eichensehr, *The Cyber-Law of Nations*, 103 GEO. L.J. 317, 350–51 (2015) ("[P]rivate parties own the majority of the underlying infrastructure that supports the cyber domain.").

63. *See, e.g.*, STEWART BAKER ET AL., MCAFEE, IN THE CROSSFIRE: CRITICAL INFRASTRUCTURE IN THE AGE OF CYBER WAR 14 (2010), https://www.govexec.com/pdfs/012810j1.pdf [https://perma.cc/BP3N-Q8LL]; N.Y. STATE DEP'T OF FIN. SERVS., REPORT ON CYBER SECURITY IN THE BANKING SECTOR 11 (2014), https://www.dfs.ny.gov/docs/reportpub/cyber/dfs_cyber_banking_report_052014.pdf [https://perma.cc/74SR-YL58] (reporting on resource constraints and stale software as persistent financial cybersecurity challenges); Bambauer, *supra* note 8, at 1036 ("Rational vendors will accordingly skimp on security investments, at least at the margins, since they will likely not be able to recover those costs via higher prices that correlate with higher quality.").

64. Tom C.W. Lin, *Compliance, Technology, and Modern Finance*, 11 BROOK. J. CORP. FIN. & COM. L. 159, 164–68, 177–78 (2016).

65. *See, e.g.*, HARRIS, *supra* note 37, at xxii ("Defending computer networks, and launching attacks on them, requires the participation, willing or otherwise, of the private sector."); Nathan Alexander Sales, *Regulating Cyber-Security*, 107 NW. U. L. REV. 1503, 1550–52 (2013) (discussing the use of both incentives and punishments to improve cybersecurity); Bruce P. Smith, *Hacking, Poaching, and Counterattacking: Digital Counterstrikes and the Contours of Self-Help*, 1 J.L. ECON. & POL'Y 171, 173 (2005); Christopher S. Yoo, *Cyber Espionage or Cyberwar?: International Law, Domestic Law, and Self-Protective Measures*, *in* CYBERWAR: LAW & ETHICS FOR VIRTUAL CONFLICTS 175, 192–93 (Jens David Ohlin, Kevin Govern & Claire Finkelstein eds., 2015) (discussing the need for "improved software engineering").

Electronic copy available at: https://ssrn.com/abstract=3480607

Ultimately, sound and sustainable financial cybersecurity requires smart leadership and partnership from both the public and private sectors.[66] As then-President Barack Obama remarked in 2015 about cybersecurity, "neither government, nor the private sector can defend the nation alone. It's going to have to be a shared mission—government and industry working hand in hand, as partners."[67] In the absence of such coordinated action, the integrity of the financial system could come into question as institutions and investors lose trust and faith in the stability and reliability of the financial system.[68] This is particularly true with the rise of financial artificial intelligence because of its heavy reliance on electronic networks and computerized systems for its operations. Furthermore, many financial artificial intelligence systems are "black box" systems, meaning that their operations are difficult or impossible to fully understand, explain, or audit.[69]

In sum, wider adoption of financial artificial intelligence will have serious ramifications on the cybersecurity and integrity of the global financial marketplace. Private and public institutions throughout the world must act with greater speed and coordination to guard against the looming threats of cyberattacks, manipulation, and other bad acts that strike at the heart of the modern, high-tech financial system.[70] It should be noted that while such urgency may be clear and present, it does not necessarily mean that such urgency would manifest in swift and smart policies and actions given various geopolitical complexities involved in a vexing issue like financial cybersecurity.[71]

### *B. On Competition*

The rise of financial artificial intelligence will have significant implications for competition within the financial industry and the greater economy. Because artificial intelligence is highly dependent on large data sets for insights, firms with captive, large sets of data built into their structural platforms may end up having a durable competitive advantage in the marketplace that ultimately hurts consumer welfare and the competitive landscape of finance.[72] The ongoing debates and investigations concerning

66. Kristen E. Eichensehr, *Public-Private Cybersecurity*, 95 TEX. L. REV. 467, 469–72 (2017).

67. Press Release, Barack Obama, U.S. President, Remarks by the President at the National Cybersecurity Communications Integration Center (Jan. 13, 2015), https://obamawhitehouse.archives.gov/the-press-office/2015/01/13/remarks-president-national-cybersecurity-communications-integration-cent [https://perma.cc/XMR5-N2MB].

68. *See* BAKER ET AL., *supra* note 63, at 14; Scopino, *supra* note 8, at 518–19 (arguing for greater regulatory attention on "digital intermediaries" in finance).

69. *See* FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION 4–6 (2015); Andrew D. Selbst & Solon Barocas, *The Intuitive Appeal of Explainable Machines*, 87 FORDHAM L. REV. 1085, 1089–96 (2018).

70. *See, e.g.*, Bambauer, *supra* note 8, at 1062–63; Scopino, *supra* note 8, at 518–19.

71. *See* Eichensehr, *supra* note 66, at 507–11 (identifying various challenges arising from public-private actions on cybersecurity).

72. *See, e.g.*, Lina M. Khan, *Amazon's Antitrust Paradox*, 126 YALE L.J. 710, 784–88 (2017) (discussing how online platforms "may facilitate anticompetitive conduct and structures").

Electronic copy available at: https://ssrn.com/abstract=3480607

competition and antitrust among large technology companies like Google, Amazon, and Facebook may soon spill over into the financial industry with large financial institutions, which are functionally large technology companies similarly powered by large troves of data.[73] In recent years, large financial institutions like JPMorgan Chase have reportedly hired more software developers and technologists than Google or Microsoft.[74]

Technological innovations and advances have been dramatically changing the financial industry.[75] The ascent of financial artificial intelligence is an important extension of this ongoing sea change. New financial technology and artificial intelligence have transformed many segments of modern finance. In trading, smart machines powered by artificial intelligence now trade most securities in global finance, often doing so better, cheaper, and faster than their human counterparts.[76] In risk management, many, if not most, large financial institutions use financial artificial intelligence programs to aid them in managing risk.[77] BlackRock, the world's largest asset management company, with trillions of dollars under management, uses Aladdin, a proprietary artificial intelligence program to manage risk for its clients. Most significant financial institutions use artificial intelligence

73. *See, e.g.*, Cecilia Kang et al., *Tech Titans Face Tough Scrutiny*, N.Y. TIMES (June 3, 2019), https://www.nytimes.com/2019/06/03/technology/facebook-ftc-antitrust.html [https://perma.cc/D3XM-9848]; Jack Nicas et al., *How Each Big Tech Company May Be Targeted by Regulators*, N.Y. TIMES (Sept. 8, 2019), https://www.nytimes.com/2019/09/08/technology/antitrust-amazon-apple-facebook-google.html [https://perma.cc/PA37-VG8D].

74. CA TECHS., HOW TO SURVIVE AND THRIVE IN THE APPLICATION ECONOMY 2 (2014), https://www.ca.com/content/dam/ca/us/files/product-brief/how-to-survive-and-thrive-in-the-application-economy.pdf [https://perma.cc/5VNH-T22T].

75. *See, e.g.*, DAVID J. LEINWEBER, NERDS ON WALL STREET: MATH, MACHINES, AND WIRED MARKETS 31–63 (2009) (charting the growth of electronic financial markets); Jonathan R. Macey & Maureen O'Hara, *From Markets to Venues: Securities Regulation in an Evolving World*, 58 STAN. L. REV. 563, 563 (2005) ("Advances in technology, combined with the dramatic decrease in the cost of information processing, have conspired to change the way that securities transactions occur."); Saule T. Omarova, *Wall Street as Community of Fate: Toward Financial Industry Self-Regulation*, 159 U. PA. L. REV. 411, 430 (2011) (highlighting how finance has changed due in large part to "fast-changing technology"); Scopino, *supra* note 8, at 445–52 (explaining the impact of new financial technology on financial markets); Felix Salmon & Jon Stokes, *Algorithms Take Control of Wall Street*, WIRED (Dec. 27, 2010, 12:00 PM), https://www.wired.com/2010/12/ff-ai-flashtrading [https://perma.cc/98CP-UEY2] ("It's the machines' market now; we just trade in it.").

76. *See* Yesha Yadav, *How Algorithmic Trading Undermines Efficiency in Capital Markets*, 68 VAND. L. REV. 1607, 1618 (2015) ("The growth of algorithmic trading over the years can be explained by the significant utilities it offers for almost all parts of the trading process."); Nathaniel Popper, *Public Exchanges Duel with Newcomers over Trade Transparency*, N.Y. TIMES (June 26, 2012), https://www.nytimes.com/2012/06/27/business/stock-exchanges-duel-with-newcomers-over-trade-transparency.html [https://perma.cc/KL9K-BT2W]; Nelson D. Schwartz & Louise Story, *Surge of Computer Selling After Apparent Glitch Sends Stocks Plunging*, N.Y. TIMES (May 6, 2010), https://www.nytimes.com/2010/05/07/business/economy/07trade.html [https://perma.cc/8WWJ-PBU4].

77. *See* Kolhatkar & Bhaktavatsalam, *supra* note 6; *The Rise of BlackRock*, ECONOMIST (Dec. 7, 2013), https://www.economist.com/news/leaders/21591174-25-years-blackrock-has-become-worlds-biggest-investor-its-dominance-problem [https://perma.cc/WVZ3-TY9F].

Electronic copy available at: https://ssrn.com/abstract=3480607

programs in their financial research efforts as well.[78] For instance, such programs can be coded to analyze market trends, read breaking news, and spot investment opportunities entirely on their own.[79] Finally, in wealth management, artificial intelligence programs can manage funds just as well as many financial advisors—at a fraction of the cost. New financial technology companies, like Wealthfront and Betterment, use artificial intelligence programs to advise and manage billions of dollars of assets for clients at lower costs with comparable returns, all from an app on one's phone.[80]

While all of the aforementioned innovations and advances made possible by artificial intelligence have created many benefits, they also raise legitimate concerns about competition in ways historically unconsidered or underappreciated by banking and antitrust regulators.[81] Because the technology and data underlying much of financial artificial intelligence requires significant investments and favors the data-rich, there is appropriate concern that early movers and better-resourced institutions would acquire durable competitive advantages that ultimately stifle innovation, eliminate meaningful competition, and harm consumer welfare.[82] It is not difficult to foresee a financial firm acquiring and leveraging its superior data in terms of quality and quantity, as well as concentrated network effects, to build an economic moat to shield itself from competition in the same manner as its more traditional technology-oriented counterparts.[83] Similar to current concerns relating to the domination of Google, Amazon, and Facebook in their respective technological territories in search, online commerce, and social media, there is good reason to believe that some large, dominant financial institutions may warrant similar scrutiny with the rise of financial artificial intelligence in the coming years.[84] Whereas federal and state regulars are currently focused on large, traditional technology companies for their anticompetitive practices and implications, in the near future such regulators may turn a similar investigatory gaze on financial institutions given the rise of financial artificial intelligence and its implications for competition within the financial industry.[85]

78. *See, e.g.*, Hope, *supra* note 6.

79. *See, e.g.*, PATTERSON, *supra* note 6, at 322–23; Stevenson, *supra* note 6.

80. Wasik, *supra* note 6.

81. Rory Van Loo, *Making Innovation More Competitive: The Case of Fintech*, 65 UCLA L. REV. 232, 261–64 (2018).

82. Khan, *supra* note 72, at 784–88.

83. *See, e.g.*, OECD, DATA-DRIVEN INNOVATION: BIG DATA FOR GROWTH AND WELL-BEING 1, 7 (2015) (discussing the data as key ingredient to economic and business growth in the modern economy); Michal S. Gal & Niva Elkin-Koren, *Algorithmic Consumers*, 30 HARV. J.L. & TECH. 309, 334–35 (2017) ("Digital markets suffer from a high level of concentration. Currently a handful of digital intermediaries with mega platforms control effective points of access to potential users.").

84. *See, e.g.*, TIM WU, THE CURSE OF BIGNESS 122–26 (2018) (highlighting the anticompetitive implications of giant technology companies).

85. *See* Steve Lohr, *New Google and Facebook Show Big Tech Scrutiny Is Rare Bipartisan Act*, N.Y. TIMES (Sept. 6, 2019), https://www.nytimes.com/2019/09/06/technology/attorney-generals-tech-antitrust-investigation.html [https://perma.cc/NPG5-

Electronic copy available at: https://ssrn.com/abstract=3480607

Therefore, as artificial intelligence becomes more common in finance, policymakers must grow more watchful, thoughtful, and action-oriented about the potential implications it may have for competition within the industry and beyond.[86]

### *C. On Societal Impact*

The rise of financial artificial intelligence will likely have a profound societal and economic impact on an individual as well as a collective basis.[87] On an individual basis, the rise of artificial intelligence in finance raises important questions about the role of humans in finance. On a collective basis, the ascent of financial artificial intelligence also raises important questions about the role and purpose of finance in society.

First, on an individual basis, financial artificial intelligence has profound implications for people working in finance, just as similar ramifications are unfolding in other sectors of our economy.[88] Artificial intelligence has gradually—then rapidly—displaced much human labor and effort in finance, and understandably so.[89] Smart machines driven by artificial intelligence with perfect memory and recall can process large volumes of data faster, cheaper, and more accurately than humans in most circumstances, and they do not tire with more work or grow irrational with "animal spirits" the way humans normally do.[90] It is worth noting that while artificial intelligence has reduced and eliminated many jobs in finance and beyond, it has also produced new jobs, some of which are highly desirable and others that are

MT67] (reporting on federal and state investigations into the anticompetitive practices of large technology companies).

86. *See* Kahn, *supra* note 72, at 797–800 (arguing for more antitrust action against online platforms).

87. *See generally* THE ECONOMICS OF ARTIFICIAL INTELLIGENCE: AN AGENDA (Ajay Agrawal et al. eds., 2019).

88. *See* JAMES BARRAT, OUR FINAL INVENTION: ARTIFICIAL INTELLIGENCE AND THE END OF THE HUMAN ERA 3–4 (2013); MARTIN FORD, RISE OF ROBOTS: TECHNOLOGY AND THE THREAT OF A JOBLESS FUTURE 83–87 (2015); JOHN MARKOFF, MACHINES OF LOVING GRACE: THE QUEST FOR COMMON GROUND BETWEEN HUMANS AND ROBOTS 327 (2015).

89. *See, e.g.*, Concept Release, *supra* note 6, at 56,573 app. 2 ("We have witnessed a fundamental shift in markets from human-based trading to highly automated electronic trading."); ERIK BRYNJOLFSSON & ANDREW MCAFEE, THE SECOND MACHINE AGE: WORK, PROGRESS, AND PROSPERITY IN A TIME OF BRILLIANT TECHNOLOGIES 57–71 (2014); FORD, *supra* note 88, at 6–28 (examining the rise of robotics and automation across multiple industries within the economy); SHERRY TURKLE, ALONE TOGETHER: WHY WE EXPECT MORE FROM TECHNOLOGY AND LESS FROM EACH OTHER 279–81 (2011); Lin, *supra* note 5, at 682 (discussing the rise of smart financial machines); Daron Acemoglu & Pascual Restrepo, *Artificial Intelligence, Automation, and Work* (Nat'l Bureau of Econ. Research, Working Paper No. 24196, 2018), https://www.nber.org/papers/w24196 [https://perma.cc/K48V-22KA].

90. *See* NICK BOSTROM, SUPERINTELLIGENCE: PATHS, DANGERS, STRATEGIES 11 (2014); David Silver et al., *Mastering the Game of Go with Deep Neural Networks and Tree Search*, 529 NATURE 484, 484 (2016). *See generally* GEORGE A. AKERLOF & ROBERT J. SHILLER, ANIMAL SPIRITS: HOW HUMAN PSYCHOLOGY DRIVES THE ECONOMY, AND WHY IT MATTERS FOR GLOBAL CAPITALISM (2009).

Electronic copy available at: https://ssrn.com/abstract=3480607

less so.[91] Despite the undeniable and impressive rise of financial artificial intelligence, humans will likely remain the critical players in modern finance (for now) because of their judgment and sophistication, especially as it relates to other humans.[92] More importantly, human engagement that touches on emotions, ethics, values, empathy, culture, and other basic human traits remains critical to the success and failure of any financial endeavor. Smart machines, although artificially intelligent, still need humans to build their initial codes and hardware as well as embed them with human values and ethics.[93] Moreover, humans can nevertheless override their smart machines in many situations. As such, in many circumstances, artificial intelligence is often outmatched by natural stupidity or natural brilliance. Ultimately, on an individual basis, financial artificial intelligence will become an even more critical technological ally for humans in finance and not their adversary. This will be the case for both government financial regulators and those they regulate.[94] The important questions in the face of these rapid technological changes in finance and beyond are less about what artificial intelligence is going to do to humans; rather, they are more about what humans are going to do with artificial intelligence going forward to make one another even better and more powerful.[95]

Second, on a collective basis, financial artificial intelligence implicates significant questions about the proper role of finance in society. As finance continues to adopt new technologies like artificial intelligence, it can sometimes lose sight of the fact that finance at its core—behind and beyond all the high-tech gadgetries, complex codes, and seas of data—is driven by real people and real social purposes.[96] Faster, cheaper, bigger, and more efficient finance does not necessarily mean a more just and socially valuable form of finance.[97] Frequently in discussing matters of finance, scholars, regulators, and policymakers forget that people and communities are at the

91. *See* MARY L. GRAY, GHOST WORK: HOW TO STOP SILICON VALLEY FROM BUILDING A NEW GLOBAL UNDERCLASS, at x–xvii (2019); H. James Wilson et al., *The Jobs That Artificial Intelligence Will Create*, MIT SLOAN MGMT. REV., Summer 2017, at 14, 14–16.

92. *See* STEPHEN BAKER, FINAL JEOPARDY: MAN VS. MACHINE AND THE QUEST TO KNOW EVERYTHING 148–69 (2011) (discussing the various limitations of artificial intelligence).

93. *See, e.g.*, High-Level Expert Grp. on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI* (Apr. 8, 2019) (EU), https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419 [https://perma.cc/Q3B7-AE6E] (discussing principles for developing better artificial intelligence systems).

94. *See* Arner et al., *supra* note 4, at 102–04; Cary Coglianese & David Lehr, *Regulating by Robot: Administrative Decision Making in the Machine-Learning Era*, 105 GEO. L.J. 1147, 1152–54 (2017) (discussing the use of machine-learning algorithms in government regulatory actions).

95. *See, e.g.*, BENJAMIN ALARIE ET AL., REGULATION BY MACHINE 1–2 (2016); DAUGHERTY & WILSON, *supra* note 2, at 138–43; MALONE, *supra* note 2, at 50–56; Kevin Roose, *A Machine May Not Take Your Job, but One Could Become Your Boss*, N.Y. TIMES (June 23, 2019), https://www.nytimes.com/2019/06/23/technology/artificial-intelligence-ai-workplace.html [https://perma.cc/KT2L-NGHC].

96. *See* FELIX MARTIN, MONEY: THE UNAUTHORISED BIOGRAPHY 27–29 (2014) (alluding to money as a social technology); KABIR SEHGAL, COINED: THE RICH LIFE OF MONEY AND HOW ITS HISTORY HAS SHAPED US 2–3 (2015) (discussing the social role of money).

97. PASQUALE, *supra* note 69, at 102–04.

Electronic copy available at: https://ssrn.com/abstract=3480607

heart of finance and markets.[98] People create supply and demand. People move markets. It is flesh and blood people who need finance and financing for education, homes, health care, investments, and other life and social pursuits.[99] Finance is ultimately a tool of social utility and connection that would lose much of its meaning without the context of people and society.[100]

One of the critical responsibilities for executives, policymakers, and regulators in the years ahead centers on how better to update a twentieth-century financial system to account for twenty-first-century financial advances like artificial intelligence without losing focus on the human-oriented missions of finance and democratic values like equal access and transparency.[101] Doing so will not be easy given the serious challenges of modern politics, old narratives, and scarce resources.[102] Furthermore, the objectives of regulating new financial technology can often be crosscutting, whereby achieving one objective like greater transparency could undercut other objectives like efficiency and fairness.[103] That said, properly recognizing the human heart of finance is key to better understanding and harnessing the power of financial artificial intelligence for positive monetary and social impact, while taming its hostilities.[104] To legislate, regulate, innovate, and act on finance divorced from its human participants, beneficiaries, and victims—while theoretically elegant—can lead to serious negative consequences.[105] In fact, as noted earlier, in the run up to the financial crisis of 2008, too many regulators and firms placed too much faith in the elegant models of smart machines and lost focus on the real-world implications of finance and markets to the detriment of society.[106]

In sum, as finance grows more reliant on new technologies like artificial intelligence, key financial stakeholders must grow more vigilant in safeguarding the people-centered, social purposes of finance.[107]

---

98. MIHIR DESAI, THE WISDOM OF FINANCE: DISCOVERING HUMANITY IN THE WORLD OF RISK AND RETURN 1 (2017).

99. *See id.* ("We see finance everywhere, from our retirement assets to our investments in housing and education.").

100. *See* YOCHAI BENKLER, THE WEALTH OF NETWORKS: HOW SOCIAL PRODUCTION TRANSFORMS MARKETS AND FREEDOM 174–75 (2006); SCHILLER, *supra* note 10, at 8–9.

101. *See, e.g.*, Ryan Calo, *Artificial Intelligence Policy: A Primer and Roadmap*, 51 U.C. DAVIS L. REV. 399, 411 (2017).

102. *See, e.g.*, Tom C.W. Lin, *The New Financial Industry*, 65 ALA. L. REV. 567, 593–95 (2014) (discussing some of the challenges to meaningful financial regulation).

103. *See, e.g.*, Brummer & Yadav, *supra* note 55, at 244 (theorizing on the trilemma of fintech regulation relating to the objectives of "(i) market integrity; (ii) rules simplicity; and (iii) financial innovation").

104. *See, e.g.*, MEREDITH BROUSSARD, ARTIFICIAL UNINTELLIGENCE: HOW COMPUTERS MISUNDERSTAND THE WORLD 177–78 (2018) (discussing the need for "human-centered design" in connection with artificial intelligence).

105. Van Loo, *supra* note 81, at 248–55, 267–69.

106. *See* Khandani & Lo, *supra* note 14, at 5–9; Krugman, *supra* note 14 ("There was nothing in the prevailing models suggesting the possibility of the kind of collapse that happened last year.").

107. *See* PASQUALE, *supra* note 69, at 141–42, 186–87 (proposing various policies and practices to better harness the benefits of artificial intelligence systems towards positive social ends while minimizing ruinous consequences).

Electronic copy available at: https://ssrn.com/abstract=3480607

## CONCLUSION

The rise and growth of artificial intelligence in finance and beyond will likely be one of the most significant developments for law, finance, and society in the coming years and decades. The early movements offer glimpses of the awesome powers and potential of financial artificial intelligence. Nevertheless, as financial artificial intelligence continues to grow and evolve, we must also become more aware of its potential risks and limitations. We must grow more cognizant of the ways financial artificial intelligence can harm and hinder individual as well as societal progress.

This Article broadly highlights some of the critical risks and limitations of financial artificial intelligence while being largely appreciative of its incredible potential applications. Specifically, it sheds light on the perils and pitfalls of artificial codes, data bias, virtual threats, and systemic risks relating to financial artificial intelligence. It also raises broader issues about the implications of financial artificial intelligence on financial cybersecurity, competition, and society in the near future. This Article aims to offer an insightful perspective for thinking anew about the wide-ranging effects at the intersection of artificial intelligence, finance, and the law with the hope of creating better financial artificial intelligence. In the end, one of the most daunting and consequential endeavors for executives, policymakers, scholars, and other stakeholders working in law and finance going forward is to create better financial artificial intelligence—one that is less artificial, more intelligent, and ultimately more humane, and more human.

Electronic copy available at: https://ssrn.com/abstract=3480607