Brooklyn Journal of Corporate, Financial & Commercial Law

Volume 11
Issue 1 *SYMPOSIUM: The Role of Technology in Compliance in Financial Services: An Indispensable Tool as well as a Threat?*

Article 6

12-1-2016

Compliance, Technology, and Modern Finance

Tom C.W. Lin

COMPLIANCE, TECHNOLOGY, AND MODERN FINANCE

Tom C.W. Lin[*]

ABSTRACT

An important transformation is happening in the financial industry. The rise of new technology and compliance has dramatically altered many of the key functions and functionaries of modern finance. Artificial intelligence, algorithmic programs, and supercomputers, instead of human actors, now constitute the core of many financial operations. At the same time, compliance officers have become just as critical to financial institutions as traders, bankers, and analysts. Finance as we knew it has changed and continues to change.

This symposium Article offers a studied commentary on these unfolding changes, the crosscutting developments in compliance, technology, and modern finance. It examines the concurrent and intersecting ascents of new financial technology and compliance as well as the potential perils linked with their ascents. It also highlights the larger implications of the changing landscape of finance associated with the growing roles of new technology and compliance. In particular, it focuses on the challenges of financial cybersecurity, the integration of technology and compliance, and the role of humans in the future of modern finance. In sum, this Article hopes to serve as a thoughtful account for thinking anew about the future of compliance, technology, and modern finance.

INTRODUCTION

The financial industry is undergoing an important transformation. The rise of new technology and compliance has changed many of the key functions and functionaries of modern finance. Artificial intelligence, algorithmic programs, and supercomputers, instead of human actors, now constitute the core of many financial operations.[1] At the same time, compliance officers have become just as critical to financial institutions as

---

* Associate Professor of Law, Temple University Beasley School of Law. Many thanks to Mercer Bullard, James Fanto, Jonathan Gottlieb, Sean Griffith, Robert Leonard, Jennifer Pacella, Arthur Pinto, H.J. Wilcox, and participants at the 2016 Brooklyn Journal of Corporate, Financial, and Commercial Law Annual Symposium for helpful comments and exchanges. Additionally, I am grateful to Leslie Minora and George Tsoflias for their extraordinary research assistance.

1. *See* Merritt B. Fox et al., *The New Stock Market: Sense and Nonsense*, 65 DUKE L.J. 191, 199–201 (2015) (attributing changes in the stock market to "the information-technology revolution"); 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, 223–24 (2015) ("Now, almost all parts of the financial markets, including the markets for futures and other derivatives, are computerized and automated to some extent, from the exchanges to the traders."); Tom C.W. Lin, *National Pastime(s)*, 55 B.C. L. REV. 1197, 1207–09 (2014) (discussing the rising adoption of artificial intelligence in finance).

traders, bankers, and analysts.[2] Finance as we knew it has changed and continues to change.

This Article is about those changes, the crosscutting developments in compliance, technology, and modern finance. This Article has two primary objectives. First, it seeks to highlight the concurrent rise of financial technology and financial compliance as well as the potential perils associated with that ascent. Second, this Article aims to provide studied commentary on the larger implications of the changing landscape of finance associated with the growing roles of new technology and compliance.

Drawing from the author's previous works and a rich panoply of scholarship on financial regulation and financial technology, this Article proceeds in three parts.[3] Part I offers an overview, describing the rise of new technology and the compliance function in modern finance. It explains how the concurrent and intersecting ascents of financial technology and compliance have changed the financial industry. Part II explores the perils of the changing financial industry. It examines the risks, threats, and vulnerabilities that emerge from the proliferation of new financial technology. Finally, Part III contends with key implications. In particular, it focuses on the challenges of financial cybersecurity, the integration of technology and compliance, and the role of humans in the future of modern finance.

I. COMPLIANCE AND THE NEW FINANCIAL INDUSTRY

Two of the most significant developments in the financial industry throughout the last few decades are the advances of new technology and compliance functionaries. These two developments are interrelated and will likely continue to play preeminent roles in the future of the financial industry.

---

2. *See* Susan Lorde Martin, *Compliance Officers: More Jobs, More Responsibility, More Liability*, 29 NOTRE DAME J.L. ETHICS & PUB. POL'Y 169, 181–82 (2015); Anthony Effinger, *The Rise of the Compliance Guru—and Banker Ire*, BLOOMBERG MKTS. (June 25, 2015), http://www.bloomberg.com/news/features/2015-06-25/compliance-is-now-calling-the-shots-and-bankers-are-bristling; Jon Marino, *At Goldman, Traders Are Out and Compliance is In*, CNBC: NETNET (Feb. 9, 2016, 11:00 AM), http://www.cnbc.com/2016/02/09/at-goldman-traders-are-out-and-compliance-is-in.html.

3. *See generally* Bernard S. Donefer, *Algos Gone Wild: Risk in the World of Automated Trading Strategies*, J. TRADING, Spring 2010, at 32; Frank J. Fabozzi et al., *High-Frequency Trading: Methodologies and Market Impact*, 19 REV. FUTURES MKTS. 8 (2011); Erik F. Gerding, *Code, Crash, and Open Source: The Outsourcing of Financial Regulation to Risk Models and the Global Financial Crisis*, 84 WASH. L. REV. 127 (2009); Joel Hasbrouck & Gideon Saar, *Low-Latency Trading,* 16 J. FIN. MKTS. 646 (2013); Steven L. Schwarcz, *Systemic Risk*, 97 GEO. L.J. 193 (2008); Kathryn Judge, *Fragmentation Nodes: A Study in Financial Innovation, Complexity, and Systemic Risk*, 64 STAN. L. REV. 657 (2012); Donald C. Langevoort & Robert B. Thompson, *"Publicness" in Contemporary Securities Regulation After the JOBS Act*, 101 GEO. L.J. 337, 347 (2013); Tom C.W. Lin, *The New Financial Industry*, 65 ALA. L. REV. 567 (2014); Andrew W. Lo & Mark T. Mueller, *Warning: Physics Envy May be Hazardous to Your Wealth!*, 8 J. INV. MGMT. 13, 14 (2010); Elizabeth Pollman, *Information Issues on Wall Street 2.0*, 161 U. PA. L. REV. 179 (2012); Charles K. Whitehead, *Reframing Financial Regulation*, 90 B.U. L. REV. 1, 5 (2010).

A. THE RISE OF FINANCIAL TECHNOLOGY

Advances in new financial technology over the last few decades have fundamentally transformed the workings of the financial industry.[4] In the financial industry, as in many other industries, human labor and intelligence have gradually been displaced by computerized automation and artificial intelligence.[5] Work in the financial industry that previously took hours, days, or weeks of human labor is now completed in minutes or seconds by supercomputers using artificial intelligence and algorithmic models.[6] Most sophisticated financial institutions are essentially high-tech companies. Not surprisingly, JPMorgan Chase has been estimated in recent years to employ "more software developers than Google and more technologists than Microsoft."[7]

This technological takeover of the financial industry implicates almost every segment of the industry, from trading to research to risk analysis to market-making to wealth management.[8] In terms of trading, autonomous, high-frequency trading programs powered by complex algorithms move billions of dollars in financial instruments across the world in fractions of a second.[9] In fact, machines and not humans now trade much of the securities in the world.[10] Machines today can trade securities and other financial

---

4. *See, e.g.*, DAVID J. LEINWEBER, NERDS ON WALL STREET: MATH, MACHINES, AND WIRED MARKETS 31–64 (2009) (chronicling 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) (describing modern finance as dependent "on fast-changing technology"); Felix Salmon & Jon Stokes, *Bull vs. Bear vs. Bot*, WIRED, Jan. 2011, at 90, 93 ("It's the machines' market now; we just trade in it."); Gregory Scopino, *Preparing Financial Regulation for the Second Machine Age: The Need for Oversight of Digital Intermediaries in the Futures Markets*, 2015 COLUM. BUS. L. REV. 439, 445–52 (2015) (discussing the impact of new technology on financial markets).

5. *See, e.g.*, MARTIN FORD, RISE OF ROBOTS: TECHNOLOGY AND THE THREAT OF A JOBLESS FUTURE 6–28 (2015) (examining the rise of robotics and automation across multiple industries within the economy); Tom C.W. Lin, *The New Investor*, 60 UCLA L. REV. 678, 682 (2013) (discussing the rise of smart financial machines); Concept Release on Risk Controls and System Safeguards for Automated Trading Environments, 78 Fed. Reg. 56,542 (Sept. 12, 2013) (to be codified at 17 C.F.R. ch. I) ("We have witnessed a fundamental shift in markets from human-based trading to highly automated electronic trading.").

6. Tom C.W. Lin, *Infinite Financial Intermediation*, 50 WAKE FOREST L. REV. 643, 653–54 (2015).

7. CA TECHNOLOGIES, HOW TO SURVIVE AND THRIVE IN THE APPLICATION ECONOMY 2 (2014).

8. *See* Timothy Lavin, *Monsters in the Market*, ATLANTIC, July–Aug. 2010, at 21.

9. SCOTT PATTERSON, DARK POOLS: HIGH-SPEED TRADERS, A.I. BANDITS, AND THE THREAT TO THE GLOBAL FINANCIAL SYSTEM 45–46 (2012); Fabozzi et al., *supra* note 3, at 8–10; Graham Bowley, *Fast Traders, in Spotlight, Battle Rules*, N.Y. TIMES, July 18, 2011, at A1.

10. *See* Bowley, *supra* note 9; Nathaniel Popper, *Public Exchanges Duel With Newcomers Over Trade Transparency*, N.Y. TIMES, June 27, 2012, at B1; Nelson D. Schwartz & Louise Story, *Surge of Computer Selling After Apparent Glitch Sends Stocks Plunging*, N.Y. TIMES, May 7, 2010, at B7.

instruments better, faster, and cheaper than their human counterparts in many instances.[11] This is even true in the traditionally clubby market for corporate bonds.[12] In terms of research, almost every significant financial institution utilizes smart machines.[13] Many hedge funds use algorithmic programs to read newsfeeds, analyze market data, and spot investment opportunities.[14] In terms of risk analysis, many financial institutions use artificially intelligent programs to analyze and manage risk for themselves and their clients.[15] For example, BlackRock, the world's largest asset management company with over $4 trillion under management as of 2016, uses a proprietary artificial intelligence program, called Aladdin, to manage risk on behalf of its clients.[16] During the financial crisis of 2008, the federal government turned to BlackRock and Aladdin for guidance on critical and complex decisions relating to distressed businesses like AIG, Bear Stearns, Citigroup, Fannie Mae, and Freddie Mac—entities with very complex financial assets and risk profiles.[17] In terms of market-making, new financial technology, along with regulatory reforms, have led to the rapid growth of high-speed electronic communication networks and alternative trading platforms, called "dark pools," which serve as real competitors to traditional public exchanges.[18] In fact, dark pools are the preferred trading platforms for many securities and financial instruments.[19] In terms of wealth management, financial advisors now face competition from smart wealth management software that cuts the human intermediary completely out of the picture. Companies, like Wealthfront and Betterment, use algorithmic programs almost exclusively to

---

11. *See, e.g.*, Yesha Yadav, *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.").

12. *See* Nathaniel Popper, *Shouts on Bond-Trading Floor Yield to Robot Beeps*, N.Y. TIMES, Oct. 20, 2014, at B1; Shawn Tully, *The Man Behind the $7.7 Trillion Bond Revolution*, FORTUNE, Dec. 22, 2014, at 98, 100, 102.

13. *See, e.g.*, Bradley Hope, *How Computers Trawl a Sea of Data for Stock Picks*, WALL ST. J. MKTS. (Apr. 1, 2015, 10:30 PM), http://www.wsj.com/articles/how-computers-trawl-a-sea-of-data-for-stock-picks-1427941801.

14. *See, e.g.*, PATTERSON, *supra* note 9, at 322–23; Seth Stevenson, *The Wolf of Wall Tweet*, SLATE: MONEYBOX (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.

15. *See* Gerding, *supra* note 3, at 130–35; *The Rise of BlackRock*, THE ECONOMIST, Dec. 7, 2013, at 13; Sheelah Kolhatkar & Sree Vidya Bhaktavatsalam, *The Colossus of Wall Street*, BLOOMBERG BUS. WK., Dec. 9, 2010, at 62, 66.

16. *See* Kolhatkar & Bhaktavatsalam, *supra* note 15; *About BlackRock Who We Are*, BLACKROCK, https://www.blackrock.com/corporate/en-us/about-us (last visited Feb. 27, 2016).

17. Kolhatkar & Bhaktavatsalam, *supra* note 15.

18. *See* SAL ARNUK & JOSEPH SALUZZI, BROKEN MARKETS: HOW HIGH FREQUENCY TRADING AND PREDATORY PRACTICES ON WALL STREET ARE DESTORYING INVESTOR CONFIDENCE AND YOUR PORTFOLIO 68–78 (2012); MICHAEL LEWIS, FLASH BOYS: A WALL STREET REVOLT 3, 42–43 (2014).

19. *See* LEWIS, *supra* note 18, at 42; Matthew Philips, *Where Has All the Stock Trading Gone?*, BLOOMBERG (May 10, 2012, 10:20 PM), http://www.bloomberg.com/news/articles/2012-05-10/where-has-all-the-stock-trading-gone.

manage billions of dollars of assets at lower costs and with comparable success.[20]

Looking ahead, this technological transformation of the financial industry will likely continue in the years ahead, because entrepreneurs and innovators continue to examine ways to disrupt traditional financial intermediaries, as evidenced by developments in recent years.[21] Like the automated wealth managers discussed earlier, online banks and brokerages have created real competition for traditional banks and brokers.[22] Peer-to-peer online platforms, like LendingClub and Prosper, which connect lenders and borrowers directly, present a legitimate alternative to traditional loans from banks.[23] New payment systems, like ApplePay, Square, Stripe, and Venmo have disrupted traditional payment intermediaries and processes.[24] Crowdfunding portals, like Kiva and Kickstarter, have helped entrepreneurs in big cities and small villages around the world to raise start-up capital in an unprecedented fashion.[25] Online platforms, like SecondMarket and SharesPost, have made it easier for people to trade securities of privately held companies.[26] Bitcoin and its blockchain technology have created an entirely new currency and transactional process devoid of traditional banking intermediaries.[27] Many of these new financial innovations have had

---

20. John F. Wasik, *Sites to Manage Personal Wealth Gaining Ground*, N.Y. TIMES (Feb. 10, 2014), http://www.nytimes.com/2014/02/11/your-money/sites-to-manage-personal-wealth-gaining-ground.html.

21. *See, e.g.*, JPMORGAN CHASE & CO., 2014 ANNUAL REPORT (FORM 10-K) 29 (2015) [hereinafter JPMORGAN CHASE REPORT], http://files.shareholder.com/downloads/ONE/15660259x0x820077/8af78e45-1d81-4363-931c-439d04312ebc/JPMC-AR2014-LetterToShareholders.pdf; Lin, *supra* note 6, at 650–52 (discussing the roles of traditional financial intermediaries); Dani Burger, *Free-Range Quant*, BUS. WK., Mar. 21, 2016, at 43.

22. *See* ANN C. LOGUE, DAY TRADING FOR DUMMIES 196 (2d ed. 2011); Hanno Beck, *Banking Is Essential, Banks Are Not: The Future of Financial Intermediation in the Age of the Internet*, 3 NETNOMICS 7 (2001); Wasik, *supra* note 20.

23. *See* Lisa T. Alexander, *Cyberfinancing for Economic Justice*, 4 WM. & MARY BUS. L. REV. 309, 335 (2013) ("Online P2P lending describes interactive websites that allow borrowers and lenders to transact with one another online without the traditional involvement of a mainstream financial institution."); Eric C. Chaffee & Geoffrey C. Rapp, *Regulating Online Peer-to-Peer Lending in the Aftermath of Dodd-Frank: In Search of an Evolving Regulatory Regime for an Evolving Industry*, 69 WASH. & LEE L. REV. 485, 508 (2012) (highlighting leading peer lending sites like Prosper and LendingClub).

24. *See* SKIP ALLUMS, DESIGNING MOBILE PAYMENT EXPERIENCES: PRINCIPLES AND BEST PRACTICES FOR MOBILE COMMERCE 59–93 (2014); Beck, *supra* note 22, at 9 (speculating on the rise of electronic payment systems).

25. *See, e.g.*, Andrew A. Schwartz, *The Digital Shareholder*, 100 MINN. L. REV. 609, 614–20 (2015) (providing an overview of crowdfunding); Alexander, *supra* note 23, at 312.

26. Pollman, *supra* note 3, at 193–201.

27. *See* PAUL VIGNA & MICHAEL J. CASEY, THE AGE OF CRYPTOCURRENCY: HOW BITCOIN AND DIGITAL MONEY ARE CHALLENGING THE GLOBAL ECONOMIC ORDER 4–10 (2015); Jerry Brito et al., *Bitcoin Financial Regulation: Securities, Derivatives, Prediction Markets, and Gambling*, 16 COLUM. SCI. & TECH. L. REV. 144, 148–49 (2014) (explaining the operations of bitcoins); Omri Marian, *Are Cryptocurrencies Super Tax Havens?*, 112 MICH. L. REV. FIRST IMPRESSIONS 38, 42 (2014) ("[T]he operation of Bitcoin is not dependent on the existence of financial intermediaries such as banks.").

beneficial effects—in many instances, they have expanded the capital markets for businesses, lowered the costs of raising capital for entrepreneurs, created greater conveniences for consumers, and provided more user-friendly tools for investors. [28]

In sum, advances in new financial technology over the last few decades have caused a sea change in the operations of the financial industry, and will likely continue to disrupt and transform the financial industry in the years to come.

B. THE RISE OF FINANCIAL COMPLIANCE

Like the rise of new technology, the ascent of the compliance function over the last few decades has dramatically changed the operations of many financial institutions.[29] The rise of financial compliance is fueled in part by increased regulatory scrutiny of financial firms as well as increased complexity in financial regulation and financial markets.[30]

The rise of the compliance function in finance has been motivated partially in response to the enhanced scrutiny of financial firms in the post-Enron regulatory era.[31] Federal regulators' and prosecutors' aggressive enforcement of a patchwork of federal financial regulations serves as an impetus for firms to do more to comply with the rules.[32] Most prominently, the Securities and Exchange Commission (SEC) and the Department of Justice (DOJ) can investigate, prosecute, and sue financial firms for improper supervision of operations and personnel based on landmark laws like the Securities Act of 1933, the Securities Exchange Act of 1934, the Investment Advisers Act of 1940, the Investment Company Act of 1940, the Foreign Corrupt Practices Act, the Sarbanes-Oxley Act of 2002 (Sarbanes-Oxley), and the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank). For instance, the Investment Advisers Act and the Investment Company Act explicitly require companies to establish and maintain robust

---

28. *See, e.g.*, Charles R. Korsmo, *High-Frequency Trading: A Regulatory Strategy*, 48 RICH. L. REV. 523, 549–50 (2014) (cataloguing benefits relating to high-frequency trading); Langevoort & Thompson, *supra* note 3, at 347 ("Today, liquidity is now much more possible outside of traditional exchanges. In the new millennium, cheap information and low communication costs have expanded markets."); Hasbrouck & Saar, *supra* note 3, at 648 (suggesting that high-frequency trading has stabilizing marketplace effects).

29. *See* James A. Fanto, *Advising Compliance in Financial Firms: A New Mission for the Legal Academy*, 8 BROOK. J. CORP. FIN. & COM. L. 1, 13–16 (2013); Sean J. Griffith, *Corporate Governance In An Era of Compliance*, 57 WM. & MARY L. REV. 2075, 2077 (2016) ("Over the past decade, compliance has blossomed into a thriving industry, and the compliance department has emerged, in many firms, as the co-equal of the legal department.").

30. GEOFFREY PARSONS MILLER, THE LAW OF GOVERNANCE, RISK MANAGEMENT, AND COMPLIANCE 1 (2014).

31. *Id.* at 2.

32. *Id.* at 168–69 (highlighting the role of federal enforcement in the development of modern compliance programs); Griffith, *supra* note 29, at 2086–92 (discussing how changing enforcement tactics led to the growth of compliance).

compliance programs or risk SEC and DOJ action.[33] Similarly, Sarbanes-Oxley requires firms to establish internal controls and procedures for their financial statements and disclosures.[34] Moreover, self-regulatory organizations like the Financial Industry Regulatory Authority (FINRA) also add to the thicket of rules and regulations that require greater supervision and surveillance by financial firms.[35]

In addition to the aforementioned patchwork of financial regulation, the Federal Sentencing Guidelines (Guidelines) also play an influential role in the booming contemporary compliance practices.[36] The Guidelines were introduced by the U.S. Sentencing Commission, which was created pursuant to the Sentencing Reform Act of 1984.[37] The Guidelines serve as guidance for establishing penalties for federal law violations, including those involving corporations and other business entities.[38] The Guidelines created a scoring system to help determine the penalties for federal offenses.[39] Aggravating factors increase the number of points of an offender's Culpability Score and thereby increase the severity of punishment.[40] Conversely, mitigating factors decrease the offender's points and thereby decrease the severity of punishment.[41] An "effective compliance and ethics program" is considered a mitigating factor that decreases a corporate offender's Culpability Score.[42] For instance, a good compliance program can help a financial firm and its executives mitigate the multi-million or billion dollar fines and prison sentences that can come with violating certain provisions of Sarbanes-Oxley.[43] Not surprisingly, given the impact of a good compliance program on the penalties that a company may face, many firms in the financial industry and elsewhere invest significant resources in creating a decent compliance program.[44]

---

33. Compliance Programs of Investment Companies and Investment Advisors, 68 Fed. Reg. 74,714 (Dec. 24, 2003) (codified at 17 C.F.R. §§ 270.38a–1, 275.206(4)–7, 275.204–2, 279.1 (2016)).

34. Sarbanes-Oxley Act of 2002 (Sarbanes-Oxley Act), Pub. L. No. 107-204, 116 Stat. 745 (2002) (codified as amended at 15 U.S.C. § 7262(a) (2012)).

35. *See* William A. Birdthistle & M. Todd Henderson, *Becoming a Fifth Branch,* 99 CORNELL L. REV. 1, 12–24 (2013) (discussing the regulatory powers of FINRA); Fanto, *supra* note 29, at 6–7.

36. Martin, *supra* note 2, at 172.

37. Comprehensive Crime Control Act of 1984, Pub. L. No. 99-646, 100 Stat. 3592 (1986) (codified as amended at 18 U.S.C. §§ 3551–3673 (2012)); The Sentencing Reform Act of 1984, Pub. L. No. 98-473, 98 Stat. 1837 (1984) (codified as amended at 28 U.S.C. §§ 991–98 (2012)).

38. 28 U.S.C. §§ 991–98 (2012).

39. U.S. SENTENCING GUIDELINES MANUAL § 8C2.5 (U.S. SENTENCING COMM'N 2013).

40. *Id.*

41. *Id.*

42. *Id.* § 8C2.5(f)(1).

43. Sarbanes-Oxley Act, Pub. L. No. 107-204, 116 Stat. 745 (2002) (codified as amended at 18 U.S.C. § 1350 (2012)).

44. *See* Martin, *supra* note 2, at 173; Griffith, *supra* note 29, at 2102.

Beyond the increased regulatory spotlight cast on financial firms, the growing complexity in financial regulation and financial markets has also played a significant role in the rise of compliance in the financial industry.[45] The financial marketplace today is incredibly complex and filled with a diverse cast of players. [46] Financial firms today operate in a global marketplace with interdependent institutions and instruments, frequently governed by crosscutting bodies of law and regulation that span multiple jurisdictions and regulatory bodies.[47] This new, more complex marketplace has generated greater opportunities for profits as well as losses.[48] To address the changing risks of the marketplace, regulators frequently promulgate new rules that in turn add greater complexity to the marketplace. This is due to the fact that financial innovation frequently finds roots in attempts to evade or arbitrage new regulations.[49] As a result of this new complexity in the marketplace, financial firms invariably devote more resources to compliance functions in order to operate consistently with the new rules and market practices of a more complex environment.[50]

---

45. *See* Martin*, supra* note 2, at 170 ("In response to a great deal of new rule making by federal agencies in the last few years, corporate compliance departments are becoming larger and more involved in line businesses in an effort to eliminate regulatory violations and to reduce fines in the event of an offense.").

46. *See, e.g.*, Dan Awrey, *Complexity, Innovation, and the Regulation of Modern Financial Markets*, 2 HARV. BUS. L. REV. 235, 242 (2012) ("Modern financial markets are very, very complex. This complexity is compounded by the nature and pace of financial innovation."); Judge, *supra* note 3, at 701; Steven L. Schwarcz, *Regulating Complexity in Financial Markets*, 87 WASH. U. L. REV. 211, 212–13 (2009) (discussing complexity "as the greatest financial-market challenge of the future"); Tom C.W. Lin, *Reasonable Investor(s)*, 95 B.U. L. REV. 461 (2015) (surveying the various types of investors in the contemporary marketplace).

47. *See* HAL S. SCOTT, INTERCONNECTEDNESS AND CONTAGION 2–7 (2012) (exploring the extent of asset and liability interconnectedness among the major financial institutions); Markus K. Brunnermeier, *Deciphering the Liquidity and Credit Crunch 2007-2008*, J. ECON. PERSP., Winter 2009, at 96 (discussing the "interwoven network of financial obligations"); Robin Greenwood & David S. Scharfstein, *How To Make Finance Work*, HARV. BUS. REV., Mar. 2013, at 107.

48. *See, e.g.*, Guillermo A. Calvo & Enrique G. Mendoza, *Rational Contagion and the Globalization of Securities Markets*, 51 J. INT'L ECON. 79, 80–83 (2000); Mariassunta Giannetti & Yrjö Koskinen, *Investor Protection, Equity Returns, and Financial Globalization*, 45 J. FIN. & QUANTITATIVE ANALYSIS 135, 135–38 (2010).

49. *See, e.g.*, Annelise Riles, *Managing Regulatory Arbitrage: A Conflicts of Laws Approach*, 47 CORNELL INT'L L.J. 63, 77–83 (2014); *see also* Charles W. Calomiris, *Financial Innovation, Regulation, and Reform*, 29 CATO J. 65, 65 (2009) (explaining how financial innovation is often motivated by "sidestepping regulatory restrictions"); Victor Fleischer, *Regulatory Arbitrage*, 89 TEX. L. REV. 227, 229 (2010) ("Regulatory arbitrage exploits the gap between the economic substance of a transaction and its legal or regulatory treatment, taking advantage of the legal system's intrinsically limited ability to attach formal labels that track the economics of transactions with sufficient precision."); Frank Partnoy, *Financial Derivatives and The Costs of Regulatory Arbitrage*, 22 J. CORP. L. 211, 227 (1997) ("Regulatory arbitrage consists of those financial transactions designed specifically to reduce costs or capture profit opportunities created by differential regulations or laws.").

50. *See* MERVYN KING, THE END OF ALCHEMY: MONEY, BANKING, AND THE FUTURE OF THE GLOBAL ECONOMY 245 (2016) ("By encouraging a culture in which compliance with detailed regulation is a defense against a charge of wrong-doing, bankers and regulators have colluded in a self-defeating spiral of complexity.").

Furthermore, because financial regulatory reform efforts historically follow economic crises and corporate scandals, policymakers tend to react and overreact in an omnibus manner.[51] In an understandable attempt to prevent the last crisis from happening again, regulators frequently use sledgehammers rather than scalpels in creating new regulations, which is often not a sensible approach to rulemaking and regulation.[52] And as crises and scandals become larger, so do the regulatory responses to them. For example, the Glass-Steagall Act of 1933, which was implemented following the Great Depression, ran 37 pages; Dodd-Frank is contained in 848 pages with thousands of pages of additional rules (and still many more forthcoming).[53] It has been estimated that it would take businesses over twenty-four million workers' hours to comply with the demands of the recently passed Dodd-Frank rules.[54] Dodd-Frank's "Volcker Rule" relating to risky proprietary trading alone is contained in 964 pages, including an 893-page preamble.[55] The rule involved 18,223 comments and 1,238 days of rulemaking.[56] Additionally, regulations promulgated in response to crises and scandals in down times frequently become deregulated in good times—creating a consequential and costly cycle of over-regulation, deregulation, and re-regulation.[57] Due in large part to this regulatory pathology and the

---

51. *See* Stuart Banner, *What Causes New Securities Regulation? 300 Years of Evidence*, 75 WASH. U. L. Q. 849, 850 (1997) ("[M]ost of the major instances of new securities regulation in the past three hundred years of English and American history have come right after crashes."); John C. Coffee, Jr., *The Political Economy of Dodd-Frank: Why Financial Reform Tends To Be Frustrated and Systemic Risk Perpetuated*, 97 CORNELL L. REV. 1019, 1020 (2012) ("[O]nly after a catastrophic market collapse can legislators and regulators overcome the resistance of the financial community and adopt comprehensive 'reform' legislation.'"); Tom C.W. Lin, *Vistas of Finance*, 61 UCLA L. REV. DISCOURSE 78, 85 (2013).

52. *See* Edward F. Greene & Elizabeth L. Broomfield, *Promoting Risk Mitigation, Not Migration: A Comparative Analysis of Shadow Banking Reforms by the FSB, USA and EU*, 8 CAP. MKTS. L.J. 6, 8 (2013) ("[The current regulatory approach] subjects diverse entities to a 'one-size-fits-all' regulatory approach, ignoring the different causes of risk, and also further complicating legal obligations for entities that are often already subject to other complex regulatory regimes.").

53. Andrew G. Haldane, Exec. Dir., Fin. Stability, Bank of Eng., Speech at the Federal Reserve Bank of Kansas City's 36th Economic Policy Symposium: The Changing Policy Landscape: The Dog and the Frisbee, Jackson Hole, Wyoming 10 (Aug. 31, 2012), https://www.kansascityfed.org/publicat/sympos/2012/ah.pdf.

54. Daniel M. Gallagher, Comm'r, Sec. & Exch. Comm'n, Remarks at the 2013 National Compliance Outreach Program for Broker-Dealers (Apr. 9, 2013), http://www.sec.gov/News/Speech/Detail/Speech/1365171515226#.UvAMT_shMuc.

55. *See* Prohibitions and Restrictions on Proprietary Trading and Certain Interests in, and Relationships with, Hedge Funds and Private Equity Funds, 79 Fed. Reg. 5779, 5804–05 (Jan. 31, 2014) (codified at 12 C.F.R. §§ 44, 248, 351, 255 (2016)).

56. Peter Coy et al., *1,238 days, 18,223 comments, 71-page rule, 893-page preamble, 5 agencies, 1 man*, BUS. WK., Dec. 16, 2013, at 41.

57. *See* ERIK F. GERDING, LAW, BUBBLES, AND FINANCIAL REGULATION 137–39 (2013); NOLAN M. MCCARTY ET AL., POLITICAL BUBBLES: FINANCIAL CRISES AND THE FAILURE OF AMERICAN DEMOCRACY 14–15 (2013); Patricia A. McCoy et al., *Systemic Risk Through Securitization: The Result of Deregulation and Regulatory Failure*, 41 CONN. L. REV. 1327, 1333 (2009); Coffee Jr., *supra* note 51 ("[R]egulatory oversight is never constant but rather increases

ever-shifting regulatory landscape, financial institutions have had to devote more resources and personnel to their compliance operations to make sure that their companies have surer footing.[58] For instance, due in part to new regulatory requirements, annual reports of publicly traded companies on Form 10-K increased from around "23,000 words in 1996 to over 49,000 words in 2013."[59]

If recent history is any guide, the importance of the compliance function will continue to rise in the years to come, given the enhanced regulatory scrutiny and marketplace complexities confronting financial firms, particularly the extremely large ones.[60] Anecdotally, in the two-year period between 2012 and 2014, JPMorgan alone invested billions of dollars and added 13,000 new employees to its compliance efforts to better meet the demands of the new regulatory normal.[61] Similarly, many other large financial institutions are investing more resources into compliance, and will likely continue to do so for the foreseeable future.[62]

II. EMERGING RISKS, THREATS, AND VULNERABILITIES

The growing technological shift in the financial industry has created a new set of perils. In this day and age, every sophisticated financial company is essentially a tech company. Beyond traditional balance sheet concerns, financial institutions must now also focus on the hazards and menaces associated with new financial technology.

A. NORMAL FINANCIAL ACCIDENTS & SYSTEMIC RISKS

The financial industry's growing reliance on advanced technology could pose significant systemic risks for the financial system.[63] Complex, high-tech

---

after a market crash and then wanes as, and to the extent that, society and the market return to normalcy[.]").

58. PRICEWATERHOUSE COOPERS, STATE OF COMPLIANCE 2014: FINANCIAL SERVICES INDUSTRY BRIEF 5–9 (2014), http://www.pwc.com/us/en/risk-management/state-of-compliance-survey/assets/pwc-soc-financial-services.pdf.

59. Travis Dyer et al., *The Ever-Expanding 10-K: Why Are 10-Ks Getting So Much Longer (And Does It Manner)?*, CLS BLUE SKY BLOG (May 5, 2016), http://clsbluesky.law.columbia.edu/2016/05/05/the-ever-expanding-10-k-why-are-10-ks-getting-so-much-longer-and-does-it-matter/.

60. *See* Martin, *supra* note 2, at 181 ("Companies, especially banks, are greatly increasing the size of their compliance departments.").

61. JPMORGAN CHASE REPORT, *supra* note 21, at 12–13.

62. Martin, *supra* note 2, at 181–83.

63. *See, e.g.*, Kristin N. Johnson, *Cyber Risks: Emerging Risk Management Concerns For Financial Institutions*, 50 GA. L. REV. 131, 137 (2015) ("[T]he evidence demonstrates that cyber risks have the potential to create systemic risks."); Amir E. Khandani et al., *Systemic Risk and the Refinancing Ratchet Effect* 38 (Harv. Bus. Sch. Fin., Working Paper No. 1472892, 2012) ("[S]ystemic risk . . . arises when large financial losses affect important economic entities that are unprepared for and unable to withstand such losses, causing a cascade of failures and widespread loss of confidence.").

systems invariably malfunction and suffer from glitches.[64] The sociologist Charles Perrow termed this truism "normal accidents."[65] Because of the complex, high-tech infrastructure that is at the heart of modern finance, "normal financial accidents" will be inevitable and could cause substantial strains on the entire financial system.[66] While much has been said and written about the systemic risk associated with "too big to fail" institutions,[67] less attention has been paid to the systemic risk associated with new financial technology. In particular, the new, high-tech financial system poses systemic risks related to links and speeds that the author has previously termed "too linked to fail" and "too fast to save," respectively.[68]

First, in terms of "too linked to fail," the high-tech interconnected and interdependent nature of modern finance means that technological disruption to certain institutions that serve as important nodes in the financial system could lead to widespread damage and crisis.[69] This systemic risk is dissimilar from "too big to fail," which revolves primarily around large, systemically important banking institutions like JPMorgan Chase, Citigroup, Goldman Sachs, Bank of America, Morgan Stanley, and Wells Fargo.[70] With the risk of "too linked to fail," smaller intermediaries that need not be banking institutions can cause serious systemic distress.[71] Smaller and less prominent financial intermediaries like clearinghouses, financial data firms, hedge funds, dark pools, and securities information processors all serve as important components in today's high-tech financial system.[72] The Depository Trust &

---

64. *See* CHARLES PERROW, NORMAL ACCIDENTS: LIVING WITH HIGH-RISK TECHNOLOGIES 71 (1999) (discussing the tendency for failures or "accidents" to compound upon one another).

65. *See generally id.*

66. 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: PART A 284–89 (Michael Lounsbury & Paul M. Hirsch eds., 2010).

67. *See, e.g.*, CONG. OVERSIGHT PANEL FOR ECON. STABALIZATION, SPECIAL REPORT ON REGULATORY REFORM: MODERNIZING THE AMERICAN FINANCIAL REGULATORY SYSTEM: RECOMMENDATIONS FOR IMPROVING OVERSIGHT, PROTECTING CONSUMERS, AND ENSURING STABILITY 15–17 (2009) (reporting on the rise of "too big to fail" financial institutions); 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 dangers and challenges presented by "too big to fail" financial institutions).

68. *See* Lin, *supra* note 5, at 711–17.

69. *See* PRICEWATERHOUSE COOPERS & INV'R RESPONSIBILITY RESEARCH CTR. INST., WHAT INVESTORS NEED TO KNOW ABOUT CYBERSECURITY: HOW TO EVALUATE INVESTMENT RISKS 1–5 (2014); ERIC SCHMIDT & JARED COHEN, THE NEW DIGITAL AGE: TRANSFORMING NATIONS, BUSINESSES, AND OUR LIVES 151–52 (2014); Schwarcz, *supra* note 3, at 200.

70. FIN. STABILITY BD., 2015 UPDATE OF LIST OF GLOBAL SYSTEMICALLY IMPORTANT BANKS 2 (2015).

71. *See* FIN. STABILITY BD., ASSESSMENT METHODOLOGIES FOR IDENTIFYING NON-BANK NON-INSURER GLOBAL SYSTEMICALLY IMPORTANT FINANCIAL INSTITUTIONS (2014); Schwarcz, *supra* note 3, at 200 (discussing systemic risks associated with the interconnectedness of certain financial institutions).

72. *See, e.g.*, Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act), Pub. L. No. 111-203, § 803(6), 124 Stat. 1376, 1805 (2010) (codified as amended in scattered

Clearing Corporation, which clears trillions of dollars in transactions daily via its high-tech platform, is a critical link in global capital markets, and any malfunction in its computer systems could cause serious disarray to the financial system. [73] In 2015, the temporary technical impairment of Bloomberg terminals caused significant strain on the global bond market, affecting billions of dollars in transactions.[74] To be clear, Bloomberg is an information services provider with about 325,000 terminals used by financial traders, not a large financial banking institution.[75] Nevertheless, because of its role as an important link in today's high-tech financial infrastructure, it is critically important to the financial system's stability. [76]

Second, in terms of "too fast to save," the high-tech, high-speed nature of modern finance increases the risks that normal financial accidents could cause significant systemic harm so quickly that prevention and intervention is not feasible.[77] Financial transactions today frequently move at values measured in billions of dollars and velocities measured in fractions of a second, because of new technology like high-speed, automated supercomputer programs.[78] Compounding the dangers related to astounding

---

sections of 7, 15, and 28 of U.S.C.) (designating certain financial entities, such as major clearinghouses, as systemically important financial market utilities); Judge, *supra* note 3, at 685; Schwarcz, *supra* note 46, at 215; Whitehead, *supra* note 3, at 5 (discussing the growth and impact of hedge funds in the modern financial marketplace); Yesha Yadav, *The Problematic Case of Clearinghouses in Complex Markets*, 101 GEO. L.J. 387, 389 (2013) ("Clearinghouses are stitched into the fabric of the financial markets and intrinsic to their operation.").

73. DEPOSITORY TRUST & CLEARING CORP., ANNUAL REPORT, SECURING TODAY. SHAPING TOMORROW. 2 (2014).

74. Nathaniel Popper & Neil Gough, *Bloomberg Data Crash Puts Market in Turmoil*, N.Y. TIMES, Apr. 18, 2015, at B1.

75. *Id.*

76. *Id.*

77. *See* FRANK PARTNOY, WAIT: THE ART AND SCIENCE OF DELAY 43 (2012); PERROW, *supra* note 64, at 71 (discussing the compounding consequences of failures and accidents); Andrew G. Haldane, Exec. Dir. Fin. Stability, Bank of Eng., Speech at the International Economic Association Sixteenth World Congress: The Race to Zero 15 (July 8, 2011), http://www.bankofengland.co.uk/archive/Documents/historicpubs/news/2011/068.pdf; *see also* Fabozzi et al., *supra* note 3, at 29 (discussing how emphasis on speed and technology fragments the financial industry); Floyd Norris, *In Markets' Tuned-Up Machinery, Stubborn Ghosts Remain*, N.Y. TIMES, Aug. 23, 2013, at B1; Matthew Baron et al., The Trading Profits of High Frequency Traders (Nov. 2012) (unpublished manuscript) (on file with the National Bureau of Economic Research) http://conference.nber.org/confer//2012/MMf12/Baron_Brogaard_Kirilenko.pdf (finding that high-frequency traders profit at the expense of ordinary investors).

78. *See* Concept Release on Equity Market Structure, Exchange Act Release No. 61,358, 75 Fed. Reg. 3594, 3610 (proposed Jan. 21, 2010) (to be codified at 17 C.F.R. pt. 242) (noting the accelerating velocity of modern financial transactions); PATTERSON, *supra* note 9, at 46; Fabozzi et al., *supra* note 3, at 8; A. D. Wissner-Gross & C. E. Freer, *Relativistic Statistical Arbitrage*, 82 PHYSICAL REV. E 056104 (2010) (studying trading opportunities near the speed of light); Graham Bowley, *The New Speed of Money*, N.Y. TIMES, Jan. 2, 2011, at BU1 ("Almost each week, it seems, one exchange or another claims a new record: NASDAQ, for example, says its time for an average order 'round trip' is 98 microseconds—a mind-numbing speed equal to 98 millionths of a second."); Quentin Hardy, *Testing a New Class of Speedy Computer*, N.Y. TIMES, Mar. 22, 2013, at B1; Matthew Philips, *Trading at the Speed of Light*, BLOOMBERG BUS. WK., Apr. 2, 2012, at 46.

speed is the fact that many of these programs are built on similar and interdependent codes.[79] As such, a glitch in a particular program or institution's computer system could cause volatile cascading and spillover effects as automated systems react instantaneously and adversely to the triggering glitch.[80] On May 6, 2010, the American stock market experienced an unprecedented event later called the Flash Crash, which was allegedly caused by a single, errant trade initiated by a computer program.[81] In the span of a few minutes, an estimated $1 trillion in market value disappeared from the U.S. stock market for no clear reason and created chaos in the marketplace.[82] More recently, in 2014, the U.S. Treasuries market experienced a 37-basis point swing during a few minutes, one of the largest changes in one session ever, for no apparent reason.[83] As the financial system becomes ever more high-tech and high-speed, aberrant volatile market events like the Flash Crash have happened more regularly and will likely happen even more in the coming years.[84]

Systemic risk is a critical challenge confronting regulators of the modern financial system.[85] As modern finance becomes more technology-oriented, regulators will need to expand their oversight, focus beyond the systemic

---

79. *See* Concept Release on Equity Market Structure, 75 Fed. Reg. at 3611 ("[M]any proprietary firms potentially could engage in similar or connected trading strategies that, if such strategies generated significant losses at the same time, could cause many proprietary firms to become financially distressed and lead to large fluctuations in market prices."); BRIAN R. BROWN, CHASING THE SAME SIGNALS: HOW BLACK-BOX TRADING INFLUENCES STOCK MARKETS FROM WALL STREET TO SHANGHAI 7 (2010); PATTERSON, *supra* note 9, at 9–10 (discussing the financial dangers of "a vicious self-reinforcing feedback loop"); Donefer, *supra* note 3, at 32; Geoffrey P. Miller & Gerald Rosenfeld, *Intellectual Hazard: How Conceptual Biases in Complex Organizations Contributed to the Crisis of 2008*, 33 HARV. J.L. & PUB. POL'Y 807, 810 (2010).

80. *See* Concept Release on Equity Market Structure, 75 Fed. Reg. at 3611; Donefer, *supra* note 3, at 32; Miller & Rosenfeld, *supra* note 79, at 810.

81. *See* U.S. COMMODITY FUTURES TRADING COMM'N & U.S. SEC. AND EXCH. COMM'N, FINDINGS REGARDING THE MARKET EVENTS OF MAY 6, 2010 REPORT OF THE STAFFS OF THE CFTC AND SEC TO THE JOINT ADVISORY COMMITTEE ON EMERGING REGULATORY ISSUES 1 (2010); Graham Bowley, *Lone Sale of $4.1 Billion in Contracts Led to 'Flash Crash' in May*, N.Y. TIMES, Oct. 2, 2010, at B1; *see also* Nathaniel Popper, *Trader's Arrest Raises Concern About Market Rigging*, N.Y. TIMES, Apr. 23, 2010, at B1.

82. Haldane, *supra* note 77, at 2.

83. U.S. DEPT. OF THE 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.

84. *See* E.S. Browning & Scott Patterson, *Complex Systems Get Blame*, WALL ST. J., Aug. 23, 2013, at C1; Nathaniel Popper, *Pricing Problem Suspends NASDAQ for Three Hours*, N.Y. TIMES, Aug. 23, 2013, at A1; Nathaniel Popper, *The Bell Rings, Computers Fail, Wall St. Cringes*, N.Y. TIMES, July 9, 2015, at A1; Louise Story & Graham Bowley, *Market Swings Are Becoming New Standard*, N.Y. TIMES, Sept. 12, 2011, at A1; James Surowiecki, *New Ways to Crash the Market*, THE NEW YORKER, May 18, 2015, at 37 ("High-speed firms tend to mimic one another's trading strategies, and in times of crisis this can amplify price swings.").

85. *See* Hal S. Scott, *The Reduction of Systemic Risk in the United States Financial System*, 33 HARV. J.L. & PUB. POL'Y 671, 673 (2010) ("Going forward, the central problem for financial regulation . . . is to reduce systemic risk.").

risks associated with size, and concentrate more on the high-tech, systemic risks associated with links and speed.

B. THE INTERNET OF FINANCIAL THREATS

The modern, high-tech financial industry faces a myriad of threats and vulnerabilities beyond the aforementioned systemic risks.[86] The financial industry's structural dependency on interconnected, computerized systems makes it vulnerable to many technological threats.[87] Many significant crimes and aggressions against financial firms now involve computers as the weapons of choice and cyberspace as the preferred crime scene.[88] The robber with a gun has been replaced by the hacker with a laptop. It has been estimated that the costs of cybercrime will be around $2 trillion by 2019.[89] For many financial institutions, computer codes, proprietary software, confidential data, and other intellectual property represent some of their most valuable assets.[90] General Keith Alexander, the former head of the National Security Agency (NSA) and the U.S. Cyber Command, called the loss of American business secrets and intellectual property to cyber-criminals "the greatest transfer of wealth in history."[91]

The emergence of the Internet of financial things is also the emergence of the Internet of financial threats.[92] Financial firms today face diverse technological threats, both external and internal in nature. External threats include antagonists like foreign nations, competitors, hackers, cyber-

---

86. *See, e.g.*, Tom C.W. Lin, *Financial Weapons of War*, 100 MINN. L. REV. 1377, 1405–08 (2016) (discussing the threats of "cyber financial weapons").

87. *See, e.g.*, OFFICE OF THE NAT'L COUNTERINTELLIGENCE EXEC., FOREIGN SPIES STEALING U.S. ECONOMIC SECRETS IN CYBERSPACE: REPORT TO CONGRESS ON FOREIGN ECONOMIC COLLECTION AND INDUSTRIAL ESPIONAGE, 2009-2011 (2011); Derek E. Bambauer, *Ghost in the Network*, 162 U. PA. L. REV. 1011, 1022 (2014) ("The Internet makes securing code much harder by exposing the inevitable bugs in software to sustained scrutiny and attack. Many—if not most—computers are connected to the Internet directly or indirectly.").

88. *See* BARRY VENGERIK ET AL., HACKING THE STREET? FIN4 LIKELY PLAYING THE MARKET 3 (2014); Michael Riley & Ashlee Vance, *The Code War*, BLOOMBERG BUS. WK., July 25, 2011, at 52.

89. JAMES MOAR, JUNIPER RESEARCH, CYBERCRIME & THE INTERNET OF THREATS (May 2015), http://www.juniperresearch.com/document-library/white-papers/cybercrime-the-internet-of-threats.

90. *See* BROWN, *supra* note 79, at 49 (2010) (discussing the urgent need for black-box firms to safeguard successful strategies for as long as possible); David Barboza & Kevin Drew, *Security Firm Sees Global Cyberspying*, N.Y. TIMES, Aug. 4, 2011, at A11 ("Cybersecurity is now a major international concern, with hackers gaining access to sensitive corporate and military secrets, including intellectual property."); Alex Berenson, *Arrest Over Trading Software Illuminates a Secret of Wall St*., N.Y. TIMES, Aug. 24, 2009, at A1 (noting the importance of computer programs to financial institutions).

91. John Seabrook, *Network Insecurity*, THE NEW YORKER, May 20, 2013, at 64 (quoting Gen. Keith Alexander).

92. *See* MOAR, *supra* note 89; 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. 16, 2013, at B5; Riley & Vance, *supra* note 88, at 52.

criminals, and cyber-mercenaries.[93] Episodes from the last few years alone highlight the diversity of external threats confronting financial institutions in this day and age. In 2011, hackers affiliated with WikiLeaks threatened Bank of America with stolen, sensitive corporate information.[94] A year later, in 2012, large, coordinated cyberattacks, widely attributed to Iran, targeted American and international financial institutions.[95] In 2013, hackers infiltrated the Associated Press's Twitter account to falsely broadcast an attack on the White House, which momentarily caused a $136 billion loss in stock market value when automated programs traded on the bogus news.[96] In 2014, it was reported that Russian hackers infiltrated the NASDAQ computer system.[97] That same year, cyber-criminals hacked into the data systems of Wall Street firms to steal material, nonpublic information.[98] In 2015, it was revealed that an international cyber-gang systemically robbed millions of dollars from over one hundred institutions around the world;[99] and an international syndicate of traders and hackers were charged with operating a

93. *See, e.g.*, SEC v. Dorozhko, 574 F.3d 42, 44–46 (2d Cir. 2009) (opining on a case involving hackers who traded on illicitly acquired, material, nonpublic information); U.S DEPT. OF DEF., THE DEPARTMENT OF DEFENSE CYBER STRATEGY 9 (2015) ("Criminal actors pose a considerable threat in cyberspace, particularly to financial institutions, and ideological groups often use hackers to further their political objectives."); 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 cyber mercenaries); INTELLIGENCE & NAT'L SEC. ALLIANCE, CYBER INTELLIGENCE: SETTING THE LANDSCAPE FOR AN EMERGING DISCIPLINE 7–9 (2011); 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); 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. 16, 2015, at A1; Michael Joseph Gross, *Silent War*, VANITY FAIR, July 2013, at 98; Nicole Perlroth, *Hunting for Syrian Hackers' Chain of Command*, N.Y. TIMES, May 18, 2013, at B1 (reporting on the difficulties of tracing hackers); Nathaniel Popper, *Wall Street's Exposure to Hacking Laid Bare*, N.Y. TIMES, July 26, 2013, at B1.

94. Nelson D. Schwartz, *Facing a New Type of Threat from WikiLeaks, a Bank Plays Defense*, N.Y. TIMES, Jan. 3, 2011, at B1.

95. *See* DAVE MARCUS & RYAN SHERSTOBITOFF, MCAFEE & GUARDIAN ANALYTICS, DISSECTING OPERATION HIGH ROLLER 3 (2012); Nicole Perlroth, *Attacks on 6 Banks Frustrate Customers*, N.Y. TIMES, Oct. 1, 2012, at B1; Nicole Perlroth & Quentin Hardy, *Bank Hacks Were Work of Iranians, Officials Say*, N.Y. TIMES, Jan. 9, 2013, at B1.

96. Amy Chozick & Nicole Perlroth, *Twitter Speaks, Markets Listen, and Fears Rise*, N.Y. TIMES, Apr. 29, 2013, at A1.

97. *See* FIREEYE, APT28: A WINDOW INTO RUSSIA'S CYBER ESPIONAGE OPERATIONS 3–6 (2014); Michael Riley, *How Russian Hackers Stole the NASDAQ*, BLOOMBERG BUS. WK., July 20, 2014, at 40.

98. *See* VENGERIK ET AL., *supra* note 88, at 3; Nicole Perlroth, *Web Thieves Using Lingo of Wall St.*, N.Y. TIMES, Dec. 2, 2014, at B1.

99. David E. Sanger & Nicole Perlroth, *Bank Hackers Steal Millions via Malware*, N.Y. TIMES, Feb. 15, 2015, at A1.

massive, international insider-trading scheme.[100] In 2016, the Society for Worldwide Interbank Financial Telecommunication (SWIFT), a critical intermediary in global finance, was hacked for over $80 million.[101]

In addition to the external threats posed by the new high-tech financial industry, financial firms must also safeguard against internal threats and vulnerabilities like rogue or misguided employees and independent contractors. IBM recently estimated that 95% of all data breaches involve human error.[102] Rogue employees and contractors with proper authorization comprise some of the most dangerous threats to financial firms in this technology-intensive era, as there are few safeguards against someone who is properly authenticated and authorized.[103] Edward Snowden, who carried out one of the largest releases of classified documents in history, was a NSA contractor with proper access and authorization.[104] Likewise, employees and contractors at financial firms pose significant potential threats in today's marketplace, because they can move millions of dollars seamlessly and quicker than the blink of an eye with a few clicks or keystrokes. [105] In 2008, a rogue trader at the illustrious French investment bank, Société Générale, nearly destroyed the firm with $69 billion in unauthorized positions over a period of several months.[106] In 2011, another rogue trader at UBS, the leading Swiss investment bank, caused $2.3 billion in losses.[107] More recently, in 2015, a Morgan Stanley financial advisor allegedly stole over 300,000 confidential client account records, which were later placed online for sale.[108] While these types of bad acts and bad actors existed in the past analog eras

100. *See* Criminal Indictment, United States v. Shalon, S1 15 Cr. 333 (S.D.N.Y. 2015); Criminal Indictment, United States v. Murgio, 15 Cr. 769, (S.D.N.Y. 2015); Matthew Goldstein & Alexandra Stevenson, *Rogue Traders, Brazen Hackers and a Wave of Arrests*, N.Y. TIMES, Aug. 12, 2015, at B1.

101. Megha Bahree, *Ex-Bangladesh Bank Chief Blames Global Transfer System for Theft*, N.Y. TIMES, June 23, 2016, at B5.

102. IBM GLOB. TECH. SERV., IBM SECURITY SERVICES 2014 CYBER SECURITY INTELLIGENCE INDEX (2015), http://media.scmagazine.com/documents/82/ibm_cyber_security_intelligenc_20450.pdf.

103. *See, e.g.*, Bambauer, *supra* note 87, at 1050 ("[I]t is not technologically possible to prevent those authorized to access data from misusing it[.]"); Steven R. Chabinsky, *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.

104. *See* GLENN GREENWALD, NO PLACE TO HIDE: EDWARD SNOWDEN, THE NSA, AND THE U.S. SURVEILLANCE STATE 9–10 (2014).

105. *See* Dune Lawrence, *Tracking the Enemy Within*, BLOOMBERG BUS. WK., Mar. 16, 2015, at 39 (reporting on the "insider threat" relating to cybersecurity from employees); *see also* MARK RUSSINOVICH, ROGUE CODE (2014) (depicting a fictional account of a rogue programmer causing global financial panic).

106. Nicola Clark, *Ex-Trader Gets 3 Years*, N.Y. TIMES, Oct. 6, 2010, at B1.

107. Julia Werdigier, *Revealing Details of Rouge Trades, UBS Raises Loss Estimate to $2.3 Billion*, N.Y. TIMES, Sept. 19, 2011, at B3.

108. Nathaniel Popper, *Breach Puts Morgan Data Up for Sale*, N.Y. TIMES, Jan. 6, 2015, at B1.

of finance, the new high-tech nature of finance renders these malfeasances more likely, more accelerated, more threatening, and more devastating.

In sum, the modern financial industry is essentially a technology industry. As such, it faces external and internal technological threats like those in the traditional technology industry. As financial technology grows more prevalent and sophisticated, the technological threats to financial firms will also grow more prevalent and sophisticated in the coming years.

III. KEY IMPLICATIONS

The rise of new financial technology and the compliance function, and its accompanying perils and promises, will have many important implications for the future of the financial industry. Three key implications are particularly noteworthy: the rising importance of financial cybersecurity, the closer integration of compliance and technology functions, and the human factor in the future of finance.

A. FINANCIAL CYBERSECURITY

Cybersecurity will be one of the most pressing challenges for the financial industry in the coming years. Part of what makes financial cybersecurity so challenging is the fact that the financial system operates in a largely privately held technological infrastructure, controlled by disparate financial intermediaries.[109] Because private financial firms control so much of the technological and cyber infrastructure in the United States, timely, coordinated, and security-enhancing actions could prove particularly difficult as businesses place short-term profits and other priorities, like secrecy, over financial cybersecurity.[110]For individual financial firms, deprioritizing cybersecurity investments may make sense in the short term, but this sensible myopia by individual firms could create greater cybersecurity risks for the entire industry.[111] Because of the linked and intermediated nature of modern finance, it is not enough for a firm to have strong financial cybersecurity; its vendors and counterparties also need to have strong financial cybersecurity

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

110. *See* STEWART BAKER ET AL., MCAFEE, IN THE CROSSFIRE: CRITICAL INFRASTRUCTURE IN THE AGE OF CYBER WAR 14 (2009); JOEL BRENNER, AMERICA THE VULNERABLE: INSIDE THE NEW THREAT MATRIX OF DIGITAL ESPIONAGE, CRIME, AND WARFARE 239 (2011) (highlighting under-spending on cybersecurity by businesses); Daniel Huang et al., *Financial Firms Bolster Cybersecurity Funds*, WALL ST. J., Nov. 17, 2014, at C3; Nicole Perlroth, *Hacked vs. Hackers: Game On*, N.Y. TIMES, Dec. 3, 2014, at F1; *see also* Tom C.W. Lin, *Executive Trade Secrets*, 87 NOTRE DAME L. REV. 911, 940–44 (2012) (describing the value of trade secrets to American businesses).

111. *See, e.g.*, Bambauer, *supra* note 87, 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.").

in order to better safeguard against the multitude of threats in the financial marketplace.

In order to better address the challenge of financial cybersecurity, the financial industry will likely witness more investments in this area and a greater push for better coordination among private and public actors. First, financial firms will likely make more investments in cybersecurity in the coming years. In 2014, JPMorgan alone "spent more than $250 million, and had approximately 1,000 people focused on cybersecurity efforts," and it expected significant growth in its cybersecurity spending in the years to come.[112] Many of JPMorgan's peer firms have similarly invested in cybersecurity, and many more will do so. While recent threats and attacks have led to greater awareness and investments in financial cybersecurity, much more will be necessary as the technological threats grow more prevalent and pernicious.[113] Furthermore, to the extent cybersecurity investments are made, they are often done in a reactionary manner following some major security breach—in response to the last threat, rather than in anticipation of the next threat. [114] As the financial industry becomes ever more dependent on technology, timely and thoughtful investment in financial cybersecurity becomes ever more important.

Second, because much of the technological infrastructure of the financial marketplace is privately held and operated, policymakers, regulators, and industry stakeholders will likely urge individual firms to work in a more concerted fashion with public and private actors to enhance financial cybersecurity.[115] Existing policies related to financial cybersecurity, like those contained in the 1998 Presidential Decision Directive 63 on Critical Infrastructure Protection and the Financial Services Modernization Act of 1999, will likely warrant more attention and better compliance.[116] Newer and

---

112. *See, e.g.*, JPMORGAN CHASE REPORT, *supra* note 21, at 142.

113. *See, e.g.*, FIN. INDUS. REGULATORY AUTH., REPORT ON CYBERSECURITY PRACTICES 4 (2015) [hereinafter CYBERSECURITY PRACTICES]; Nicole Perlroth & Elizabeth A. Harris, *Cyberattack Insurance a Challenge for Business*, N.Y. TIMES, June 9, 2014, at B1; Jessica Silver-Greenberg & Matthew Goldstein, *After Breach, Push to Close Security Gaps*, N.Y. TIMES, Oct. 22, 2014, at B1.

114. *See, e.g.*, Huang et al., *supra* note 110, at C3; Silver-Greenberg & Goldstein, *supra* note 113, at B1.

115. *See, e.g.*, HARRIS, *supra* note 93, at xxii ("Defending computer networks, and launching attacks on them, requires the participation, willing or otherwise, of the private sector."); Christopher S. Yoo, *Cyber Espionage or Cyberwar?: International Law, Domestic Law, and Self-Protective Measures*, *in* CYBERWAR: LAW & ETHICS FOR VIRTUAL CONFLICTS 192–93 (J. Ohlin et al. eds., 2015) (advocating for "improved software engineering"); Nathan Alexander Sales, *Regulating Cyber-Security*, 107 NW. L. REV. 1503, 1550–52 (2013) (discussing the use of incentives 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).

116. *See* Resolution Trust Corporation Completion Act, Pub. L. No. 103-204, 107 Stat. 2369 (1993) (codified as amended at 12 U.S.C. § 1811 (2012)); Gramm-Leach-Bliley Financial Modernization Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended at 15 U.S.C. § 6805 (2012)); Presidential Decision Directive 63 on Critical Infrastructure Protection: Sector Coordinators, 63 Fed. Reg. 41,804, 1998 WL 438395 (Aug. 5, 1998); Standards for

forthcoming regulatory efforts will also push firms to share more information among themselves and with the regulators. In 2011, the SEC issued non-binding guidance for companies to disclose cybersecurity risks.[117] In 2014, FINRA also recommended third-party penetration testing for financial firms as a way to assess their cybersecurity feasibility and vulnerability.[118] And in 2015, collectives of private firms created platforms, like Soltra and ThreatExchange, to share information about cyber-threats.[119] In the foreseeable future, there will likely be more regulation and coordinated actions of private and public actors relating to financial cybersecurity.

As technology and technological threats play larger roles in the operations of the financial industry, financial cybersecurity will inevitably become more and more salient to those working in the industry.

B. INTEGRATED COMPLIANCE AND TECHNOLOGY

Because of the concurrent rise of compliance and new financial technology, the compliance and technology functions at many financial firms will become more integrated, because both functions will become inextricably linked in the modern financial marketplace.[120] In order to be effective, compliance operations at many financial firms will need to better leverage the powers of new information technology, just as many firms have already done so in trading, investment, research, and other business-side operations.[121]

Compliance will grow more reliant on new information technology systems in response to regulatory and management pressures.[122] Modern financial firms are complex businesses operating in a very dynamic, complicated market and regulatory environment.[123] The deluge of data and regulations that compliance departments at financial institutions now oversee

---

Safeguarding Customer Information, 67 Fed. Reg. 36,493 (May 23, 2002) (codified at 16 C.F.R. §§ 314.1–.5 (2016)); FIN. SERVS. INFO. SHARING & ANALYSIS CTR., https://www.fsisac.com/ (last visited Feb. 26, 2016).

117. Div. of Corp. Fin., Sec. & Exch. Comm'n, *CF Disclosure Guidance: Topic No. 2, Cybersecurity*, U.S. SEC. & EXCHANGE COMMISSION (Oct. 13, 2011), https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

118. *See* CYBERSECURITY PRACTICES, *supra* note 113, at 34.

119. *See About*, FIN. SERVS. INFO. SHARING & ANALYSIS CTR., https://www.fsisac.com/CyberIntelligenceRepository (last visited Oct. 28, 2015); THREATEXCHANGE, https://threatexchange.fb.com (last visited Oct. 28, 2015).

120. *See supra* Part I.B for a discussion of marketplace complexity and the rise of compliance in the financial industry.

121. *See supra* Part I.A for a discussion of the rise of new financial technology.

122. *See Lessons Learned in Risk Management Oversight at Federal Financial Regulators: Hearing Before the Subcomm. on Sec., Ins., and Inv. of the S. Comm. on Banking, Hous., and Urban Affairs,* 111th Cong. 12 (2009) (statement of Roger T. Cole, Dir., Div. of Banking Supervision and Regulation, Bd. of Governors of the Fed. Reserve Sys.); Kenneth A. Bamberger, *Technologies of Compliance: Risk and Regulation in a Digital Age*, 88 TEX. L. REV. 669, 672 (2010).

123. Manuel A. Utset, *Complex Financial Institutions and Systemic Risk*, 45 GA. L. REV. 779, 797–801 (2011).

simply demands the monitoring, analytical, and processing power of new information technology.[124] Governance, risk, and compliance (GRC) technology systems are now standard tools at major financial institutions.[125] GRC systems allow compliance departments to automate and analyze large volumes of information related to risk management and regulatory reporting in a timely and efficient manner, which would otherwise be nearly impossible to replicate manually for firms with thousands of employees in offices around the world.[126] Good GRC systems allow financial firms to create more effective compliance practices from a regulatory perspective and more effective risk management practices from a management perspective.

At more and more financial firms in the near future, compliance strategy will be technology strategy, and technology strategy will be compliance strategy. Many financial firms already use their own technologists to build their compliance technology systems in-house, helping them monitor and supervise their operations.[127] Others use third-party GRC system providers, which are often leading tech companies like Microsoft, Oracle, and IBM. It has been estimated that corporate spending in GRC systems "will grow from $15.98 billion in 2015 to $31.77 billion by 2020."[128] For GRC systems in the financial industry, it was estimated that spending was around $2.6 billion in 2015.[129] In recent years, JPMorgan alone spent over $600 million annually on resources related to compliance technology.[130] This trend towards greater investment in compliance technology will likely continue for the foreseeable future. In the near future, if not so already, having a good compliance system at a financial firm will be synonymous with having a good information

124. *See* Bamberger, *supra* note 122, at 673 ("Given the scale and complexity of contemporary business institutions and the massive amount of information involved in corporate operations, the types of risk controls that regulation demands simply cannot function without the data collection, analyzing, and monitoring capacities of integrated computer technology.").

125. *See generally* DAVID CAU, DELOITTE, GOVERNANCE, RISK AND COMPLIANCE (GRC) SOFTWARE: BUSINESS NEEDS AND MARKET TRENDS, http://www2.deloitte.com/content/dam/Deloitte/lu/Documents/risk/lu_en_ins_governance-risk-compliance-software_05022014.pdf.

126. *See id.* at 31; Bamberger, *supra* note 122, at 687; Suzanne Dickson, *Compliance Automation: Software Tools Can Give Auditors More Insight Into the Controls and Policies Their Organization Needs to Meet Regulatory Mandates*, INTERNAL AUDITOR, Feb. 1, 2007, at 27 ("With so many different regulations to consider across an entire enterprise, it is nearly impossible to correlate business requirements with regulations and policies without an automated tool set.").

127. *See, e.g.*, Letter from Jamie Dimon, Chairman & Chief Exec. Officer, JP Morgan Chase to Fellow Sharholders 13 (Apr. 9, 2014), http://files.shareholder.com/downloads/ONE/1586573639x0x742267/e2efaf60-814f-430e-869e-6889ba3ec0ec/2013AR_Chairman-CEO_letter.pdf.

128. Rohan Salgarkar, *Enterprise Governance, Risk and Compliance Market Projected to $31.77 Billion by 2020*, WHATECH (June 20, 2015), http://www.whatech.com/market-research/financial-services/69453-enterprise-governance-risk-and-compliance-market-projected-to-31-77-billion-by-2020.

129. David Bannister, *Tabb: Capital Markets Compliance Spend Will Soar to $2.6 Billion This Year*, BANKING TECH. (June 15, 2015), http://www.bankingtech.com/327292/tabb-capital-markets-compliance-spend-will-soar-to-2-6-billion-this-year/.

130. Letter from Jamie Dimon, *supra* note 127, at 13.

technology system. And the tech savvy compliance officer will become one of the most valuable creatures in the modern financial ecosystem.

C. THE HUMAN FACTOR

The ascents of smart machines in finance and financial compliance naturally raise existential questions about the role of humans in the future of the financial industry, just as similar questions are being raised by technological advancement in other industries throughout the economy.[131] Yet upon further examination, one would likely conclude that the human factor will remain a critical ingredient in successful financial and compliance operations in the near future.

Smart machines powered by artificial intelligence undeniably are superior to humans based on a variety of measures. Smart machines do not suffer from the irrational "animal spirits" that move humans.[132] Smart machines have nearly perfect recall and memory. Smart machines using complex algorithms can process large volumes of data faster, more accurately, and more precisely than humans, yet do not tire nor require rest the way humans do. As such, it should be of little surprise that many tasks in the financial industry have been automated; smart machines have taken over the roles of many hardworking humans from eras past.[133]

The power, speed, accuracy, and efficiency of smart machines have led many in the financial industry and beyond to extol smart machines and their data-driven algorithms as antidotes to human folly, but such extolment is sometimes misguided.[134] While there is much to admire about artificially intelligent machines with their data-driven models, such admiration should also recognize the limitations of smart machines and their elegant models.[135] The financial crisis of 2008 precipitated so dramatically because high-powered computer models failed to properly account for the speed, consequences, and impact of a bursting housing market bubble.[136] To their

---

131. *See* JAMES BARRAT, OUR FINAL INVENTION: ARTIFICIAL INTELLIGENCE AND THE END OF THE HUMAN ERA 3–4 (2013); Ford, *supra* note 5, at 83–87.

132. *See generally* GEORGE A. AKERLOF & ROBERT J. SHILLER, ANIMAL SPIRITS: HOW HUMAN PSYCHOLOGY DRIVES THE ECONOMY, AND WHY IT MATTERS FOR GLOBAL CAPITALISM (2009).

133. *See, e.g.*, ERIK BRYNJOLFSSON & ANDREW MCAFEE, THE SECOND MACHINE AGE: WORK, PROGRESS AND PROSPERITY IN A TIME OF BRILLIANT TECHNOLOGIES 57–71 (2014); SHERRY TURKLE, ALONE TOGETHER: WHY WE EXPECT MORE FROM TECHNOLOGY AND LESS FROM EACH OTHER 279–81 (2011).

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

135. *See, e.g.*, JAMES OWEN WEATHERALL, THE PHYSICS OF WALL STREET: A BRIEF HISTORY OF PREDICTING THE UNPREDICTABLE 36–39 (2013); Lo & Mueller, *supra* note 3, at 21; Paul Krugman, *How Did Economists Get it So Wrong?*, N.Y. TIMES MAG., Sept. 6, 2009, at 2 ("[E]conomists, as a group, mistook beauty, clad in impressive-looking mathematics, for truth.").

136. *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?*, 5 J.

peril, too many institutions, regulators, and investors all placed too much faith and confidence in the elegant models of smart machines in the lead up to the financial crisis.[137] Uncertainty and risk in finance can never be perfectly modeled, reduced, or eliminated.[138] Despite all the advances in new financial technology and artificial intelligence, there exists no machine so smart that it flawlessly forecasts financial futures and economic risks in a world filled with flawed, whimsical, and random human actors.[139] After losing a large sum of money during the South Sea Bubble in 1720, Isaac Newton remarked: "I can calculate the motion of heavenly bodies but not the madness of people."[140]

Despite all the advances in new financial technology, smart machines still lack the judgment and sophistication of smart humans.[141] The human factor will likely remain the critical factor in financial operations in the foreseeable future. Machines, no matter how artificially intelligent, are still not as smart as humans (yet).[142] The human brain, with its billions of neurons and trillions of synaptic connections, remains one of the most sophisticated and powerful of all analytical machines.[143] Smart machines still require humans to create their initial operating systems and codes. Humans will need to serve as analog safeguards to the autonomous digital systems that have

---

INV. MGMT. 5, 5–9 (2007); Krugman, *supra* note 135, at 2 ("There was nothing in the prevailing models suggesting the possibility of the kind of collapse that happened last year.").

137. *See, e.g.*, Bamberger, *supra* note 122, at 705 (discussing the perils of over-reliance on compliance technology); Khandani & Lo, *supra* note 136, at 5–9; Tom C.W. Lin, *Too Big to Fail, Too Blind to See*, 80 MISS. L.J. 355, 371–73 (2010) (discussing the role of overconfidence in financial models in connection with the financial crisis); Joe Nocera, *Risk Management*, N.Y. TIMES MAG., Jan. 4, 2009, at MM24 (opining on the flawed prevailing risk models prior to the 2008 financial crisis).

138. *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 & Mueller, *supra* note 3, at 14.

139. *See* FRANK, *supra* note 138, 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 135, at 36–39; Kenneth A. Bamberger, *Regulation as Delegation: Private Firms, Decisionmaking, and Accountability in the Administrative State*, 56 DUKE L.J. 377, 430 (2006) (discussing the difficulties of managing risks at private firms); Lo & Mueller, *supra* note 3, at 21; Mark Whitehouse, *Economists' Grail: A Post-Crash Model*, WALL ST. J., Nov. 30, 2010, at A1 (reporting on the fallacies of financial models in light of the financial crisis of 2008).

140. PATTERSON, *supra* note 93, at 12 (internal quotation marks omitted).

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

142. *See* BRIAN CHRISTIAN, THE MOST HUMAN HUMAN: WHAT TALKING WITH COMPUTERS TEACHES US ABOUT WHAT IT MEANS TO BE ALIVE 5–10 (2011) (discussing the limitations of computerized communications with humans); CHRISTOPHER STEINER, AUTOMATE THIS: HOW ALGORITHMS CAME TO RULE OUR WORLD 5–6 (2012) (opining on the need for humans to manage algorithmic processes); John Markoff, *How Many Computers to Identify a Cat? 16,000*, N.Y. TIMES, June 26, 2012, at B1.

143. ELLEN E. PASTORINO & SUSANN M. DOYLE-PORTILLO, WHAT IS PSYCHOLOGY? 355 (2011).

grown so prevalent in finance and compliance.[144] Human interactions that implicate persuasion, empathy, culture, spirit, emotion, values, and other innate human characteristics remain key factors in any successful and effective legal and compliance practice.[145] Smart machines with their smart programs and smart models stand little chance against stupid human behavior. Many compliance officers, attorneys, and business executives in the financial industry can probably attest to that mismatch. Artificial intelligence is simply no match for natural stupidity. As such, in addition to greater investments in new financial technology, many financial firms in recent years are also aggressively hiring former spies and intelligence officers in connection with their compliance efforts to bolster their human compliance capabilities.[146]

This discussion about the limitations of smart machines is not intended to suggest that smart machines will not play a leading role in the future of law and compliance in the financial industry.[147] Smart machines, like those at the heart of many leading GRC systems, will undoubtedly continue to play an important role in the legal and compliance functions of finance, but they will not fully replace humans as functionaries. Rather, smart machines will complement smart lawyers and smart compliance officers in their work. Smart machines will likely be better suited for functions in areas where there are plainly defined rules that can be clearly, precisely, and predictably modeled and assessed.[148] Human actors, on the other hand, will likely be better suited for functions in areas where there are standards that require factual flexibility, contextual analysis, values assessments, and nuanced judgments that are not well suited for the rigidity of amoral machine thinking.[149] Since laws and policies governing financial firms involve both rules and standards, there will invariably be a place for both smart machines and smart humans in the future of finance. Just as law works better when

144. *See*, *e.g.*, David Sax, *State-of-the-Art Safeguards*, BLOOMBERG BUS. WK., Mar. 14, 2016, at 51 (discussing how human-operated analog mechanism can serve as great safeguards in the digital age).

145. *See*, *e.g.*, IAN AYRES, SUPER CRUNCHERS: WHY THINKING-BY-NUMBERS IS THE NEW WAY TO BE SMART 117 (2007) (discussing the role of human expertise in a data-driven world); DANIEL GOLEMAN, EMOTIONAL INTELLIGENCE: WHY IT CAN MATTER MORE THAN IQ 60–72 (1995) (explicating on the importance of emotional intelligence in human relationships); NEIL POSTMAN, TECHNOPOLY: THE SURRENDER OF CULTURE TO TECHNOLOGY 71–72 (1992).

146. Gavin Finch et al., *Ex-Spies Go Hunting For Rogue Traders*, BLOOMBERG BUS. WK., Feb. 22, 2016, at 40.

147. *See supra* Part III.B.

148. *See* Bamberger, *supra* note 122, at 676 ("Computer code . . . operates by means of on-off rules[.]"); Seana Valentine Shiffrin, *Inducing Moral Deliberation: On the Occasional Virtues of Fog*, 123 HARV. L. REV. 1214, 1214 (2010) (discussing the clear, predictable nature of rules).

149. *See, e.g.*, Russell B. Korobkin, *Behavioral Analysis and Legal Form: Rules vs. Standards Revisited*, 79 OR. L. REV. 23, 37–38 (2000); Antonin Scalia, *The Rule of Law as a Law of Rules*, 56 U. CHI. L. REV. 1175, 1178–79 (1989); Shiffrin, *supra* note 148, at 1222; Kathleen M. Sullivan, *The Justices of Rules and Standards*, 106 HARV. L. REV. 22, 26 (1993); Cass R. Sunstein, *Problems With Rules*, 83 CALIF. L. REV. 953, 991–92 (1995).

there are both rules and standards, it can be argued that the legal and compliance functions also work better when there are smart machines working with smart humans.[150]

Ultimately, the critical contests in the future of legal and compliance operations in the financial industry are not contests between humans and machines; instead they are contests about humans *with* machines.[151] The future of the legal and compliance functions in the financial industry is not about what smart machines are going to do to replace attorneys and compliance officers, rather it is about what attorneys and compliance officers are going to do with smart machines to create more lawful, more compliant, and more profitable institutions in the financial sector in the years to come.

CONCLUSION

A fundamental transformation is happening in the financial industry. The rise of new financial technology and compliance has dramatically changed the operations of financial firms. This Article offered an early perspective on this unfolding sea change. It examined the concurrent and intersecting ascents of new financial technology and compliance as well as the potential risks linked with their ascents. It also highlighted the larger implications of the changing financial landscape associated with the growing roles of new technology and compliance. In particular, it focused on the challenges of financial cybersecurity, the integration of technology and compliance, and the role of humans in the future of modern finance. In the end, this Article hopes to serve as a studied account for thinking anew about the future of compliance, technology, and modern finance.

150. *See* Yuval Feldman & Alon Harel, *Social Norms, Self-Interest and Ambiguity of Legal Norms: An Experimental Analysis of the Rule vs. Standard Dilemma*, 4 REV. L. & ECON. 81, 81 (2008) (suggesting the proper balance of legal standards and rules to symbiotically generate more better decision-making frameworks).

151. *See, e.g.*, Hugh Son & Laura J. Keller, *Tracking Traders' Emotions*, BLOOMBERG BUS. WK., Sept. 5, 2016, at 34 (discussing the use of biometric devices to improve human trading activity).