Compliance, Technology, and Modern Finance

Tom C.W. Lin

Follow this and additional works at: http://brooklynworks.brooklaw.edu/bjcfcl

Part of the Agency Commons, Banking and Finance Law Commons, Law and Society Commons, Legal Ethics and Professional Responsibility Commons, Legal Profession Commons, and the Science and Technology Law Commons

Recommended Citation
Available at: http://brooklynworks.brooklaw.edu/bjcfcl/vol11/iss1/6

This Article is brought to you for free and open access by BrooklynWorks. It has been accepted for inclusion in Brooklyn Journal of Corporate, Financial & Commercial Law by an authorized editor of BrooklynWorks. For more information, please contact matilda.garrido@brooklaw.edu.
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. 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.

* 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.

traders, bankers, and analysts.\textsuperscript{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.\textsuperscript{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.


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


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


instruments better, faster, and cheaper than their human counterparts in many instances.\textsuperscript{11} This is even true in the traditionally clubby market for corporate bonds.\textsuperscript{12} In terms of research, almost every significant financial institution utilizes smart machines.\textsuperscript{13} Many hedge funds use algorithmic programs to read newsfeeds, analyze market data, and spot investment opportunities.\textsuperscript{14} In terms of risk analysis, many financial institutions use artificially intelligent programs to analyze and manage risk for themselves and their clients.\textsuperscript{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.\textsuperscript{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.\textsuperscript{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.\textsuperscript{18} In fact, dark pools are the preferred trading platforms for many securities and financial instruments.\textsuperscript{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

\textsuperscript{11} See, e.g., Yesha Yadav, \textit{Algorithmic Trading Undermines Efficiency in Capital Markets}, 68 \textit{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.”).


\textsuperscript{17} Kolhatkar & Bhaktavatsalam, \textit{supra} note 15.


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


\(^{22}\) 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 NETOMICS 7 (2001); Wasik, supra note 20.


\(^{24}\) 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).


\(^{26}\) Pollman, supra note 3, at 193–201.

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.”).


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.\textsuperscript{33} Similarly, Sarbanes-Oxley requires firms to establish internal controls and procedures for their financial statements and disclosures.\textsuperscript{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.\textsuperscript{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.\textsuperscript{36} The Guidelines were introduced by the U.S. Sentencing Commission, which was created pursuant to the Sentencing Reform Act of 1984.\textsuperscript{37} The Guidelines serve as guidance for establishing penalties for federal law violations, including those involving corporations and other business entities.\textsuperscript{38} The Guidelines created a scoring system to help determine the penalties for federal offenses.\textsuperscript{39} Aggravating factors increase the number of points of an offender’s Culpability Score and thereby increase the severity of punishment.\textsuperscript{40} Conversely, mitigating factors decrease the offender’s points and thereby decrease the severity of punishment.\textsuperscript{41} An “effective compliance and ethics program” is considered a mitigating factor that decreases a corporate offender’s Culpability Score.\textsuperscript{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.\textsuperscript{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.\textsuperscript{44}

\begin{thebibliography}{9}
\addcontentsline{toc}{section}{References}
\bibitem{compliance}

\bibitem{SOx}

\bibitem{FINRA}

\bibitem{sentencing}
Martin, supra note 2, at 172.

\bibitem{crimecontrol}

\bibitem{sentencingguidelines}

\bibitem{federalguidelines}
U.S. SENTENCING GUIDELINES MANUAL § 8C2.5 (U.S. SENTENCING COMM’N 2013).

\bibitem{mitigating}
Id.

\bibitem{mitigatingfactors}
Id. § 8C2.5(f)(1).

\bibitem{effectivecompliance}

\bibitem{improvingpenalties}
See Martin, supra note 2, at 173; Griffith, supra note 29, at 2102.
\end{thebibliography}
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.\textsuperscript{45} The financial marketplace today is incredibly complex and filled with a diverse cast of players.\textsuperscript{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.\textsuperscript{47} This new, more complex marketplace has generated greater opportunities for profits as well as losses.\textsuperscript{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.\textsuperscript{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.\textsuperscript{50}

\textsuperscript{45} See Martin, \textit{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.”).


\textsuperscript{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. 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. 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). 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. Dodd-Frank’s “Volcker Rule” relating to risky proprietary trading alone is contained in 964 pages, including an 893-page preamble. 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. Due in large part to this regulatory pathology and the


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) (“[T]he 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.”).


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.

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.\textsuperscript{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.”\textsuperscript{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.\textsuperscript{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.\textsuperscript{61} Similarly, many other large financial institutions are investing more resources into compliance, and will likely continue to do so for the foreseeable future.\textsuperscript{62}

\section*{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.

\subsection*{A. NORMAL FINANCIAL ACCIDENTS \& SYSTEMIC RISKS}

The financial industry’s growing reliance on advanced technology could pose significant systemic risks for the financial system.\textsuperscript{63} Complex, high-tech

---

\begin{itemize}
\item \textsuperscript{60} See Martin, supra note 2, at 181 (“Companies, especially banks, are greatly increasing the size of their compliance departments.”).
\item \textsuperscript{61} JPMorgan Chase Report, supra note 21, at 12–13.
\item \textsuperscript{62} Martin, supra note 2, at 181–83.
\end{itemize}
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 &
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. In 2015, the temporary technical impairment of Bloomberg terminals caused significant strain on the global bond market, affecting billions of dollars in transactions. To be clear, Bloomberg is an information services provider with about 325,000 terminals used by financial traders, not a large financial banking institution. 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.

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. 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. 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).
75. Id.
76. Id.
speed is the fact that many of these programs are built on similar and interdependent codes.\textsuperscript{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.\textsuperscript{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.\textsuperscript{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.\textsuperscript{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.\textsuperscript{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.\textsuperscript{84}

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

\textsuperscript{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).

\textsuperscript{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.


\textsuperscript{82} Haldane, supra note 77, at 2.


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.\(^8\) The financial industry’s structural dependency on interconnected, computerized systems makes it vulnerable to many technological threats.\(^7\) Many significant crimes and aggressions against financial firms now involve computers as the weapons of choice and cyberspace as the preferred crime scene.\(^8\) 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.\(^9\) For many financial institutions, computer codes, proprietary software, confidential data, and other intellectual property represent some of their most valuable assets.\(^10\) 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.”\(^11\)

The emergence of the Internet of financial things is also the emergence of the Internet of financial threats.\(^12\) Financial firms today face diverse technological threats, both external and internal in nature. External threats include antagonists like foreign nations, competitors, hackers, cyber-

---


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.”).


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).


certain criminals, and cyber-mercenaries. 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. a year later, in 2012, large, coordinated cyberattacks, widely attributed to iran, targeted american and international financial institutions. 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. in 2014, it was reported that russian hackers infiltrated the nasdaq computer system. that same year, cyber-criminals hacked into the data systems of wall street firms to steal material, nonpublic information. in 2015, it was revealed that an international cyber-gang systemically robbed millions of dollars from over one hundred institutions around the world, 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. In 2016, the Society for Worldwide Interbank Financial Telecommunication (SWIFT), a critical intermediary in global finance, was hacked for over $80 million.

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. 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. Edward Snowden, who carried out one of the largest releases of classified documents in history, was a NSA contractor with proper access and authorization. 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. 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. In 2011, another rogue trader at UBS, the leading Swiss investment bank, caused $2.3 billion in losses. 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.

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.


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).


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. 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. 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. 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.


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.\footnote{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.\footnote{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.\footnote{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.\footnote{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.\footnote{116} Newer and

\begin{itemize}
\item \footnote{112}{See, e.g., JPMORGAN CHASE REPORT, supra note 21, at 142.}
\item \footnote{114}{See, e.g., Huang et al., supra note 110, at C3; Silver-Greenberg & Goldstein, supra note 113, at B1.}
\item \footnote{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).}
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. In 2014, FINRA also recommended third-party penetration testing for financial firms as a way to assess their cybersecurity feasibility and vulnerability. And in 2015, collectives of private firms created platforms, like Soltra and ThreatExchange, to share information about cyber-threats. 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. 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.

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


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


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.


simply demands the monitoring, analytical, and processing power of new information technology.\textsuperscript{124} Governance, risk, and compliance (GRC) technology systems are now standard tools at major financial institutions.\textsuperscript{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.\textsuperscript{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.\textsuperscript{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.”\textsuperscript{128} For GRC systems in the financial industry, it was estimated that spending was around $2.6 billion in 2015.\textsuperscript{129} In recent years, JPMorgan alone spent over $600 million annually on resources related to compliance technology.\textsuperscript{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

\textsuperscript{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.”).


\textsuperscript{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.”).

\textsuperscript{127} See, e.g., Letter from Jamie Dimon, Chairman & Chief Exec. Officer, JP Morgan Chase to Fellow Shareholders 13 (Apr. 9, 2014), http://files.shareholder.com/downloads/ONE/1586573639x0 x742267/e2efaf60-814f-430e-869e-6889ba3e00ec/2013AR_Chairman-CEO_letter.pdf.


\textsuperscript{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/.

\textsuperscript{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. 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. 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.

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. 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.

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.

---


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


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.

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).


147. See supra Part III.B.


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.\textsuperscript{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 \textit{with} machines.\textsuperscript{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.
