FINANCIAL REGULATION IN THE BITCOIN ERA

William Magnuson

TABLE OF CONTENTS

FINANCIAL REGULATION IN THE BITCOIN ERA

William Magnuson[*]

Abstract

The recent decade has witnessed an extraordinary degree of innovation in the financial sector. Developments in financial technology, computing power, and networking theory have allowed decentralized online platforms such as Bitcoin to introduce fundamental changes in the way that financial services are provided. While these innovations have been applauded by many as introducing a welcome degree of competition into a sector dominated by incumbents, they also create a set of challenges for current financial regulation. How do fiduciary standards apply to algorithms? How does online finance affect the behavior of investors? And more generally, how can regulators monitor and constrain the financial industry when it is increasingly run by autonomous, dispersed computer networks? This Article argues that current financial regulation is inadequate to address the unique problems presented by the rise of Bitcoin and other fintech industries. In particular, these innovations raise concerns about the ability of financial regulation to promote three inter-related financial goals: the efficient allocation of capital, the protection of consumers, and the prevention of systemic risk. These three goals, at the core of current approaches to financial regulation, are all challenged by fintech's defining feature: its reliance on disembodied institutions and complex algorithms for its functioning. These traits render the traditional tools used by regulators to discipline markets—substantive behavioral obligations, the threat of sanctions, and the constraining effect of reputation—largely ineffective. The Article concludes by proposing a set of principles to guide lawmakers in designing a more effective financial regulatory structure for the Bitcoin era.

[*] Associate Professor, Texas A&M University School of Law; J.D., Harvard Law School; M.A., Università di Padova; A.B., Princeton University. .

INTRODUCTION

The recent decade has witnessed an extraordinary degree of innovation in the financial sector. Upstart financial technology (or "fintech") firms have introduced a dizzying area of new financial products and services into the market. Online crowdfunding platforms such as Kickstarter and LendingClub have changed the way that companies and individuals raise capital. Digital robo-advisors have challenged the business models of investment advisors and asset managers alike. And, most emblematically, cryptocurrencies such as Bitcoin have emerged as viable alternatives to traditional national currencies. This new Bitcoin era, defined by the rapid proliferation of fintech firms into an ever broader array of industries, has altered the landscape of finance in fundamental ways.

Financial regulators across the world have recently started to take notice of these changes. Several regulators, such as the Securities Exchange Commission and the Office of the Comptroller in the United States, have issued white papers and sought comments on how, and whether, current regulations should apply to fintech companies.[1] Others have begun to crack down on fintech actors, finding that many of them fail to comply with existing financial rules.[2] Still others have created "regulatory sandboxes" for fintech firms, allowing them to operate under relaxed compliance regimes in order to encourage experimentation and innovation.[3] The diverse array of policy proposals and enforcement initiatives in recent months reflects, among other things, the great difficulty that regulators have had in fashioning appropriate regulatory responses to the rapid rise of the Bitcoin era.

This Article aims to fill that gap. It argues that fintech's unique model of finance raises concerns about the ability of regulators to achieve three essential goals of financial regulation: the efficient allocation of capital, the protection of consumers, and the prevention of systemic risk. Each of these goals is undermined by fintech's defining

---

[1] *See* SECURITIES EXCHANGE COMMISSION, INVESTOR BULLETIN: INITIAL COIN OFFERINGS (2017), available at https://www.sec.gov/oiea/investor-alerts-and-bulletins/ib_coinofferings; OFFICE OF THE COMPTROLLER OF THE CURRENCY, SUPPORTING RESPONSIBLE INNOVATION IN THE FEDERAL BANKING SYSTEM: AN OCC PERSPECTIVE (2016).

[2] *See* Chao Deng, *China's Interference on Bitcoin Tests Currency's Foundation*, WALL ST. J., Sept. 18, 2017.

[3] *See* Max Colchester & Rachel Witkowski, *U.K. Takes Novel Approach on Fintech*, WALL ST. J., Apr. 11, 2016; Michelle Chen & Michelle Price, *Hong Kong to Launch Banking Fintech "Sandbox" As Rivals Pull Ahead*, REUTERS, Sept. 6, 2016; Clare Dickinson, *Bank of England Gathers Minds for Fintech Salon*, FIN. NEWS, Mar. 17, 2017.

features—its reliance on disembodied institutions, complex algorithms, and frequent adaptation to provide an evolving set of financial services to consumers. These features render the conventional tools of financial regulators largely ineffective by increasing the cost of identifying, monitoring and sanctioning market participants. In order to resolve these problems, financial regulation must adopt new tools that are better designed to address the unique structure of fintech markets.

This Article makes three contributions to the literature on financial regulation. First, it identifies the key features of fintech firms that distinguish them from traditional financial institutions. Fintech industries tend to be typified by high levels of *diffusion*, in that market actors are small and dispersed rather than large and concentrated. Fintech industries tend to rely on high levels of *automation*, in that they rely on algorithms and big data for their essential functions. And fintech industries tend to demonstrate high frequencies of *adaptation*, in that they undergo significant structural transformations in response to changes in market conditions. Thus, an initial aim of the Article is to taxonomize the core features of the Bitcoin era and demonstrate how these features are different in important ways from traditional finance.

Second, the Article assesses the consequences of fintech's structure on the efficacy of current financial regulation. The Article argues that fintech's unique model of finance places pressure on, and indeed undermines, several core purposes of financial regulation. It may reduce the capacity of the financial sector to allocate capital efficiently within the economy. It may increase the likelihood that consumer protections will be weakened or evaded. And it raises a set of systemic risk concerns that are potentially more troubling than the "too big to fail" concerns that have motivated recent financial reform efforts. Thus, an additional aim of the Article is to demonstrate the existential difficulties that the Bitcoin era poses for financial regulation.

Third, the Article proposes a set of reforms aimed at creating a "law of fintech" that better addresses the particular features and risks of the Bitcoin era. It argues that the law of fintech should focus on three overriding priorities. First, regulators should adopt a set of *information forcing* rules requiring fintech actors to disseminate accurate and comprehensive information about fintech products. Second, regulators should adopt a set of *security forcing* rules requiring fintech firms to adopt cybersecurity procedures that match the level of idiosyncratic risk they present to consumers, investors and third parties. And third, regulators should establish a set of *tradeoff forcing* rules requiring fintech firms and government authorities alike to explicitly acknowledge the policy tradeoffs of their decisions.

This Article will proceed in four parts. Part I will describe the structure of fintech and the key innovations that the Bitcoin era has

brought to the financial sector. Part II will describe the ways that fintech's business model challenges conventional financial regulation's core goals. Part III will propose a set of benchmark principles that should guide future efforts to devise a law of fintech. Part IV will address a set of objections to the Article's central proposals.

I. THE STRUCTURE OF FINTECH

This Part argues that the fintech industry, while covering a wide array of financial services and encompassing a disparate group of actors, is characterized by three core features. First, the fintech sector is typified by a high degree of *diffusion*, that is, fintech actors tend to be small and dispersed rather than large and concentrated. Second, fintech firms tend to rely on algorithmic *automation* for many of their essential functions. Third, the fintech industry is typified by frequent and sudden bursts of *adaptation*. These three characteristics—diffusion, automation, and adaptation—allow fintech firms to compete with established financial institutions despite the presence of high barriers to entry in the market. And while the particular services offered by fintech firms vary significantly, from virtual currencies to robo-advice to e-payment services to crowdfunding, these key features remain central to their business models.

Before proceeding, it may be worthwhile as an initial matter to set forth the parameters of the discussion. While the term "fintech" has at times been used to describe any use of technology in finance,[4] this generic use of the term tends to obscure the categorical differences between recent developments in finance and previous generations of financial development. This Article will thus adopt a narrower definition of the field. Fintech will be used to refer to the new breed of companies and organizations that specialize in providing financial services through technologically-enabled mobile and online platforms.[5]

---

[4] *See* Tom C. W. Lin, *Infinite Financial Intermediation*, 50 WAKE FOREST L. REV. 643, 655-56 (2015) (arguing that "[t]his type of substitutive disintermediation is more superficial than substantive in nature" because "while [fintech] companies like Wealthfront have replaced human money managers with algorithmic programs, they have simply substituted a human intermediary with a computerized one"); Leslie Picker, *"Fintech" Loses Some of Its Attraction for Investors*, N.Y. TIMES, Apr. 6, 2016 (noting that "[e]ven industry leaders are divided over what separates a fintech company from a plain old financial services company that uses technology").

[5] Other efforts to define the field have reached similar conclusions. *See* OFFICE OF THE COMPTROLLER OF THE CURRENCY, SUPPORTING RESPONSIBLE INNOVATION IN THE FEDERAL BANKING SYSTEM: AN OCC PERSPECTIVE (2016); ECONOMIST, THE DISRUPTION OF BANKING 2 n.2 (defining fintech as "new entrants that use Internet-based and mobile technologies to create new or superior banking products"), available at https://www.eiuperspectives.economist.com/sites/default/files/EIU-

Fintech organizations rely on the internet, website, smartphones and other technologies to produce and deliver their financial services to consumers and investors. Thus, fintech captures a wide range of companies and technologies, from Bitcoin to Kickstarter to Venmo, all of which have inserted themselves into previously staid financial industries and created new methods for facilitating transactions.

A. *Diffusion*

In recent years, a number of scholars and policymakers have argued that the increasingly concentrated nature of the financial sector has created a number of serious risks for the economy.[6] These scholars have identified a set of related pathologies that have been created or exacerbated by the ever-increasing size and power of large Wall Street banks.[7] Perhaps the most common critique in this line of scholarship is that of the "too-big-to-fail" problem.[8] Too-big-to-fail generally refers

---

The%20disruption%20of%20banking_PDF_0.pdf; NATIONAL ECONOMIC COUNCIL, A FRAMEWORK FOR FINTECH 2 (2017), available at https://www.whitehouse.gov/blog/2017/01/13/framework-fintech (defining fintech as a "wide spectrum of technological innovations which impact a broad range of financial activities, including payments, investment management, capital raising, deposits and lending, insurance, regulatory compliance, and other activities in the financial services space").

[6] *See, e.g.*, Jeffrey N. Gordon & Christopher Muller, *Confronting Financial Crisis: Dodd-Frank's Dangers and the Case for a Systemic Emergency Insurance Fund*, 28 YALE J. REG. 151, 154-55 (2011); Prasad Krishnamurthy, *Regulating Capital*, 4 HARV. BUS. L. REV. 1, 1 (2014); Felix B. Chang, *The Systemic Risk Paradox: Banks and Clearinghouses Under Regulation*, 2014 COLUM. BUS. L. REV. 747, 747 (2014); Manuel Utset, *Complex Financial Institutions and Systemic Risk*, 45 GA. L. REV. 779 (2011); Edward R. Morrison, *Is The Bankruptcy Code an Adequate Mechanism for Resolving the Distress of Systemically Important Institutions?*, 82 TEMP. L. REV. 449 (2009); Kenneth Ayotte & David A. Steel, Jr., *Bankruptcy or Bailouts*, 35 J. CORP. L. 469 (2010); Michael C. Munger & Richard M. Salsman, *Is "Too Big to Fail" Too Big?*, 11 GEO. J. L. & PUB. POL'Y 433 (2013); Arthur E. Wilmarth, *The Dodd-Frank Act: A Flawed and Inadequate Response to the Too-Big-To-Fail Problem*, 89 ORE. L. REV. 951 (2011); David Zaring, *A Lack of Resolution*, 60 EMORY L.J. 97, 106 (2010);

[7] *See, e.g.*, Jonathan C. Lipson, *Against Regulatory Displacement: An Institutional Analysis of Financial Crises*, 17 U. PA. J. BUS. L. 673 (2015); Tom C.W. Lin, *The New Financial Industry*, 65 ALA. L. REV. 567 (2014).

[8] *See* ANDREW ROSS SORKIN, TOO BIG TO FAIL: THE INSIDE STORY OF HOW WALL STREET AND WASHINGTON FOUGHT TO SAVE THE FINANCIAL SYSTEM--AND THEMSELVES (2010); John Crawford, *Predicting Failure*, 7 VA. L. & BUS. REV. 171, 173 (2012); Zachary Gubler, *Regulating in the Shadows: Systemic Moral Hazard and the Problem of the Twenty-First Century Bank Run*, 63 ALA. L. REV. 253 (2012) Marcelo Dabos, *Too Big to Fail in the Banking Industry: A Survey*, in TOO BIG TO FAIL: POLICIES AND PRACTICE IN GOVERNMENT BAILOUTS 141 (2004).

to the belief that large banks have become so central to the health of the financial sector, and the economy more generally, that no rational government could allow them to go bankrupt.[9] This situation alone might not be problematic if it were not for its downstream behavioral effects on banks. Banks, aware of the implicit guarantee offered by national governments, felt free to engage in excessively risky behavior—such as making risky bets on the housing market and issuing complicated credit default swaps—a situation that eventually led to the financial crisis.[10] But the problems of concentration in the financial sector also created a set of other pathologies related to competition, information and conflicts of interest in the financial markets.[11]

Fintech, however, has largely defied this conventional understanding about the direction of financial markets and institutions towards increasingly concentrated markets. Fintech markets instead tend to be highly diffuse, spreading decisionmaking and power among a number of small, disparate actors. These actors have smaller sections of the market, focus on narrow industry areas, and often are made up of a number of nimble start-ups. The actors may be small fintech firms, individuals, or even computer servers. The diffusion of financial operations to a wide number of actors has important implications for the way that finance functions, and in many ways defies fundamental assumptions about financial markets. It also generates different categories of risks and benefits.

One particularly stark example of the diffusion of power in fintech markets is provided by the emergence of virtual currencies in recent years. Virtual currencies like Bitcoin and Ethereum have grown at precipitous rates over the last few years, both in terms of value and in their wider use, but their business model is based on the radical concept that currency need not be issued and controlled by a single actor.[12]

---

[9] *See* Steven L. Schwarcz, *Systemic Risk*, 97 GEO. L. J. 193 (2008); Hal S. Scott, *The Reduction of Systemic Risk in the United States Financial System*, 33 HARV. J.L. & PUB. POL'Y 671, 673 (2010).

[10] *See* John Crawford, *The Moral Hazard Paradox of Financial Safety Nets*, 25 CORNELL J. L. & PUB. POL'Y 95, 95 (2015); Viral V. Acharya, Deniz Anginer & A. Joseph Warburton, *The End of Market Discipline? Investor Expectations of Implicit State Guarantees*, Working Paper, June 12, 2016, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1961656.

[11] *See* Andrew F. Tuch, *Financial Conglomerates and Information Barriers*, 39 J. CORP. L. 563 (2014); Andrew F. Tuch, *The Fiduciary Dilemma in Large-Scale Organizations: A Comparative Analysis*, in RESEARCH HANDBOOK ON FIDUCIARY LAW (Andrew Gold & Gordon Smith, eds., 2017).

[12] *See* Kevin V. Tu & Michael W. Meredith, *Rethinking Virtual Currency Regulation in the Bitcoin Age*, 90 WASH. L. REV. 271 (2015); Carla L. Reyes, *Moving Beyond Bitcoin to an Endogenous Theory of Decentralized Ledger Technology Regulation: An Initial Proposal*, 61 VILL. L. REV. 191 (2016).

Bitcoin and ethereum currencies are not represented by physical bills or coins, and they are not backed by the authority of national governments.[13] Instead, they are based on blockchain technology that allows decentralized, peer-to-peer networks to register and confirm transactions in the currencies.[14] When an owner of Bitcoin transfers the currency to another party, this transaction is recorded on a public ledger, known as the blockchain.[15] Other users continuously download this ledger and thereby authenticate valid transactions.[16] The network of users forms a kind of distributed decisionmaker, and it relies for its functioning on the consensus of the community.[17] The users that provide the computing power to process these transactions are granted new currency as a reward for their contributions.[18] And while the currency is entirely "virtual," with no real-world counterparts, it can be used to purchase a wide variety of goods and services, and a large number of virtual currency exchanges have sprung up to facilitate these conversions.[19] Indeed, companies and individuals pay significant amounts of natural money, whether it be dollars, euros, or yen, to buy the virtual currencies. The value of Bitcoin has increased dramatically in recent months—the price for a single Bitcoin rose from $963 on January 1, 2017 to an all-time high of $20,089 in December 2017, an increase of nearly 2000% in less than a year. The rise in Ethereum has been even more staggering—the price of a single token of Ether rose from $7.98 on January 1, 2017 to $1,432 on January 13, 2018, an increase of more than 17800%.[20]

While the cryptocurrency industry is a particularly pronounced example of the phenomenon, diffusion is also typical of other fintech industries. Crowdfunding, for example, takes advantage of mobile and online platforms to allow companies seeking capital to access wide groups of investors.[21] Crowdfunding firms, while standing as the

---

[13] *See* EUR. CENT. BANK, VIRTUAL CURRENCY SCHEMES 5 (2012), available at http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf.

[14] *See* Jesse Yli-Huumo, Deokyoon Ko, Sujin Choi, Sooyong Park & Kari Smolander, *Where Is Current Research on Blockchain Technology?-A Systematic Review*, 10 PLOS ONE, e163477 (2016), available at http://journals.plos.org/plosone/article?id=10.1371/journal.pone.0163477.

[15] *See* Reyes, *supra* note 12, at 198

[16] *See id*. at 197-99.

[17] *See* THE ECON., *How Does Bitcoin Work?*, Apr. 11, 2013.

[18] *See* Tu & Meredith, *supra* note 12, at 283; PEDRO FRANCO, UNDERSTANDING BITCOIN: CRYPTOGRAPHY, ENGINEERING, AND ECONOMICS 101 (2015).

[19] *See* Nikolei M. Kaplanov, *Nerdy Money: Bitcoin, the Private Digital Currency, and the Case Against Its Regulation*, 25 LOY. CONSUMER L. REV. 111, 116 (2012).

[20] *See* WORLD COIN INDEX, BITCOIN AND ETHEREUM PRICE CHARTS, available at https://www.worldcoinindex.com.

[21] *See* Kathryn Judge, *The Future of Direct Finance: The Diverging Paths of Peer-*

intermediaries behind the platforms, tend to take a light hand in the process.[22] As a result, companies (and, more and more, individuals) seeking equity investments or loans can more or less directly tap willing markets.[23] Kickstarter, an early pioneer in the area, has emerged as a remarkably effective way for early stage companies to raise money for new projects.[24] It has developed a particular strength in the video game industry and other creative projects. Peer-to-peer lending firms, on the other hand, have specialized in connecting small businesses, startups, and individuals with large groups of parties willing to lend them money.[25] These firms, sometimes called "crowdlending" platforms, essentially crowdsource lending decisions, with borrowers submitting requests to a central database, and potential lenders reviewing the terms and rates and deciding whether to invest. While the platform firms perform some substantive roles, including verifying the identity of borrowers and providing basic background information about them, the actual lending decisions are made by large groups of outside investors, who may be individuals, companies, or more conventional banks.[26] This outsourcing of risk to large numbers of dispersed actors has contributed to a lowering of interest rates in a variety of markets, from auto loans to student loans to home mortgages.[27]

Thus, fintech markets tend to defy conventional understandings about the necessity of large, concentrated actors within finance. Most

---

to-Peer Lending and Kickstarter, 50 WAKE FOREST L. REV. 603 (2015); Donald C. Langevoort & Robert B. Thompson, *''Publicness" in Contemporary Securities Regulation After the JOBS Act*, 101 GEO. L.J. 337, 339 (2013); Joan MacLeod Heminway, *Crowdfunding and the Public/Private Divide in U.S. Securities Regulation*, 83 U. CIN. L. REV. 477 (2014); C. Steven Bradford, *Crowdfunding and the Federal Securities Law*, 2012 COLUM. BUS. L. REV. 1 (2012); Joan MacLeod Heminway, *What is a Security in the Crowdfunding Era?*, 7 OHIO ST. ENTRPREN. BUS. L.J. 335 (2012); Joan MacLeod Heminway & Shelden Ryan Hoffman, *Proceed at Your Peril: Crowdfunding and the Securities Act of 1933*, 78 TENN. L. REV. 879 (2011).

[22] *See* THE ECON., *Global Crowdfunding*, Apr. 4, 2015

[23] *See* FINANCIAL CONDUCT AUTHORITY, A REVIEW OF THE REGULATORY REGIME FOR CROWDFUNDING AND THE PROMOTION OF NON-READILY REALISABLE SECURITIES BY OTHER MEDIA 5 (2015); Christine Hurt, *Pricing Disintermediation: Crowdfunding and Online Auction IPOs*, 2015 U. ILL. L. REV. 217, 221 (2015).

[24] *See* Kickstarter, *Need Some Reward Ideas? Here Are 96 of Them*, available at https://www.kickstarter.com/blog/need-some-reward-ideas-here-are-96-of-them.

[25] *See* Judge, *supra* note 21, at 608-21; William S. Warren, *The Frontiers of Peer-to-Peer Lending: Thinking About a New Regulatory Approach*, 14 Duke L. & Tech. Rev. 298 (2016); Zachary Adams Mason, *Online Loans Across State Lines: Protecting Peer-to-Peer Lending Through the Exportation Doctrine*, 105 Geo. L. J. 217 (2016).

[26] *See* Judge, *supra* note 21, at 611.

[27] *See See* Robert Farrington, *The Rise of Peer to Peer Student Loans*, FORBES, Aug. 13, 2014; THE ECON., *Car Loans: New Engine*, May 7, 2016; Ben McLannahan, *Fintech Start-Ups Look to Build on US Mortgage Market Share*, FIN. TIMES, Nov. 24,

fintech companies are themselves small and narrowly focused. What is more, they tend to outsource decisionmaking to large numbers of other actors. By dispersing ever-growing aspects of decisionmaking to large numbers of actors, fintech capitalizes on one of its greatest advantages: its ability to connect widely dispersed groups for the purpose of facilitating low cost transactions.

B. *Automation*

In addition to high levels of diffusion, the fintech sector is also typified by high levels of automation. Fintech firms are heavily, indeed existentially, dependent on the technological infrastructure that underlies their systems. This infrastructure is based on advances in artificial intelligence,[28] big data,[29] machine learning,[30] and, more generally, algorithmic decisionmaking.[31] In all of these areas, fintech firms employ increasingly sophisticated mechanisms to allow financial transactions to be entered into at high speed and with minimal or no human input.[32]

The delegation of decisionmaking to computers has, of course, affected nearly every aspect of society today, and its consequences have been studied widely.[33] Its impact on finance can hardly be overstated. In recent years, advancements in computer science, the sophistication of algorithms, the increasing online presence of individuals, and the

---

2016.

[28] SCOTT PATTERSON, DARK POOLS: HIGH-SPEED TRADERS, A.I. BANDITS, AND THE THREAT TO THE GLOBAL FINANCIAL SYSTEM (2012).

[29] VIKTOR MAYER-SCHONBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK AND THINK (2013); Andrew McAfee & Erik Brynjolfsson, *Big Data: The Management Revolution*, HARV. BUS. REV., Oct. 2012, at 60–68

[30] *See* Harry Surden, *Machine Learning and Law*, 89 WASH. L. REV. 87 (2014); Cary Coglianese & David Lehr, *Regulating by Robot: Administrative Decision Making in the Machine-Learning Era*, 105 GEO. L. J. 1146 (2017).

[31] *See* Joshua A. Kroll et al., *Accountable Algorithms*, 165 U. PA. L. REV. 633 (2017); 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, 130–35 (2009); Lin, *supra* note 7, at 573-74; IRENE ALDRIDGE, HIGH-FREQUENCY TRADING: A PRACTICAL GUIDE TO ALGORITHMIC STRATEGIES AND TRADING SYSTEMS (2010).

[32] *See* Lin, *supra* note 7, at 573-74.

[33] *See* John O. McGinnis, *Accelerating AI*, 104 NW. U. L. REV. 1253 (2010); David C. Vladeck, *Machines Without Principals: Liability Rules and Artificial Intelligence*, 89 WASH. L. REV. 117, 121 (2014); Ryan Calo, *Robotics and the Lessons of Cyberlaw*, 103 CALIF. L. REV. 513 (2015); Matthew U. Scherer, *Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies*, 29 HARV. J. L. & TECH. 353 (2016).

ever-expanding amounts of information open and available on the internet have enabled a sea-change in the capabilities of computers to make real-world decisions.[34] These algorithms can in many ways outperform humans due to their ability to process larger amounts of information in short time spans.[35] Fintech firms, in turn, have premised their business models on extensive use of these technologies.

Take, for example, the investment advisor industry. The asset management industry has long prided itself on the importance and value of individualized and personal advice.[36] Brokers and investment advisers tout their ability to develop relationships with clients and create tailored investment strategies to meet their needs. But in recent years, a number of digital advisors have emerged that promise to improve investment results and reduce costs, all without the need for any human intervention at all. These "robo-advisors" deploy sophisticated algorithms to assess an individual investor's risk profile, time horizon, and other characteristics to fashion investment portfolios.[37] Potential investors simply go to the robo-advisor's internet site, fill out a simple questionnaire, and then can hand over control of their investments to the robo-advisor's algorithm. The algorithm can send out buy and sell orders, rebalance portfolios, and even respond to changing legal incentives, such as engaging in "tax harvesting" to reduce the investor's income taxes. Sites such as Wealthfront have seen enormous increases in the size of their assets under management.[38] These companies argue that their algorithms provide higher quality advice, with fewer conflicts, and with less chance for human error or emotion to skew investment decisions. They can make decisions faster and more reliably than

---

[34] *See* Yesha Yadav, *How Algorithmic Trading Undermines Efficiency in Capital Markets*, 68 VAND. L. REV. 1607, 1617-31 (2015); SCOTT PATTERSON, DARK POOLS: THE RISE OF THE MACHINE TRADERS AND THE RIGGING OF THE STOCK MARKET 322-35 (2013).

[35] *See* Frank J. Fabozzi et al., *High-Frequency Trading: Methodologies and Market Impact*, 19 REV. FUTURES MARKETS 7, 9-10 (2011).

[36] *See* Harvey Bines, *The Varieties of Investment Management Law*, 21 FORDHAM J. CORP. & FIN. L. 71 (2016); Ryan Sklar, *Hedges or Thickets: Protecting Investors From Hedge Fund Mangers' Conflicts of Interests*, 77 FORDHAM L. REV. 3251 (2009); Roberta S. Karmel, *The Challenge of Fiduciary Regulation: The Investment Advisers Act After Seventy-Five Years*, 10 BROOK. J. CORP. FIN. & COM. L. 405 (2016); Edward B. Rock, *Foxes and Hen Houses? Personal Trading by Mutual Fund Managers*, 73 WASH. U. L. Q. 1601 (1995); Arthur B. Laby, *Fiduciary Obligations of Broker-Dealers and Investment Advisers*, 55 VILL. L. REV. 701 (2010).

[37] *See* Tom Baker & Benedict G.C. Dellaert, *Regulating Robo Advice Across the Financial Services Industry*, 103 IOWA L. REV. (forthcoming 2017).

[38] In the period from 2012 to 2017, Wealthfront increased its assets under management from $700 million to $5 billion, an increase of 614%. *See* Andrew Meola, *Wealthfront Review 2017: Fees, Returns, Investing Services & Competitors*, BUSINESS INSIDER, Feb. 9, 2017.

human advisors.

Blockchain similarly relies on automation for its functions. Virtual currencies based on blockchain technology rely on distributed databases maintained by peer to peer networks.[39] Their core functioning is based on digital cryptography in order to ensure that they are reliable and transparent. These codes record transactions on the public ledger and allow networks of other computers to verify the validity of the transactions. While transactions in Bitcoin and Ethereum are sometimes initiated by individuals, they are increasingly handled by automated "bots" that facilitate the smooth functioning of the network.[40] Because there is no central administrator of the blockchain, this ecosystem can sometimes struggle to deal with unintended, or even illegal, uses of the technology. For example, in 2014, Mt. Gox, a Bitcoin exchange that at one point dominated the industry, accounting for 70% of worldwide Bitcoin transactions, collapsed when it was discovered that a hacker had exploited a software bug in Bitcoin to steal 744,000 bitcoins, an amount that represented 6% of all Bitcoins in circulation.[41]

The increasing sophistication of algorithms in financial markets has also allowed for the rise of a new field of investing, often referred to as "high frequency trading."[42] High frequency traders develop programs that automatically execute trades on the basis of market information.[43] These trading strategies rely on speed and automation to gain an advantage over their rivals. They can process information and make investment decisions based on that information much faster than any human could ever hope to do so—in some cases, the algorithms allow trading firms to purchase or sell securities in a matter of microseconds.[44] JP Morgan even reported that its newly-developed algorithms could analyze 12,000 commercial loan contracts in seconds, a task that it estimated would take lawyers and loan officers 360,000 hours to do.[45] High frequency trading has had dramatic effects on the

---

[39] *See* discussion *supra* Part I.A.

[40] *See* Kayla Matthews, *The Role of Trading Bots in the Cryptocurrency Market*, BITCOIN MAGAZINE, Aug. 7, 2017.

[41] *See* Robert McMillan, *The Inside Story of Mt. Gox, Bitcoin's $460 Million Disaster*, WIRED, Mar. 3, 2014.

[42] *See* Yesha Yadav, *The Failure of Liability in Modern Markets*, 102 VA. L. REV. 1031 (2016); Jeffrey MacIntosh, *High Frequency Traders: Angels or Devils?* 3-5 (C.D. Howe Institute Commentary No. 391, 2013); IOSCO TECHNICAL COMM., REGULATORY ISSUES RAISED BY THE IMPACT OF TECHNOLOGICAL CHANGES ON MARKET INTEGRITY AND EFFICIENCY: CONSULTATION REPORT 10 (July 2011).

[43] *See* Yesha Yadav, *How Algorithmic Trading Undermines Efficiency in Capital Markets*, 68 VAND. L. REV. 1607 (2015).

[44] *See* Chris Brummer & Yesha Yadav, *The Fintech Trilemma*, unpublished manuscript (2017) (manuscript on file with author).

[45] *See Machine Learning Promises to Shake Up Large Swathes of Finance*, THE

functioning of securities markets, speeding up the process of information diffusion and market adjustment.[46] It has also, more worrisomely, been blamed for creating or worsening market crashes, due to its reliance on pre-programmed algorithms that do not adjust to reflect unexpected market changes.[47]

The automation that underlies fintech contributes to market diffusion. Because the core functions of fintech firms are performed, not by humans, but by computers, algorithms, or networks, fintech firms do not need the scale and size that other financial institutions benefit from. Their business models are not premised on the same economies of scale that more traditional financial institutions do, and they do not need large, diversified employee bases. Instead, automation allows fintech firms to stay small and concentrate on narrow, targeted sectors of the financial industry.[48] Similarly, the diffuse nature of fintech markets encourages firms to automate ever greater portions of their services, integrating algorithms deeper into their businesses. Thus, fintech's diffusion and automation tend to complement and reinforce one another in important ways.

C. *Adaptation*

Finally, the fintech industry is also typified by high levels of adaptation. Adaptation, in this case, refers to the tendency of markets to change in response to external circumstances.[49] These changes may be as simple as shifting a company's target market or advertising strategy, or as fundamental as changing the structure of the business itself. Some changes are spurred by a recognition of flaws or failures in previous markets, while others are spurred by innovations that create entirely new markets. Regardless of the area, however, fintech markets have demonstrated a remarkable ability to adapt and change in light of new information. This adaptation has proven essential in the growth and spread of fintech into ever greater sectors of the financial industry,

---

ECONOMIST, May 25, 2017.

[46] *See* Yadav, *supra* note 43, at 1612.

[47] See STAFFS OF THE CFTC AND SEC, FINDINGS REGARDING THE EVENTS OF MAY 6, 2010 45 (2010), available at http://www.sec.gov/news/studies/2010/marketevents-report.pdf.

[48] *See* William Magnuson, *Regulating Fintech*, 71 VAND. L. REV. (forthcoming 2018).

[49] *See* Raymond E. Miles, Charles C. Snow, Alan D. Meyer & Henry J. Coleman, *Organizational Strategy, Structure, and Process*, 3 ACAD. MAN. REV. 546 (1978); Daryl O. McKee, P. Rajan Varadarajan & William M. Pride, *Strategic Adaptability and Firm Performance: A Market-Contingent Perspective*, 53 J. MARKTNG. 21 (1989); Bryan A ukase, *Strategic Type, Market Orientation, and the Balance Between Adaptability and Adaptation*, 45 J. Bus. Res. 147 (1999).

even while leading to high levels of volatility in several sectors.

Perhaps the best example of this adaptability comes from the world of virtual currency. The cryptocurrency market is remarkably segmented. Bitcoin, the most well-known virtual currency, had an aggregate value of nearly $45 billion in August 2017, but its success has led to criticisms of what some actors view as a flaw in the underlying programming: Bitcoin transactions can only be processed at a rate of seven transactions per second.[50] Believing that this problem would inhibit the currency's growth, a group of miners argued that the Bitcoin structure should be altered to increase the size of Bitcoin blocks and thus speed up transactions.[51] When other members of the community refused to approve the change, the Bitcoin network split into two versions, in a process known as a "fork."[52] As a result, Bitcoin suddenly adapted into two versions: one, the traditional one, with the same limits on the speed of the transaction, and another, named BitcoinCash, with additional flexibility on the size and speed of transactions.[53] This adaptation occurred swiftly—the time from the announcement of the fork to the completion of the fork was just a week—and efficiently—it required no new factories, equipment, or employees, just the consent of a sufficiently large group of miners.

But the adaptability of the cryptocurrency market is also evidenced by the remarkable spread of new forms of virtual currency based on alterations in blockchain technology. For example, the cryptocurrency Ethereum is based on the same basic blockchain programming as Bitcoin, but its creators inserted additional features aimed to make the currency better suited to be used as a basis for virtual contract, also known as "smart contracts."[54] These smart contracts utilize Ethereum technology to create a set of automated commands that serve to enforce contractual obligations, forcing parties to abide by the terms of their agreements.[55] The capabilities of Ethereum have proven useful to banks seeking to monitor their financial contracts, and in 2017, a consortium of banks including Microsoft and JP Morgan Chase, reached an agreement to create a computing system based on

---

[50] *See* Daniela Sonderegger, *A Regulatory and Economic Perplexity: Bitcoin Needs Just a Bit of Regulation*, 47 WASH. U. J.L. & POL'Y 175, 186 n.88 (2015).

[51] *See* Paul Vigna, *Bitcoin's Sectarian Battles Heat Up*, WALL ST. J., Oct. 25, 2017.

[52] *See* Nathaniel Popper, *Some Bitcoin Backers Are Defecting to Create a Rival Currency*, N.Y. TIMES, July 25, 2017.

[53] *Id*.

[54] *See* Paul Vigna, *Bitcoin Rival Ethereum Gains Traction*, WALL ST. J., June 20, 2016.

[55] *See* Reyes, *supra* note **Error! Bookmark not defined.**, at 200.

Ethereum.[56] When concerns arose about the lack of confidentiality in Bitcoin, a group of programmers launched yet another virtual currency, ZCash, promising complete anonymity for all transactions and participants.[57] Each of these variations of currency has received significant interest from consumers, and the speed at which they emerge in response to changing demand or new information would be unimaginable among national currencies. The introduction of the Euro in 1999, for example, to foster greater integration among members of the European Union, required decades of negotiations and planning.[58]

Similarly, the crowdlending industry has demonstrated a remarkable degree of adaptation in the face of new opportunities. The crowdlending sector was created on the basis of advancements in peer-to-peer technology.[59] These advancements made it easier and more convenient for individuals to transact over online platforms.[60] At the same time, with the spread of smartphones and internet commerce, consumers became more comfortable with the idea of buying and selling goods and services without ever seeing their counterparties.[61] Out of this confluence of factors, a number of crowdlending companies arose to facilitate consumer loans: peer-to-peer lending platforms such as Prosper began connecting small borrowers with individuals willing to lend money.[62] When these companies met with great success, the market quickly shifted to other sectors of the credit markets that were seen as faulty or malfunctioning. SoFi, for example, was formed in 2011 to focus on the student loan market, and initially it focused on connecting wealthy alumni from particular universities with current students at those universities that needed to fund their education.[63] Similarly, another set of peer-to-peer lending platforms, such as Funding Circle, were created to focus on small business loans, a sector of the market that traditional banks retreated from in the wake of the

---

[56] *See* Nathaniel Popper, *Business Giants to Announce Creation of a Computing System Based on Ethereum*, N.Y. TIMES, Feb. 27, 2017.

[57] *See* THE ECONOMIST, *Digital Money: Known Unknown*, Oct. 27, 2016; Nathaniel Popper, *ZCash, A Harder to Trace Virtual Currency, Generates Price Frenzy*, N.Y. TIMES, Oct. 31, 2016.

[58] *See* Jens Damman, *Paradise Lost: Can the European Union Expel Countries from the Eurobond?*, 49 VAND. J. TRANSNAT'L L. 693 (2016).

[59] *See* Elaine Moore & Tracy Alloway, *Peer-to-Peer Lending: The Wisdom of Crowds*, FINANCIAL TIMES., May 19, 2014.

[60] *See* Christine Hurt, *Pricing Disintermediation: Crowdfunding and Online Auction IPOs*, 2015 U. ILL. L. REV. 217, 221 (2015).

[61] *See id*.

[62] *See* Liz Moyer, *From Wall Street Banking, A New Wave of Fintech Investors*, N.Y. TIMES, Apr. 6, 2016.

[63] *See* Peter Rudegeair & Telis Demos, *Slump Might Turn Anti-Bank SoFi Into a Bank*, WALL ST. J., Jul. 12, 2016.

financial crisis.[64] In response to changing market conditions, including the risk tolerance of banks, crowdlending platforms have managed to transform the credit industry, lowering interest rates for borrowers, expanding access to credit to wider audiences, and giving investors diversified opportunities to invest their capital. The landscape of the crowdlending industry has shifted quickly, as entrepreneurs identified opportunities in new sectors and new strategies.

The ability of fintech markets to adapt and change in response to market demand gives fintech an advantage over more traditional financial institutions, which, for a number of reasons, tend to be slow to change their basic business models and assumptions. Fintech companies are small and nimble, and the price of entering new markets is low. They, thus, do not need to achieve the same extensive knowledge of the industry that financial intermediaries typically require. And because they do not have massive numbers of employees running their operations—the average virtual currency company in North America has just 12 employees[65]—they can easily communicate new strategies and business models without the need for costly transition periods, or the hiring of consulting firms.

But it is also important to note that the high level of adaptation found in fintech does not necessarily correspond with high levels of stability. In other words, the fact that the industry itself is highly adaptive does not mean that particular companies in the industry are especially resilient. If anything, the opposite appears to be true—fintech companies are notoriously volatile. The average life of a Bitcoin exchange is a mere 381 days.[66] Crowdlending platforms are similarly unstable. One study found that, in China, where there are approximately 3,900 crowdlending companies, over 1,200 had run into some form of major distress, ranging from frozen funds to complete cessation of operations.[67] An incredible 266 of those companies had CEOs that had fled the authorities, under accusations of fraud, corruption, and other crimes.[68] As will be described further below, this volatility should not be surprising, as the very adaptability of fintech contributes to its rapid change and upheaval.

Finally, the high levels of adaptation in fintech industries

---

[64] *See* THE ECONOMIST, *Crowdfunding: Cool, Man*, May 9, 2015.

[65] GARRICK HILEMAN & MICHAEL RAUCHS, GLOBAL CRYPTOCURRENCY BENCHMARKING STUDY 25 (2017).

[66] *See* Tyler Moore & Nicolas Christin, *Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk*, 7859 FIN. CRYPTOGRAPHY & DATA SECURITY 25 (2013).

[67] *See China's P2P Lending Boom: Taking Flight*, THE ECONOMIST, Jan. 23, 2016.

[68] *Id.*

strengthen, and are in turned strengthened by, fintech's other core features, its diffusion and its automation. The fact that fintech markets are dominated by small companies makes it easier for these markets to change—there are no dominant actors that can prevent market shifts that challenge their competitive position. Similarly, the fact that fintech industries are heavily automated makes it easier for these industries to expand or modify their businesses—the barriers to entry for new markets are lower when a company's underlying technology applies just as well to, say, auto loans as it does to mortgages. Conversely, the speed of adaptation and change in fintech has encouraged companies to stay small. Decisionmakers, after all, naturally hesitate to invest in large infrastructure projects or hire large numbers of employees when the demand for those projects or employees can swiftly disappear. And the speed at which fintech industries change and evolve puts ever greater weight on companies' ability to stay at the forefront of innovation in programming and automation.

II. FINTECH'S REGULATORY CHALLENGE

The rise of fintech in the recent decade has brought great change to the financial services industry. Where traditional financial markets were dominated by a small number of large actors, fintech markets are dominated by a large number of small ones. These markets are heavily dependent on automation and algorithmic decisionmaking for their proper functioning. And they tend to exhibit high rates of adaptation, constantly shifting and transforming in response to external information. These changes have the potential to provide significant benefits for the economy. They reduce the cost of transacting in finance, from raising capital to investing capital to spending capital. They reduce the risk of monopolistic behavior and abuses of dominant positions. And they expand access to the financial system to sectors that have traditionally been underserved or underbanked.

At the same time, fintech's structure raises a set of concerns about whether current legal regimes adequately guide and constrain financial markets.[69] These concerns can be usefully understood as related to the three core purposes of financial regulation: efficiency, fairness, and stability. First, fintech may reduce the financial sector's ability to efficiently allocate capital. Second, fintech may create greater opportunities for actors to take advantage of unsophisticated consumers. Third, fintech may create a set of systemic risks that threaten to affect

[69] *See* Rory Van Loo, *Making Innovation More Competitive: The Case of Fintech*, 65 UCLA L. REV. 232 (2018) (arguing that the structure of competition law has hindered innovations in financial technology); Yadav, *supra* note 43.

the broader economy. Each of these concerns is at the core of modern day financial regulation. Without a better understanding of how fintech threatens these goals, policymakers will struggle to fashion rules that appropriately address the unique risks of the industry.

A. *Efficient Allocation of Capital*

One of the core functions of the financial sector is to allocate resources towards their most efficient uses.[70] Those who possess capital are not always capable of deploying that capital well, and those that are capable of deploying capital do not always have the capital necessary to do so. Banks and other financial institutions fill this void, intermediating between capital owners and capital users. Thus, finance at its core is a method for ensuring that capital is allocated efficiently.[71] Banks take deposits from savers, and they then loan those deposits out to borrowers who need the money—perhaps for the purchase of equipment for a farm, or the launch of a new store for a small business. The decision about where capital is allocated is essential to the proper functioning of the broader economy.[72]

But financial markets do not always—or even ever—allocate capital optimally. They may, for example, overvalue companies that operate in trendy or fashionable sectors.[73] Conversely, they may undervalue small companies that do not have widespread media coverage.[74] They may discount the likelihood of events with low probabilities, and they may overweight the importance of events with high probabilities.[75] The root cause of these inefficiencies varies depending on the case, but it is often connected to market failures (such as the presence of monopolies) or behavioral irregularities (such as

---

[70] *See* Joseph E. Stiglitz, *The Allocation Role of the Stock Market: Pareto Optimality and Competition*, 36 J. FIN. 235, 235 (1981); EUGENE F. FAMA & MERTON H. MILLER, THE THEORY OF FINANCE 3-15 (1972); Eugene F. Fama, *Efficient Capital Markets: A Review of Theory and Empirical Work*, 25 J. FIN. 383, 383 (1970).

[71] *See* JOHN ARMOUR, DAN AWREY, PAUL DAVIES, LUCA ENRIQUES, JEFFREY N. GORDON, COLIN MAYER & JENNIFER PAYNE, PRINCIPLES OF FINANCIAL REGULATION 22-51 (2015).

[72] *Id*. at 26.

[73] *See* JASON ZWEIG, YOUR MONEY AND YOUR BRAIN: HOW THE NEW SCIENCE OF NEUROECONOMICS CAN HELP MAKE YOU RICH 8 (2008) (noting that "[d]uring 1998 and 1999, one group of stocks outperformed the rest of the technology industry by a scorching 63 percentage points—merely by changing their corporate names to include .com, .net, or internet").

[74] Mark Rubinstein, *Rational Markets: Yes or No? The Affirmative Case*, 57 FIN. ANALYSTS J. 15, 23-26 (May-June 2001).

[75] *See* NICHOLAS NASSIM TALEB, THE BLACK SWAN: THE IMPACT OF THE HIGHLY IMPROBABLE (2007).

overconfidence bias) in the industry.[76]

Fintech's great promise is that it reduces or eliminates many of the inefficiencies present in traditional financial markets. By eliminating costly intermediaries and reducing transaction costs, fintech allows financial participants to engage in a greater variety of transactions with fewer delays. By spreading market power among a larger number of smaller actors, fintech reduces concerns about harmful monopolistic behaviors. By automating decisionmaking, fintech minimizes the potential for cognitive biases to skew financial decisions. All of these features suggest that fintech will lead to greater efficiency in the financial sector.

But while the nature of fintech reduces a sub-set of efficiency-related concerns in the financial industry, it also exacerbates another sub-set of concerns. It is only natural, of course, that different markets will create different risks. But in the case of fintech, these concerns are particularly pronounced, and are likely to become only more so as fintech expands.

First, the disaggregation and diffusion of fintech markets increase the likelihood that public goods will be underprovided in the industry. It is perhaps counterintuitive that an increase in the number of actors in a market can reduce efficiency in the market—it is, after all, a commonplace that competition increases as the number of competitors increases.[77] But the large number of actors in fintech creates a different problem related, not to competition, but rather to cooperation. Diffuse markets are more likely to suffer from public goods problems.[78] Public goods, of course, refer to that category of goods that are non-rivalrous and non-excludible, in the sense that any one actor's consumption of the good does not reduce the ability of other actors to consume the good and

---

[76] *See* Stiglitz, *supra* note 70, at 387.

[77] *See, e.g.*, Louis Kaplow, *Market Share Thresholds: On the Conflation of Empirical Assessments and Legal Policy Judgments*, 7 J. COMP. L. & ECON. 243 (2011) (describing the use of market share thresholds for the determination of whether antitrust rules have been violated); William M. Landes & Richard A. Posner, Market Power in Antitrust Cases, 94 HARV. L. REV. 937, 937 (1981); David T. Scheffman & Mary Coleman, *Quantitative Analyses of Potential Competitive Effects from a Merger*, 12 GEO. MASON L. REV. 319 (2004) (discussing the theoretical basis for numerical analyses of market share for competition levels).

[78] *See, e.g.*, MANCUR OLSON, JR., THE LOGIC OF COLLECTIVE ACTION: PUBLIC GOODS AND THE THEORY OF GROUPS (1965); ELINOR OSTROM, GOVERNING THE COMMONS: THE EVOLUTION OF INSTITUTIONS FOR COLLECTIVE ACTION (1990) (describing the ways in which small groups resolve collective action problems that trouble larger groups); Elinor Ostrom, *Collective Action and the Evolution of Social Norms*, 14 J. ECON. PERSP. 137 (2000); Oliver Kim & Mark Walker, *The Free Rider Problem: Experimental Evidence*, 43 PUB. CHOICE 3 (1984).

no actor can be prevented from utilizing the good.[79] The paradigmatic examples of such goods are the environment and the national military—once these goods exist, everyone benefits from them. But public goods also exist in the financial industry. For example, the production of "best practices" guidelines related to cybersecurity or the dissemination of knowledge about how to promote a sound banking system both constitute public goods that may benefit society more generally.[80] The problem with public goods is that private markets tend to produce them at suboptimal rates.[81] These problems can sometimes be overcome in concentrated markets, where the actors are known to each other and can observe (and potentially sanction) the behavior of the others.[82] But in diffuse markets, where actors are dispersed and have few interactions with each other, the likelihood that collective action problems can be overcome decreases exponentially.[83] Fintech, of course, demonstrates all the traits of a diffuse market, and thus the likelihood that fintech actors will voluntarily produce public good-type resources is significantly lower than one would expect in traditional, more concentrated financial sectors.[84]

Second, fintech's reliance on automation and algorithmic decisionmaking may reduce efficiency in financial markets. Again, this point may seem counterintuitive: if we can have computers make decisions faster and more reliably than humans, one might expect that efficiency would increase in financial markets. But this may not always hold true in fintech. In particular, the delegation of decisionmaking to pre-programmed algorithms creates the possibility of "model risk."[85] Even the most sophisticated trading algorithms rely on simplified assumptions about the nature of markets and individuals. When these assumptions are proved wrong, or errors are made in the programs, the speed and automaticity of algorithmic decisionmaking makes the consequences potentially more harmful. In 2012, one high-frequency trader, the Knight Capital Group, lost $440 million in just 45 minutes due to the failure of a technician to include new code in one of the firm's servers.[86] Several studies have shown that the rise of high-frequency

---

[79] *See* Olson, *supra* note 78, at 132-34.

[80] *See* Richard K. Gordon, *On the Use and Abuse of Standards for Law: Global Governance and Offshore Financial Centers*, 88 N.C. L. Rev. 501, 508 (2010); Elaine M. Sedenberg & Deirdre K. Mulligan, *Public Health as a Model for Cybersecurity Information Sharing*, 30 BERKELEY TECH. L. J. 1687 (2015).

[81] *See* OLSON, *supra* note 78, at 132-34.

[82] *See id.*; Ostrom, *supra* note 78, at 149.

[83] *See* OLSON, *supra* note 78, at 132-34.

[84] *Id.*

[85] *See* Yadav, *supra* note 43, at 1647-52.

[86] *See* Nathaniel Popper, *Knight Capital Says Trading Glitch Cost It $440 Million*, N.Y. TIMES, Aug. 2, 2012.

algorithmic trading has led to increases in volatility in stock markets.[87] One study identified 18,520 "ultrafast extreme events" in financial markets from the years 2006-2011, and found a close correlation between the proliferation of such events and system-wide financial collapse.[88] Automation also may reduce allocative efficiency by increasing herd behavior.[89] This may occur in several different ways, but perhaps the simplest involves computer programs sharing certain programming templates. If an algorithm proves successful in the market, other actors may be tempted to simply copy or replicate the algorithm. If they do, then the inaccuracies and flawed assumption of a single model may be propagated throughout the system, thereby significantly increasing the chance of financial contagion or other inefficient behaviors.[90]

---

[87] *See, e.g.*, Neil Johnson et al., *Abrupt Rise of Machine Ecology Beyond Human Response Time*, NATURE SCIENTIFIC REPORTS (Sept. 11, 2013), http://www.nature.com/articles/srep02627; Frank Zhang, *High-Frequency Trading, Stock Volatility, and Price Discovery* (Dec. 2010) (unpublished manuscript), http://ssrn.com/abstract=1691679.

[88] *See* Neil Johnson et al., *Abrupt Rise of Machine Ecology Beyond Human Response Time*, NATURE SCIENTIFIC REPORTS (Sept. 11, 2013), http://www.nature.com/articles/srep02627.

[89] *See* David Scharfstein & Jeremy Stein, *Herd Behavior and Investment*, 80 AMER. ECON. REV. 465 (1990); Marcel Kahan & Michael Klausner, *Path Dependence in Corporate Contracting: Increasing Returns, Herd Behavior and Cognitive Biases*, 74 WASH. U. L. QU. 347, 356 (1996).

[90] For a discussion of such model risks, see Toshiyasu Kato & Toshinao Yoshiba, *Model Risk and its Control*, 18 MONETARY & ECON. STUD. 129 (2000). Herd behavior risk is only exacerbated when the particular action, while beneficial when taken by a single actor, becomes harmful when taken by large numbers of actors. The rise of index investing, a staple of robo-advising companies, may prove to be one such phenomenon. The strategy of passively investing in a broad index of the market as a whole, rather than actively choosing stocks that are expected to outperform the market, has grown steadily more popular in recent years, with passive mutual funds and exchange traded funds increasing their share of S&P 500 companies from 4.6% to 11.6% in the period from 2005 to 2016. *See* Tom McGinty, Sarah Krouse & Elliot Bentley, *Index Funds Are Taking Over the S&P 500*, WALL ST. J., Oct. 17, 2016. A number of studies have concluded that the passive strategy, on average, outperforms active stock management, at least partially because it costs less. But the rise of index investing also raises concerns about whether stocks will continue to respond to market signals.[90] In other words, if all investors adopt an index approach, then all stocks would be purchased by all buyers. It would not matter if a company had a bad earnings report or just launched a new drug—if the company is part of the index, the investor is obligated to own it. Some companies have more than 30% of their stock owned by passive funds, with one company, Meredith Corp. having an incredible 39.7% of its shares controlled by such funds. *See* Chris Dieterich & Corrie Driebusch, *Wall Street's Newest Puzzle: What Passive Buying and Selling Means for Individual Stocks*, WALL ST. J., Sep. 21, 2017. Thus, while index investing as a strategy functions on an individual investor level, it may lead to dysfunctions in markets if it is adopted more widely.

Finally, the speed of adaptation and change in fintech may also have negative effects on the efficient allocation of capital. With new fintech companies and innovations arising or disappearing seemingly every day, the problem of asymmetric information between market participants becomes severe.[91] Asymmetric information generally refers to the imbalance of information between insiders, who have direct access to information about the benefits and risks of particular products or industries, and outsiders, who lack such information.[92] Asymmetric information can lead to market failure if insiders are able to extract rent from outsiders or, alternatively, if outsiders refrain from entering into the market at all.[93] In either case, the result is an inefficient market.[94] Information asymmetries tend to erode over time, however, as information about the market and its participants eventually spreads to broader audiences.[95] But because fintech has a tendency to adapt and change so quickly, outsiders often do not have sufficient time to resolve information asymmetry problems. Cryptocurrencies, and in particular the rise of "initial coin offerings," provide a good example of this problem.[96] New cryptocurrency is built on different underlying infrastructure, different programming, and different decisionmaking procedures. Outsiders that are considering investing in initial coin offerings thus must learn of the currency, attempt to understand its fundamental risk-reward structure, and then decide whether to invest in it. This process is extraordinarily complex and difficult, and investors may well resort to heuristics, rather than reasoned analysis, in order to resolve it.[97] Even if outsiders manage to overcome the information

---

[91] *See* Joseph Stiglitz, *The Contributions of the Economics of Information to Twentieth Century Economics*, 115 Q. J. ECON. 1441 (2000); Pierre Barbaroux, *From Market Failures to Market Opportunities: Managing Innovation Under Asymmetric Information*, 3 J. INNOV. & ENT. 5 (2015).

[92] *See* Stiglitz, *supra* note 91, at 1441.

[93] *See* George Akerlof, *The Market for "Lemons": Quality Uncertainty and the Market Mechanism*, 84 Q.J. ECON. 488 (1970).

[94] *See* Stiglitz, *supra* note 92, at 1445.

[95] *See* Barbaroux, *supra* note 92.

[96] For the Securities Exchange Commission's opinion on initial coin offerings, see SECURITIES EXCHANGE COMMISSION, INVESTOR BULLETIN: INITIAL COIN OFFERINGS (2017), available at https://www.sec.gov/oiea/investor-alerts-and-bulletins/ib_coinofferings.

[97] On the difficulties of assessing the value of initial coin offerings, the New York Times recently offered the following assessment: "Imagine that a friend is building a casino and asks you to invest. In exchange, you get chips that can be used at the casino's tables once it's finished. Now imagine that the value of the chips isn't fixed, and will instead fluctuate depending on the popularity of the casino, the number of other gamblers and the regulatory environment for casinos. Oh, and instead of a friend, imagine it's a stranger on the internet who might be using a fake name, who might not actually know how to build a casino, and whom you probably can't sue for fraud if he

asymmetry problem, the process itself is costly: each new venture or innovation requires outsiders to devote time and resources to the learning process.[98] The learning benefits that come from well-established markets with repeated interactions and observed behaviors are thus noticeably absent in many fintech markets.

For all these reasons, fintech raises a set of concerns about the efficient allocation of capital through financial markets. Fintech may lead to markets that underproduce social goods such as best practices on cybersecurity or sound banking procedures. It may lead to more volatile markets that fail to respond appropriately to new information. And it may lead to markets in which informational asymmetries impede informed bargaining. These concerns suggest that regulation will need to adjust to improve the efficiency of fintech markets.

B. *Consumer Protection*

In addition to efficiency, financial regulation is also concerned with ensuring fairness in financial markets.[99] Financial reform efforts have often been driven by a belief that consumers or investors require greater protections than are available in a purely deregulated environment. The perceived abuses and frauds perpetrated in the 1920s, for example, led to the introduction of the Securities Act and the Securities Exchange Act, which increased the disclosure and reliability of securities issued to the public.[100] The corporate and accounting scandals of the early 2000s led to the enactment of the Sarbanes Oxley Act, which required greater internal reporting and audit obligations for companies listed on the stock exchange.[101] And perceived abuses in the mortgage and credit industries in the late 2000s led to the creation of the Consumer Finance Protection Bureau in 2011.[102] In each of these

---

steals your money and uses it to buy a Porsche instead. That's an I.C.O." Kevin Rose, *Is There a Cryptocurrency Bubble?*, N.Y. TIMES, Sept. 15, 2017.

[98] *See* Akerlof, *supra* note 93, at 489.

[99] *See* Oren Bar-Gill & Elizabeth Warren, *Making Credit Safer*, 157 U. PA. L. REV. 1, 6 (2008) (arguing that "for a growing number of families that are steered into overpriced and misleading credit products . . . credit products benefit only the lenders").

[100] *See* RALPH F. DE BEDTS, THE NEW DEAL'S SEC 1-85 (1964); JOSEPH P. LASH, DEALERS AND DREAMERS: A NEW LOOK AT THE NEW DEAL 137-71 (1988); FERDINAND PECORA, WALL STREET UNDER OATH (1968); James M. Landis, *The Legislative History of the Securities Act of 1933*, 28 GEO. WASH. L. REV. 29 (1959)

[101] *See* Roberta Romano, *The Sarbanes-Oxley Act and the Making of Quack Corporate Governance*, 114 YALE L.J. 1521 (2005).

[102] *See* Leonard J. Kennedy, Patricia A. McCoy & Ethan Bernstein, *The Consumer Financial Protection Bureau: Financial Regulation for the Twenty-First Century*, 97 CORNELL L. REV. 1141 (2012).

instances, legislators have sought to protect investors and consumers in financial transactions from being treated in ways that violate a fundamental sense of fairness, even when these transactions may be entered into willingly.

It is unsurprising that fintech raises a number of consumer protection concerns. Innovation always raises questions about how old law applies to new circumstances. Lawmakers can never foresee the infinite variety of ways in which companies and individuals can act, and the very structure of law can shape the way that businesses develop. Many of the consumer protection concerns surrounding fintech are also present in more traditional financial services industries, but are only heightened in the fintech context. Others are entirely unique to the fintech industry. This Part will highlight the key categories of consumer protection risk in fintech and identify the ways in which these risks are heightened in fintech industries.

First and foremost, fintech presents important privacy concerns for consumers. Fintech firms, after all, often rely on consumers providing them with access to significant amounts of sensitive personal and financial information.[103] Personal finance companies like Mint, for example, request that users grant them access to view their bank account and retirement account information.[104] Online payment companies require authorization to transfer money from one account to another.[105] Traditional banks have raised concerns about granting computers access to personal accounts, but they have been rebuked by the Consumer Financial Protection Bureau for limiting precisely this sort of access.[106] At the same time, more and more fintech firms are gaining access to broad and deep information about individuals and their financial and personal lives. As more firms have access to, and control over, such information, the risk of public exposure through hacking or otherwise increases.[107] While consumers (in some cases) turn over this information willingly, they may well not fully understand the

---

[103] *See* Dina Moussa, *Protecting Payment Privacy: Reconciling Financial Technology and the Fourth Amendment*, 1 GEO. L. TECH. REV. 339 (2017).

[104] *See* Nathaniel Popper, *Banks and Tech Firms Battle Over Something Akin to Gold: Your Data*, N.Y. TIMES, Mar. 23, 2017.

[105] *Id*.

[106] In the European Union, regulators have gone even further in demanding that traditional banks open themselves up to competition from fintech firms. In 2018, the EU's new Payment Services Directive went into effect, requiring banks to cooperate with fintech firms seeking access to customer account data and payment services. *See* THE ECONOMIST, *Europe's Banks Face a Glut of New Rules*, Nov. 30, 2017.

[107] *See* Michael Murphy & John Barton, *From a Sea of Data to Actionable Insights: Big Data and What It Means for Lawyers*, 26 Intell. Prop. & Tech. L.J. 8, 12–13 (2014); Sasha Romanosky et al., *Empirical Analysis of Data Breach Litigation*, 11 J. Emp. Leg. Stud. 74, 74–75 (2014).

vulnerabilities of the firms to which they are turning it over. This will put further pressure on cybersecurity and privacy law to fulfill their mandate of protecting confidential information from disclosure or improper use.

Second, one of fintech's greatest advantages—its speed and ease of use—also creates concerns about whether consumers will enter into financially significant transactions on an uninformed basis. Fintech firms pride themselves on how convenient and easy it is to access their services: Sindeo, a San-Francisco based firm that specializes in home mortgages, promises on its website that prospective homeowners can "shop more than one thousand loans in just 5 minutes."[108] But the elimination of the barriers that have long stood between consumers and complicated financial products may have the less desirable effect of causing significant financial decisions to be made on the basis of snap judgments.[109] One need only consider the irrational exuberance surrounding recent initial coin offerings, described above, to understand the scope of the problem.[110] Similarly, fintech reduces the capacity for intermediaries, such as banks and brokers, to fulfill their gatekeeping function in financial markets. In the crowdlending industry, for example, borrowers are directly connected with lenders, and banks often play little or no role in the process. While this structure may reduce costs, it also eliminates the ability of banks to serve as gatekeepers and block bad actors from entering the market.[111] While banks certainly do not always fulfill this function perfectly, they are generally viewed as having a reputational interest in preventing abusive or unfair products from being marketed.[112] The removal of intermediaries from financial services, one of the professed goals of many fintech firms, thus may serve to reduce the quality of financial services on the market.

---

[108] Sindeo.com, accessed October 1, 2017.

[109] *See* Amos Tversky & Daniel Kahneman, *Judgment Under Uncertainty: Heuristics and Biases*, 185 SCIENCE 1124 (1974) (describing the various biases that affect decisionmaking under conditions of uncertainty); DANIEL KAHNEMAN, THINKING, FAST AND SLOW 105 (2011); Daniel Kahneman & Shane Frederick, *Representativeness Revisited: Attribute Substitution in Intuitive Judgment*, in HEURISTICS AND BIASES 49 (Thomas Gilovich et al. eds., 2002).

[110] *See* THE ECONOMIST, *The Market in Initial Coin Offerings Risks Becoming a Bubble*, Apr. 27, 2017.

[111] For a description of the gatekeeping role of financial intermediaries, see Elisabeth de Fontenay, *Private Equity Firms as Gatekeepers*, 33 REV. BANKING & FIN. L. 115 (2013); Stephen Choi, *Market Lessons for Gatekeepers*, 92 NW. U. L. REV. 916, 918 (1998); Reinier H. Kraakman, *Gatekeepers: The Anatomy of a Third-Party Enforcement Strategy*, 2 J.L. ECON. & ORG. 53, 54 (1986); John C. Coffee, Jr., *Gatekeeper Failure and Reform: The Challenge of Fashioning Relevant Reforms*, 84 B.U. L. REV. 301, 309 (2004); Andrew F. Tuch, *Multiple Gatekeepers*, 96 VA. L. REV. 1583 (2010).

[112] *See* de Fontenay, *supra* note 112, at 119.

Third, fintech's widespread use of anonymous online transactions likely attracts greater levels of crime and fraud to the sector. Anonymity, in this case, does not refer solely to the formal anonymity granted by some virtual currencies. It also covers other financial services that can be purchased and sold through online portals without the intervention of humans. Robo-advisors, for example, typically never meet their customers and channel all interactions through their online sites.[113] Crowdfunding platforms allow businesses and individuals to raise money without ever meeting their investors, or, for that matter, the platform itself.[114] But surely one of the more worrying developments in fintech has been the use of virtual currencies as the medium of choice for criminals. In the "Wannacry" ransomware attack that affected hundreds of thousands of computers worldwide in 2017, hackers managed to freeze access for computer owners to their computers, and, in order to unfreeze it, users had to send a certain amount of bitcoin, typically around $300, to a specific bitcoin account.[115] Adding to the difficulty of tracking the ransom money, the hackers are suspected to have converted the bitcoin into another virtual currency, Monero, which is widely believed to be even more secure and anonymous than bitcoin.[116] Similarly, bitcoin was the currency of choice for The Silk Road, a dark web online site that was notorious for trafficking in drugs.[117] If fintech allows criminals and fraudsters to evade national regulations, it could well cause significant harm to consumers.

Finally, fintech's use of "big data" strategies may lead to hidden discrimination, intentional or not, within the financial services industry.[118] While computers are not subject to the errors and biases of humans, they are only as effective as the algorithms that underlie their outputs.[119] To the extent that those algorithms incorporate inputs that

---

[113] *See* WALL STREET J, *Can Robo Advisors Replace Human Financial Advisors*, Feb. 28, 2016, https://www.wsj.com/articles/can-robo-advisers-replace-human-financial-advisers-1456715553.

[114] *See* Dale A. Oesterle, *Intermediaries in Internet Offerings: The Future Is Here*, 50 WAKE FOREST L. REV. 533 (2015).

[115] *See* Nicole Perlroth, Mark Scott & Sheera Frenkel, *Cyberattack Hits Ukraine Then Spreads Internationally*, N.Y. TIMES, June 27, 2017.

[116] *See* Ryan Browne, *Hackers Have Cashed Out on $143,000 of Bitcoin from the Massive WannaCry Ransomware Attack*, CNBC, Aug. 3, 2017; Sean Gallagher, *Researchers Say WannCry Operator Moved Bitcoins to "Untraceable" Monero*, ARS TECHNICA, Aug. 4, 2017.

[117] *See* Ben Tarnoff, *The Dark Web's Dark Prince*, WALL STREET J., June 12, 2017.

[118] *See* Salon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CAL. L. REV. 671 (2016).

[119] *See* EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES,

either explicitly discriminate between users on the basis of protected traits or are closely correlated with those traits, they may lead to pernicious bias and discrimination, and in ways that are more difficult to discover.[120] One could imagine, for example, that "big data" analytics could conclude that residents of certain zip codes were better, or worse, credit risks, and thus assign them better or worse interest rates based on that information. If these zip codes were closely correlated with race, or religion, or national origin, then the increasing use of such algorithms could lead to problematic discriminatory effects. And the presence of such correlations might well themselves only reflect past discrimination, leading to a self-justifying furtherance of biased means and ends in finance. Even determining whether such discrimination was occurring would be difficult, given the complexity of big data analytics tools.

In sum, the rise of fintech presents a set of troubling concerns about consumer protection. It may lead to heightened privacy concerns, as more personal and financial information is stored by an increasing proliferation of companies. It may lead to unsophisticated investors making uninformed, but deeply impactful, financial decisions based on spur-of-the-moment judgments. It may increase the prevalence of crime and fraud within the financial sector. And it may cause certain vulnerable groups to face hidden bias and discrimination in financial transactions. These are the sorts of problems that financial regulation has long sought to stamp out, and their presence in the fintech sector is troubling.

C. *Systemic Risk*

In addition to efficiency and fairness, financial regulation also aims to promote stability. Indeed, this aspect of financial regulation is one of the distinguishing features of banking law. To a greater degree than perhaps any other area of law, the law governing financial institutions focuses on preventing, not just harm to other parties, but

---

PRESERVING VALUES (May 2014), http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf

[120] *See* Michael Schrage, *Big Data's Dangerous New Era of Discrimination*, HARV. BUS. REV., Jan. 29, 2014; Cynthia Dwork & Deirdre K. Mulligan, *It's Not Privacy, and It's Not Fair*, 66 STAN. L. REV. ONLINE 35 (2013); Joseph W. Jerome, *Buying and Selling Privacy: Big Data's Different Burdens and Benefits*, 66 STAN. L. REV. ONLINE 47 (2013); Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. Rev. 93 (2014); Max N. Helveston, *Consumer Protection in the Age of Big Data*, 93 Wash. U. L. Rev. 859 (2016).

instability within the industry itself. The reason is a simple one: the financial sector is so central to the functioning of modern economies that when it struggles, the effects ripple out broadly to the broader society.[121] Thus, economic growth depends heavily on the health and stability of the financial sector.[122]

Financial regulation has sought to promote stability in the financial sector by adopting several mechanisms aimed at increasing the resilience and robustness of banks. For example, banks must maintain certain capital to asset ratios to ensure that, in the event of an adverse change in the market, they can absorb losses and avoid catastrophic consequences.[123] Similarly, banks must contribute funds to the Federal Deposit Insurance Corporation so that depositors can remain confident that their deposits will be protected from loss.[124] The ex post justification for these rules is that, in times of market turmoil, banks and consumers will be protected from loss. But the ex ante justification is that the very existence of the rules renders it less likely that the losses will occur in the first place. After all, if market participants are aware that banks have large reserves in place to be able to withstand losses, they will be more likely to continue to do business with them on ordinary terms, thus preventing further losses. Similarly, if depositors are aware that their accounts at banks are insured against loss, they will be less likely to withdraw their deposits in times of market turmoil, thus preventing the kind of runs that banks experienced during the Great Depression.

Since the financial crisis, financial regulators have focused their attentions on resolving the systemic risks presented by large, "too big to fail" banks.[125] This regulatory response was driven by the belief that

---

[121] *See* Alan Binder, *It's Broke, Let's Fix It: Rethinking Financial Regulation*, 6 INT'L J. CENT. BANKING 277, 279-80 (2010).

[122] *See* JOHN ARMOUR, DAN AWREY, PAUL DAVIES, LUCA ENRIQUES, JEFFREY N. GORDON, COLIN MAYER & JENNIFER PAYNE, PRINCIPLES OF FINANCIAL REGULATION 51-52 (2015).

[123] *See* John C. Coffee, Jr., *Systemic Risk After Dodd-Frank: Contingent Capital and the Need for Regulatory Strategies Beyond Oversight*, 111 Colum. L. Rev. 795 (2011); Hal S. Scott, *Reducing Systemic Risk Through Reform of Capital Regulation*, 13 J. INT'L ECON. L. 763 (2010).

[124] ARMOUR ET AL., *supra* note 122, at 316-40.

[125] *See* Gordon & Muller, *Confronting Financial Crisis: Dodd-Frank's Dangers and the Case for a Systemic Emergency Insurance Fund*, 28 YALE J. REG. 151, 154-55 (2011); Prasad Krishnamurthy, *Regulating Capital*, 4 HARV. BUS. L. REV. 1, 1 (2014); Felix B. Chang, *The Systemic Risk Paradox: Banks and Clearinghouses Under Regulation*, 2014 COLUM. BUS. L. REV. 747, 747 (2014); Manuel Utset, *Complex Financial Institutions and Systemic Risk*, 45 GA. L. REV. 779 (2011); Kenneth Ayotte & David A. Steel, Jr., *Bankruptcy or Bailouts*, 35 J. CORP. L. 469 (2010); Michael C. Munger & Richard M. Salsman, *Is "Too Big to Fail" Too Big?*, 11 GEO. J. L. & PUB. POL'Y 433 (2013); Arthur E. Wilmarth, *The Dodd-Frank Act: A Flawed and*

banks in the pre-crisis period had exploited the implicit governmental guarantee on their activities to engage in excessively risky behavior. Knowing that their failure would impose catastrophically large costs on broader society, and that any rational government would be forced to bail them out to avoid these costs from materializing, banks had incentives to take risky bets on mortgages and create ever more complex derivatives that would create short-term profits at the risk of long-term losses. The failure of Lehman Brothers in 2009 provided a powerful example of the threat that "too big to fail" banks posed to the wider economy.[126] In order to resolve this problem, legislators enacted the Dodd-Frank Act, which imposed a set of onerous requirements on "systemically important financial institutions" and established new governmental entities aimed at monitoring the large banks and their risk exposures.[127]

From the perspective of size, fintech firms assuredly do not present the same risks as more traditional Wall Street firms. They are significantly smaller on any number of dimensions, from employment,[128] to assets,[129] to profits.[130] No fintech firm (at least presently) would fall under the umbrella of regulation aimed at "systemically important financial institutions." Thus, fintech largely evades systemic-risk related regulatory scrutiny.

This is problematic because fintech firms present a number of concerns related to systemic risk.[131] First, because of their small size,

---

Inadequate Response to the Too-Big-To-Fail Problem, 89 ORE. L. REV. 951 (2011); David Zaring, *A Lack of Resolution*, 60 EMORY L.J. 97, 106 (2010); Andrew F. Tuch, *Financial Conglomerates and Information Barriers*, 39 J. CORP. L. 563 (2014);.

[126] Of course, the very fact that Lehman Brothers was allowed to fail suggests that the "too big to fail" moniker is not entirely accurate. It does not, however, refute the possibility that banking executives *believed* that their banks would not be allowed to fail.

[127] *See* Hilary J. Allen, *Putting the "Financial Stability" in Financial Stability Oversight Council*, 76 OHIO ST. L. J. 1087, 1113-20 (2015).

[128] *See* GARRICK HILEMAN & MICHAEL RAUCHS, GLOBAL CRYPTOCURRENCY BENCHMARKING STUDY 25 (2017) (noting that virtual currency companies in the United States have an average of only 12 employees).

[129] One of the larger robo-advisors, Wealthfront, had $5.5 billion in assets under management as of March 2017. *See* Tom Anderson, *Man vs. Machine: How to Figure Out if You Should Use a Robo-Advisor*, CNBC, Mar. 13, 2016. Vanguard, on the other hand, had approximately $4 trillion in assets under management as of December 31, 2016. *See* VANGUARD, FAST FACTS ABOUT VANGUARD, available at https://about.vanguard.com/who-we-are/fast-facts/.

[130] Prosper, for example, a prominent small business lending company based in San Francisco, has yet to turn a profit. *See* Oscar Williams-Grut, *Funding Circle CEO Says It's a "Golden Age" For Marketplace Lending as Revenue Jumps 144%*, BUS. INSIDER, Oct. 1, 2016.

[131] *See generally* William Magnuson, *Regulating Fintech*, 71 VAND. L. REV. (forthcoming 2018) (describing the systemic risk of fintech innovations); Kathryn

fintech actors are much more vulnerable to rapid, adverse shocks. Even relatively small losses, from the perspective of Wall Street investment banks, would sink many fintech firms. And while the magnitude of the harm from the failure of a single fintech actor is smaller than a comparable failure at a large Wall Street bank, the probability of its occurrence is significantly higher. A recent study of Bitcoin exchanges, for example, found that new exchanges have an expected lifespan of just 381 days.[132] Systemic risk is created by the interaction between the magnitude of a loss, the probability of its occurrence, and the likelihood that the loss will spread to other parts of the financial sector.[133] As fintech becomes more closely integrated into our financial system, and pathways for contagion multiply, systemic risk concerns will only grow.

Second, because of the large number of actors in fintech markets, regulators struggle to monitor the behavior of relevant participants. Regulatory regimes are only effective if regulators can identify, observe, and sanction actors within the given sphere of activity.[134] Unlike traditional finance, in which a few concentrated actors control a significant portion of the market, fintech is typified by the proliferation of many small actors. This poses an obstacle for regulators that must identify the particular firms and individuals of interest to them. Even if regulators are capable of identifying the relevant actors within a given fintech sector, they also must grapple with the related problem of understanding the risks generated by those actors, many of whom rely heavily on algorithms and computer coding for their

---

Judge, *Investor Driven Financial Innovation*, 7 HARV. BUS. L. REV. (forthcoming 2018) (describing the ways in which investor-driven financial innovation can increase fragility within markets).

[132] *See* Tyler Moore & Nicolas Christin, *Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk*, 7859 FIN. CRYPTOGRAPHY & DATA SECURITY 25 (2013).

[133] *See, e.g.*, Timothy Geithner, *Are We Safe Yet? How to Manage Financial Crises*, 96 FOREIGN AFFAIRS 54 (2013); Olivier de Bandt & Philipp Hartmann, *Systemic Risk: A Survey* 10-18 (Eur. Cent. Bank, Working Paper No. 35 2000); Markus K. Brunnermeier & Martin Oehmke, *Bubbles, Financial Crises, and Systemic Risk*, in 2B HANDBOOK OF THE ECONOMICS OF FINANCE 1221, 1233-38 (George M. Constantinides, Milton Harris & Rene M. Stulz eds., 2013); Graciela Kaminsky, Carmen Reinhardt & Carlos Vegh, *The Unholy Trinity of Financial Contagion*, 15 J. ECON. PERSP. 51 (2003); NASSIM NICHOLAS TALEB, ANTIFRAGILE: THINGS THAT GAIN FROM DISORDER 20-21 (2012); Lawrence H. White, *Antifragile Banking and Monetary Systems*, 33 CATO J. 471 (2013).

[134] *See* Gary S. Becker, *Crime and Punishment: An Economic Approach*, 76 J. POL. ECON. 169, 172-73 (1968); George J. Stigler, *The Optimum Enforcement of Laws*, 78 J. POL. ECON. 526 (1970); A. Mitchell Polinsky & Steven Shavell, *Enforcement Costs and the Optimal Magnitude and Probability of Fines*, 35 J. L. & ECON. 133, 135-39 (1992).

decisionmaking.[135] These are difficult tasks even for those who specialize in the industry, let alone for regulators who are often ill-equipped and under-resourced.[136] Without an appropriate level of oversight and monitoring by capable regulators, fintech companies will be more likely to engage in risky behavior and yet avoid detection.

Third, the characteristics of fintech companies create an environment in which cooperative behaviors and norms are less likely to develop.[137] Even competitive markets such as finance and asset management often end up displaying surprising amounts of cooperation: actors may work together to create "best practices" or share information about security vulnerabilities or, in particularly dire circumstances, to ensure the survival of the market itself.[138] Large institutions such as Wall Street banks interact with regulators and one another frequently, and thus have strong incentives to maintain their reputation as cooperative partners.[139] Fintech firms, on the other hand, have fewer opportunities for such interaction, and often have shorter time horizons.[140] As a result, they will perceive fewer benefits from contributing to the production of wider social goods, such as the promotion of industry guidelines on risk management or cybersecurity.

For all of these reasons, fintech firms present a set of systemic risk concerns that are distinct from the concerns that are generated by more traditional financial institutions. These risks are derived from fintech's disaggregated model of finance, its heavy reliance on automation, and its high levels of adaptation and change. The risks are only likely to grow as the various technologies gain greater acceptance and are increasingly incorporated into the wider economy. And to the extent that current financial regulations aimed at limiting systemic risk focus primarily on the risks of large institutions, these regulations may be misguided.

III. TOWARDS A LAW OF FINTECH

The fintech industry has seen rapid growth in recent years and has introduced significant changes in the structure of financial markets and the ways that financial services are delivered. While these changes

---

[135] *See* Magnuson, *supra* note 48, at 37.

[136] *See* Lawrence G. Baxter, *Capture Nuances in Financial Regulation*, 47 WAKE FOREST L. REV. 537, 560-61 (2012).

[137] *See* Magnuson, *supra* note 48, at 38-44.

[138] *See* Saul Levmore, *Competition and Cooperation*, 97 MICH. L. REV. 216 (1999).

[139] *See* William D. Cohen, *Three Days That Shook The World*, FORTUNE, Dec. 16, 2008.

[140] *See supra* Part I.A.

provide a number of benefits for consumers and investors, they also raise questions about the efficacy of current financial regulatory structures. In sum, they suggest that financial rules aimed at promoting efficiency, fairness and stability in the financial sector are misguided or incomplete.

These problems call for a wider reassessment of financial regulation of the fintech sector. This Section will argue that fintech is sufficiently distinct from traditional financial institutions that it calls for tailored regulation that is substantively different from general financial law. The goals of such a "law of fintech" would naturally be similar to the goals of all financial regulation: promoting the efficient allocation of capital, protecting consumers and investors, and increasing stability and systemic resilience. But the methods for arriving at these goals, and thus the focus and target of regulation, will look significantly different. In particular, fintech regulation should be guided by three overriding principles. First, it should focus on improving the quality and quantity of information that is available with respect to fintech products and services. Second, it should emphasize the centrality of cybersecurity for all fintech firms, and it should aim to exclude actors and industries that fail to adopt appropriate safeguards. Third, it should simplify and centralize regulatory authority over fintech in order to better allow regulatory authorities to balance priorities and goals.

A. *Information-Forcing Rules*

Asymmetric information has long been recognized as a central cause of market failure.[141] In industries in which insiders have significantly more information about a product and its risks than outsiders, voluntary market transactions may lead to inefficient results, either because the insiders take advantage of the outsiders, or because the outsiders refuse to do business at all.[142] One way to correct for these problems is for insiders to voluntarily provide better information to outsiders: home sellers, for example, could hire an independent inspection firm to confirm that houses do not have any hidden defects;

---

[141] *See* ROBERT COOTER & THOMAS ULEN, LAW AND ECONOMICS 41-42 (2016); ROBERT L. GLICKSMAN & RICHARD E. LEVY, ADMINISTRATIVE LAW: AGENCY ACTION IN LEGAL CONTEXT 15-19 (2010); Van

[142] *See* William W. Bratton & Michael L. Wachter, *The Case Against Shareholder Empowerment*, 158 U. PA. L. REV. 653, 696-705 (2010); Manuel A. Utset, *Complex Financial Institutions and Systemic Risk*, 45 GA. L. REV. 779, 803-09 (2011); Kathryn Judge, *Fragmentation Nodes: A Study in Financial Innovation, Complexity, and Systemic Risk*, 64 STAN. L. REV. 657, 696-97 (2012); Gary Gorton & Lixin Huang, *Bank Panics and their Endogeneity of Central Banking*, 53 J. MONETARY ECON. 1613 (2006).

or, in the financial industry, financial firms could hire ratings agencies to inspect their financial products for adequacy and reliability.[143] But such voluntary actions are both costly and potentially faulty, as the independence of such outside inspectors may themselves be suspect.[144] Thus, information asymmetries are problematic for markets and market-based mechanisms and often call for regulatory intervention to force better information production.

As mentioned above, fintech suffers from particularly acute information asymmetries. The disaggregated nature of fintech, and the growth in the variety and number of actors in the industry, places investors and consumers at a disadvantage when attempting to gauge the reputation and reliability of particular actors. For example, in the crowdfunding industry, investors must decide on whether to invest in particular companies based primarily on information voluntarily provided by the companies themselves. In traditional finance, investment banks or other financial institutions would normally be expected to perform a significant amount of due diligence for the companies that they were working for. In other words, they act as "gatekeepers" ensuring that investors have some measure of certainty about the reputation of their counterparties.[145] But crowdfunding platforms perform such gatekeeping functions only reluctantly, and sometimes not at all. It is not uncommon for such websites to includes in their terms and conditions a "disclaimer of warranties" that explicitly provides that the platform does not guarantee the accuracy, adequacy, or usefulness of any content on the site. Fintech's widespread elimination of gatekeepers creates a situation ripe for information problems.[146]

And importantly, the significant information asymmetries in fintech lie at the root of many of our concerns about the industry. From the perspective of *efficiency*, information asymmetries within fintech have the potential to lead to a breakdown in markets, causing an increase in the number and size of inefficient transactions, a decrease in the number and size of efficient transactions, or both. The increased

---

[143] *See* Cooter & Ulen, *supra* note 141, at 42.

[144] *See* Kia Dennis, *The Ratings Game: Explaining Rating Agency Failures in the Build Up to the Financial Crisis*, 63 U. MIAMI L. REV. 1111 (2009).

[145] For a description of the gatekeeping function of financial intermediaries, see Reinier H. Kraakman, *Gatekeepers: The Anatomy of a Third-Party Enforcement Strategy*, 2 J.L. ECON. & ORG. 53, 54 (1986); John C. Coffee, Jr., *Gatekeeper Failure and Reform: The Challenge of Fashioning Relevant Reforms*, 84 B.U. L. REV. 301, 309 (2004); Ronald J. Gilson & Reinier H. Kraakman, *The Mechanisms of Market Efficiency*, 70 VA. L. REV. 549, 618 (1984); Stephen Choi, *Market Lessons for Gatekeepers*, 92 NW. U. L. REV. 916, 918 (1998); Elisabeth de Fontenay, *Private Equity Firms as Gatekeepers*, 33 REV. BANKING & FIN. L. 115, 121-24 (2013).

[146] *See* Choi, *supra* note 145, at 934-39.

transaction costs associated with information-scarce markets acts as a drag on the efficient allocation of capital. From the perspective of *fairness*, the information asymmetries within fintech markets can be expected to lead to a higher frequency of consumer or investor fraud, as well as more mundane, but potentially more problematic, irrational behavior on the part of these actors. Without comprehensive and reliable information about the costs and benefits of particular fintech services, consumers may be taken advantage of by unscrupulous businesses that promise them above-market returns.[147] They may also be more likely to engage in herd behavior that leads them to contribute to asset bubbles that are divorced from the asset's intrinsic value.[148] Finally, from the perspective of *stability*, information asymmetries within the fintech industry increase the possibility that fintech will create systemic risk for the wider economy.[149] Without better information about the structure and functioning of fintech markets, regulators will struggle to monitor and constrain fintech services with respect to broader system risks.[150] Similarly, consumers that lack information about the resilience and solvency of actors are more likely to be susceptible to panicked behavior and contagion in the event of adverse market shocks.[151]

It is unlikely that, in the absence of regulatory pressure, private market mechanisms will lead to the appropriate level of information disclosure in fintech. Because fintech tends to connect parties through disintermediated platforms, many of the participants in the industry are unsophisticated. Such participants will likely be unaware of the appropriate level of information that they should receive with respect to financial transactions and thus cannot realistically be expected to press for it. And the ease with which consumers can enter into fintech transactions—one can purchase tokens in an initial coin offering in a matter of minutes entirely through the internet—discourages wider-ranging negotiation through which information might be disclosed. Even sophisticated investors may not succeed in pressuring market participants to provide fulsome disclosures about transaction risks. Sophisticated investors, after all, have limited time and capacity to review and process the terms of complex financial instruments. During

---

[147] *See* David Z. Morris, *The Rise of Cryptocurrency Ponzi Schemes*, THE ATLANTIC, May 31, 2017.

[148] *See* Kevin Rose, *Is There a Cryptocurrency Bubble?*, N.Y. TIMES, Sept. 15, 2017.

[149] *See* Magnuson, *supra* note 48, at 10.

[150] *See* Kathleen Judge, *Information Gaps and Shadow Banking*, 103 VA. L. REV. 411 (2017).

[151] *See* Steven Schwarcz, *Identifying and Managing Systemic Risk: An Assessment of Our Progress*, 1 HARV. BUS. L. REV. 94 (2011).

the financial crisis, large banks—some of the most sophisticated actors in the industry—found that their exposures to the home mortgage crisis and related derivatives were substantially larger than their models had predicted. And to the extent that the growth of fintech markets is driven by demand among unsophisticated investors, sophisticated investors may have little leverage to negotiate for better terms.

For these reasons, any financial regulation aiming to improve the functioning of fintech markets needs to focus on resolving the significant information asymmetries that exist within fintech.[152] This will require regulators to drive information production, ensuring that industry participants provide comprehensive, accurate and consistent disclosures about their business models, functions, and risks, and that they provide this information in easily digestible and accessible formats. The disclosures should be directed and tailored to two general audiences: first, to the regulators themselves, in order to improve their ability to monitor risks as they emerge; and second, to consumers and investors, in order to improve their ability to make informed decisions in the market.[153]

While a full discussion of the specific disclosure requirements for fintech firms is beyond the scope of this article, and would certainly vary depending on the type of company and industry at issue, a few simple guidelines should apply across fintech sectors. First, fintech companies must be held responsible for the accuracy and reliability of the information on their sites. While this would seem to be a relatively uncontroversial and common-sense proposal, it would in fact signal a marked change from the approach of many firms in the fintech industry. Both robo-advisors and crowdfunding platforms, for example, often disclaim any warranty for the accuracy or appropriateness of the information on their sites. Thus, a first step in reducing information asymmetries in fintech would be to require fintech firms to be liable for inaccuracies or misinformation they provide about their services.

Just as important as holding fintech firms responsible for the information they provide is forcing the firms to provide the information in the first place. Regulators must ensure that fintech firms provide comprehensive information about their services and businesses prior to entering the market. Without such a requirement, the imposition of liability for inaccurate disclosures might paradoxically cause fintech

---

[152] *See* Donald C. Langevoort, *Toward More Effective Risk Disclosure for Technology-Enhanced Investing*, 75 WASH. U. L. Q. 753 (1997); Troy S. Brown, *Legal Political Moral Hazard: Does the Dodd-Frank Act End Too Big to Fail?*, 3 ALA. C.R. & C.L. L. REV. 1, 37-46 (2012).

[153] *See* Mary Jo White, *Opening Remarks at the Fintech Forum*, Nov. 14, 2016, available at https://www.sec.gov/news/statement/white-opening-remarks-fintech-forum.html.

firms to reduce the total amount of information they disclose, the precise opposite of the desired result. At a minimum, the substantive disclosure obligations should include basic information such as quantitative and qualitative discussion of the business, past performance, and risk factors. To the extent that regulators require access to sensitive information that might harm the company if disclosed to the public, fintech firms should be allowed to divulge sensitive information solely to their relevant regulator under a confidential disclosure process.

An essential question in any disclosure regime, of course, is the capacity of the audience to process and understand the information that is eventually disclosed.[154] Fintech presents particularly thorny receptivity problems. For example, if a virtual currency's code is publicly available, is this sufficient information for regulators and consumers to be able to understand the risks of the currency? Or if a crowdlending platform states in its terms and conditions that it relies on a particular type of technology to model credit risks, is such a disclosure likely to be understood or even read by most investors? The existence of such problems suggests that fintech disclosures will require a significant amount of "translation" work aimed at making the disclosures readily accessible and easily understood by the desired audiences. This may well require regulators to create fintech-focused divisions that have the operational and technical expertise to assess fintech risks. One model for such bodies is the recently created cyber division of the Securities Exchange Commission, which focuses on identifying and sanctioning "cyber-related misconduct."[155]

Perhaps the greatest benefit of information-forcing rules is that they impose relatively low burdens on fintech companies themselves. The majority of the information that would need to be disclosed under plausible disclosure regimes should be readily available to the relevant actors and thus will require minimal additional research on the part of firms. The low cost of information production has the additional advantage of avoiding inadvertent incentives for firms to engage in regulatory arbitrage. Recent reforms of financial regulation have been sharply criticized for their tendency to escalate regulatory costs, thereby creating incentives for firms to go underground or shift services to less-regulated sectors.[156] Such "shadow banks" operate largely out of sight of government bodies and can create risks that leak into the broader

---

[154] *See* OMRI BEN-SHAHAR & CARL E. SCHNEIDER, MORE THAN YOU WANTED TO KNOW: THE FAILURE OF MANDATED DISCLOSURE (2014).

[155] *See* SECURITIES EXCHANGE COMMISSION, SEC ANNOUNCES ENFORCEMENT INITIATIVES TO COMBAT CYBER-BASED THREATS AND PROTECT RETAIL INVESTORS, Sept. 25, 2016, available at https://www.sec.gov/news/press-release/2017-176.

[156] *See* Steven Schwarcz, *Regulating Shadow Banking*, 31 Rev. Banking & Fin. L. 619, 624 (2011).

economy. Information-forcing rules would avoid this costly dynamic.

B. *Security-Forcing Rules*

In addition to improving information flows, the law of fintech must also focus on increasing the security and resiliency of fintech platforms. It is now a fact of life that online sites are subject to data breaches and hacking attacks on a daily basis. Such breaches have targeted government databases, technology companies, and military contractors. The seemingly unending series of disclosures about successful cyber-intrusions into prominent corporations is troubling from a number of perspectives, but it has particular salience to the financial industry.[157]

The possibility—indeed, one might go so far as to say the inevitability—that an ever greater portion of financial transactions will take place through online platforms increases the urgency of putting in place laws that ensure that financial institutions establish appropriate cyber-safeguards. This problem is not unique to fintech per se. Even traditional financial institutions have struggled to prevent and respond to hacking attacks. In 2014, for example, a cyberattack on JP Morgan is believed to have compromised the private data of over 80 million customers.[158] The same year, a hacking attempt that is suspected to have originated in Russia infiltrated the systems of nine unidentified financial institutions. One official at the cyberdivision of the Federal Bureau of Investigation has instructed financial institutions, "You're going to be hacked. Have a plan."[159]

Cybersecurity is of particular importance in the fintech industry, however, for a number of reasons. First, since fintech firms tend to rely on mobile and online platforms for their essential functions, they are especially dependent on the safety and security of their systems. Second, given the relative newness of many of those systems and technologies, the likelihood of unexpected or unknown vulnerabilities in their cybersecurity systems is high. For example, in one of the more

---

[157] *See* Brian B. Kelly, *Investing in a Centralized Cybersecuritry Infrastructure: Why "Hacktivism" Can and Should Influence Cyber Security Reform*, 92 B.U. L. Rev. 1663 (2012); Peter M. Shane, *Cybersecurity: Toward a Meaningful Policy Framework*, 90 TEX. L. REV. 87 (2012); Eric T. Jensen, *Cyber Warfare and Precautions Against the Effects of Attacks*, 88 TEX. L. REV. 1533 (2010); Scott J. Shackelford & Scott Russell, *Operationalizing Cybersecurity Due Diligence: A Transatlantic Case Study*, 67 S.C. L. REV. 609 (2016); MICHAEL E. BLEIER, TIMOTHY NAGLE & CHRISTOPHER J. FATHERLEY, THE CURRENT STATE IN FINANCIAL SERVICES CYBERSECURITY (2013).

[158] *See* Erin Kelly, *Officials Warn 500 Million Financial Records Hacked*, USA TODAY, Oct. 20, 2014

[159] *Id*.

notorious examples of the vulnerabilities of virtual currencies, in 2016, a hacker exploited a flaw in the coding of an autonomous organization known as the DAO to steal $55 million of ethereum. The vulnerability was created by the use of a lower case "t", rather than an upper case "T", in line 666 of the code.[160] Small mistakes or oversights in complex algorithms can lead to significant losses.

Crafting a law of fintech that focuses on improving cybersecurity should simultaneously promote all of the primary interests that financial regulation aims to protect. It has consequences for the efficient allocation of capital because breaches of cybersecurity protocols may lead to thefts or improper transfers of capital to criminals and rogue states.[161] It has consequences for consumer protection because hackers may steal sensitive financial and personal information for individuals.[162] It has consequences for systemic stability because cyber-intrusions may lead to markets or transactions being frozen or seizing up.[163]

Given the centrality of cybersecurity for the efficient, fair, and stable functioning of the financial sector, and the particular vulnerability of fintech technologies to cyber-intrusions, fintech regulation must place a special emphasis on ensuring that actors in the sector implement proper systems and procedures for preventing, detecting, and resolving cyberattacks. Current cybersecurity laws tend to be vague in substance and generic in application. For example, the primary statute that the Federal Trade Commission has used to prosecute corporations for failing to implement cybersecurity procedures is 15 U.S.C. Section 45(a), which merely states that "unfair or deceptive acts or practices in or affecting commerce" are unlawful.[164] As one industry participant has put it, "[t]he SEC hasn't been very specific about what it wants firms to do on cybersecurity."[165] Such vagueness, while placing broad

---

[160] *See* Leising, *supra* note 161.

[161] Prominent examples of thefts involving virtual currencies include the disappearance of hundreds of thousands of bitcoins from the bitcoin exchange Mt. Gox in 2014 and the hack of the ethereum-based DAO organization. *See* McMillan, *supra* note 41; Matthew Leising, *The Ether Thief*, BLOOMBERG, June 13, 2017.

[162] In the Equifax hack of 2017, for example, hackers were able to expose the names, addresses, birth dates, and Social Security numbers of over 140 million Americans. *See* AnnaMaria Andriotis, Michael Rapoport & Robert McMillan, *"We've Been Breached": Inside the Equifax Hack*, WALL ST. J., Sept. 18, 2017.

[163] *See* Alexander Osipovich, *Pentagon Turns to Hig-Speed Traders to Fortify Markets Against Cyberattack*, WALL ST. J., Oct. 15, 2017.

[164] 15 U.S.C. § 45(a)(1) (2012); Fed. Trade Comm'n, 2016 Privacy and Data Security Update (2016), available at https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2016/privacy_and_data_security_update_2016_web.pdf.

[165] *See* BARRON'S, *SEC to Advisors: Improve Cybersecurity Preparedness*, Aug.

discretion within the hands of regulators to prosecute companies for lax cybersecurity policies, fails to give companies guidance about proper levels of cybersecurity.

Fintech law must remedy this problem by giving better guidance to firms about the appropriate levels of protection that must be implemented before a firm may enter into sensitive financial transactions. It can do so in several ways. First, regulations should set forth minimum levels of cybersecurity preparedness that fintech firms must implement.[166] Such rules should address not just written policies and procedures, but also employee training, regular inspections, and maintenance issues. These rules should be tailored to address the particular cybersecurity concerns of the technology at issue: virtual currency cybersecurity protocols, for example, might look quite different from robo-advisor cybersecurity protocols.

Second, regulators should establish a "fintech cybersecurity" body that has the ability and the expertise necessary to monitor and investigate cybersecurity practices in the industry. Such a body might be modeled on the National Examination Program of the Securities Exchange Commission, which regularly undertakes comprehensive examinations of cybersecurity procedures within the broker-dealer industry.[167] The centralization of expertise and monitoring capabilities would improve the ability of regulators to identify fintech vulnerabilities before they are exploited.

Third, fintech law should not just set forth substantive standards and enable regulators to enforce them, but it should also proactively encourage fintech firms to engage with regulators on their cybersecurity procedures.[168] Such engagement would certainly include reporting

---

9, 2017.

[166] *See, e.g.*, OFFICE OF COMPLIANCE INSPECTIONS AND EXAMINATIONS, NATIONAL EXAM PROGRAM RISK ALERT: OBSERVATIONS FROM CYBERSECURITY EXAMINATIONS (2017), available at https://www.sec.gov/files/observations-from-cybersecurity-examinations.pdf (hereinafter, OCIE REPORT); FINANCIAL INDUSTRY REGULATORY AUTHORITY, REPORT ON CYBERSECURITY PRACTICES (2015), available at https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf; FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL, FFIEC CYBERSECURITY ASSESSMENT TOOL: OVERVIEW FOR CHIEF EXECUTIVE OFFICERS AND BOARDS OF DIRECTORS (2015), available at https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_CEO_Board_Overview_June_2015_PDF1.pdf; NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (2014), available at https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

[167] *See* OCIE REPORT, *supra* note 166, at 1.

[168] *See* Sam Young, *Contemplating Corporate Disclosure Obligations Arising*

intrusions and attempted intrusions, but it might also include broader cooperative efforts. The Department of Homeland Security, for example, offers free "cyberhygiene" scans of state voting systems.[169] Such an approach would be relatively low-cost and could provide significant benefits for the security and stability of financial markets.

But of course, even the best cybersecurity procedures are not invulnerable to breach, and thus the law of fintech should not just set forth substantive standards for the kinds of protections that fintech firms must incorporate into their models, it should also create rules governing how fintech firms must respond to breaches. This would include at a minimum an obligation for firms to establish a plan for limiting the harm from system breaches, as well as an obligation to report breaches immediately to the relevant regulators. Too often, private firms fail to disclose breaches in a timely manner, thus preventing regulators and consumers from taking steps to protect themselves from harm stemming from the breaches.[170] Given the centrality of financial services, and financial information, to the modern economy, fintech firms must be held to higher standards.

Imposing higher levels of cybersecurity obligations on fintech firms will certainly be more intrusive than the disclosure obligations outlined in the previous section. It will also require regulators to have exceptional knowledge and skill in deciding the appropriate standards. Both of these facts suggest that regulators should tread carefully, and solicit industry and interest-group feedback on proposed regulations, before enacting comprehensive cybersecurity regulation aimed at the fintech sector. But the cost of not doing so is large and difficult to calculate, given the capability for cybertheft to work long-term damage to investor and consumer credit and confidence. Thus, it must be at the center of any prudent attempt to improve the law of fintech.

C. *Tradeoff-Forcing Rules*

As described above, the law of fintech must prioritize information disclosure and cybersecurity preparation, two areas in which fintech currently raises significant concerns and which, if resolved, could provide benefits along all of financial regulation's priorities. But a third aspect of fintech law is perhaps a less obvious one: balancing priorities. While the first two features of fintech law

---

from Cybersecurity Breaches, 38 J. CORP. L. 659 (2013).

[169] *See* Michael Wines, *Wary of Hackers, States Moves to Upgrades Voting Systems*, N.Y. TIMES, Oct. 14, 2017.

[170] *See* Ted Lieu, *We Need a Law Requiring Faster Disclosure of Data Breaches-Now*, Slate, Sept. 15, 2017; Chris Isidore, *Equifax's Delayed Hack Disclosure: Did It Break the Law?*, CNN, Sept. 8, 2017.

require the creation of substantive standards and behavioral requirements, this feature focuses instead on the process and methods by which those standards are created. Fintech law must make difficult choices about the priorities it seeks to realize, and in doing so, it will necessarily require regulators to make tradeoffs between the core purposes of financial regulation—efficiency, fairness and stability. These decisions should be made consciously and explicitly. And while of course all regulation requires a balancing of costs and benefits, the process is even more important in the fintech industry given the disaggregated nature of fintech and its dispersed decisionmaking structure.[171]

The tradeoffs in fintech regulation are similar to those facing more general financial regulation.[172] It is impossible for financial regulation to perfectly achieve all of its purposes, as the pursuit of some of these purposes may simultaneously inhibit the pursuit of the others. Efficient markets may at times lead to results that are perceived as unfair. Strong consumer protection rules may lead to markets that are less efficient. Regulation aimed to promote stability within a system may simultaneously reduce efficiency or investor rights in the system. These tradeoffs are seen in all financial regulation, but they are particularly acute in the case of fintech.

Fintech markets, as mentioned before, tend to be heavily populated with small, disaggregated actors. But small actors are precisely the kinds of actors that are least able to bear regulatory costs.[173] Unlike large financial institutions, who employ hundreds of lawyers to ensure compliance with the mosaic of laws that apply to them, fintech companies tend to be leanly staffed and to rely on maintaining low overhead. Costly regulation that might be borne easily by large financial institutions might well make the difference between a profitable and an unprofitable business in the fintech world.[174] Indeed, to the extent that large financial institutions view fintech companies as potential competitors, they may well push for regulations that impose large, industry-wide costs on firms in order to increase the barriers to

---

[171] *See* Howell E. Jackson, *Variation in the Intensity of Financial Regulation: Preliminary Evidence and Potential Implications*, 24 YALE J. ON REG. 253 (2007); John C. Coates IV, *Cost-Benefit Analysis of Financial Regulation: Case Studies and Implications*, 124 YALE L. J. 882 (2015); Brummer & Yadav, *supra* note 44, at 15-30 (arguing that fintech regulation faces a "trilemma" preventing it from satisfying its three goals of clear rules, market integrity and financial innovation).

[172] *See* Brummer & Yadav, *supra* note 44, at 15-30.

[173] *See* Jeff Schwartz, *The Law and Economics of Scaled Equity Market Regulation*, 39 J. CORP. L. 347 (2014).

[174] *See* Rory van Loo, *Rise of the Digital Regulator*, 66 DUKE L. J. 1267 (2017).

entry for fintech companies.[175]

Fintech firms are also more likely to be able to shift their activities to unregulated or unobserved sectors.[176] Unlike large financial institutions, which have no plausible options for "going underground" or shifting their operations abroad in order to avoid costly regulation, fintech firms have both the incentive and the means to restructure or reorganize in response to regulatory costs. They are small and adaptable, and to the extent that a new regulation imposes excessive costs, they are capable of redirecting their operations to avoid those costs. Blockchain-based virtual currencies, for example, have applications outside the currency realm, and companies that have an expertise in one area can easily apply that expertise in another.[177]

For these reasons, the law of fintech will face significantly more constraints on the magnitude and breadth of its reach. Any regulation aimed at shoring up consumer protection rules risks diverting fintech activity, either to other jurisdictions or to other less-regulated use-cases. Similarly, regulation aimed at improving capital buffers in fintech banking companies risks creating strong incentives for companies to set up abroad or redefine their business models in ways that avoid the capital requirements. Fintech firms are more elastic and responsive to regulatory costs than traditional finance, and thus these tradeoffs can be expected to be faced sooner and more often than they would be in traditional financial regulation.

The implications of this analysis are simple: politicians and regulators will need to explicitly identify the priorities that they are seeking to pursue in regulating the fintech industry. If the priority is to prop up systemic stability in the industry, then doing so may come at a cost to consumer protection and efficiency. If the priority is to protect consumers from ill-advised transactions, then doing so may create some reduction in the system's efficiency and stability. And if the priority is to increase the efficient allocation of capital in the system, then regulators may be forced to accept a certain amount of risk and unfairness in the industry. These choices should be made openly and publicly.

Too often, lawmakers fail to recognize the tradeoffs they are

---

[175] *See* Elizabeth Pollman & Jordan Barry, *Regulatory Entrepreneurship*, 90 S. CAL. L. REV. 383 (2017)

[176] *See* Christina Parajon Skinner, *Regulating NonBanks: A Plan for SIFI Lite*, 105 GEO. L. J. 1379 (2017).

[177] *See* THE ECONOMIST, *Land Grab: Governments May Be Big Backers of the Blockchain*, June 1, 2017 (describing how one company based in Tbilisi, Georgia, shifted from a business focused on mining bitcoin to one focused on backing up Georgian government records).

making in enacting new rules.[178] It is not uncommon, for example, for legislators and regulators to claim that their new laws promote every possible desirable outcome—consumers will be protected, markets will function better, and systems will be more resilient.[179] This approach to regulation, while perhaps good politics, creates an environment in which public discussion about priorities and relative preferences is suppressed. The democratic legitimacy of laws depends on a conscious acceptance of the costs and benefits of those laws.[180]

How can the law of fintech better balance the threefold goals of financial regulation? As described above, two specific reforms that can come at relatively low cost and provide significant benefits along several fronts are better information and better cybersecurity. This kind of low-hanging fruit, though, is quickly exhausted, and then more difficult tradeoffs must come into consideration.

Two general paradigms, however, suggest themselves. First, regulators could adopt a "maximalist" paradigm in which regulators seek greater control over fintech markets, even at the cost of sensitive intrusions into markets.[181] One could, for example, imagine a kind of Securities Act for Fintech, under which new financial innovations could only be launched after a long and comprehensive registration process with federal authorities. Such a reform might reduce the potential for consumer abuse or market instability, but it would likely come at the expense of market efficiency: many beneficial innovations might be excluded from the market due to the time and expense of registering the new financial product.

A second, "minimalist" paradigm for fintech would instead adopt a wait-and-see approach, allowing fintech markets to develop with minimal intrusion from regulations.[182] One could imagine, for

---

[178] *See, e.g.*, Timur Kuran & Cass R. Sunstein, *Availability Cascades and Risk Regulation*, 51 Stan. L. Rev. 683 (1999); Gary M. Lucas, Jr., *Out of Sight, Out of Mind: How Opportunity Cost Neglect Undermines Democracy*, 9 N.Y.U. J. L. & LIBERTY 249 (2015).

[179] *See, e.g.*, George W. Bush, *Remarks on Signing the Sarbanes-Oxley Act of 2002*, July 30, 2002, available at http://www.presidency.ucsb.edu/ws/index.php?pid=73333; Barack Obama, *President Obama Signs Wall Street Reform: "No Easy Task"*, July 21, 2010, available at https://obamawhitehouse.archives.gov/blog/2010/07/21/president-obama-signs-wall-street-reform-no-easy-task.

[180] *See* Richard H. Fallon, Jr., *Legitimacy and the Constitution*, 118 HARV. L. REV. 1787 (2005) (describing the three types of legitimacy in constitutional law);

[181] For examples of such an approach to fintech regulation, see Lawrence G. Baxter, *Adaptive Financial Regulation and RegTech: A Concept Article on Realistic Protection for Victims of Bank Failure*, 66 DUKE L. J. 567 (2016); William S. Warren, *The Frontiers of Peer-to-Peer Lending: Thinking About a New Regulatory Approach*, 14 DUKE L. & TECH. REV. 298 (2016).

[182] For examples of a minimalist regime for fintech, see Angela Walch, *The Path*

example, a broad deregulatory effort for fintech, one that would lead to reduced regulatory burdens for small fintech companies. Such an approach would likely encourage market efficiency by reducing the cost of innovation, and thus spurring companies to develop new financial services that reduce transaction costs. But at the same time, it would likely decrease the ability of regulators to patrol the market to prevent consumer fraud. It could also increase systemic risk if complex new financial products are put on the market without a full understanding of how they might interact with other forms of finance.

These two paradigms of fintech regulation are of course not specific regulatory dictates, but rather legislative baselines that might inform the lawmaking process and enforcement efforts. They are also located at two sides of the spectrum, one involving a "light touch" approach to regulation and the other involving more heavy-handed intrusions into markets. The ultimate regulatory regime for fintech will likely fall somewhere along the spectrum, rather than at the extreme ends of it. But forcing regulators to identify where they fall along the spectrum, and the costs that are involved in doing so, would provide welcome transparency to the industry.

IV. OBJECTIONS

The revolution in the fintech industry in recent years has profoundly changed the landscape of finance. Innovations in virtual currencies, capital formation and asset management, enabled by advancements in algorithmic decisionmaking and the increasing prevalence of online transactions, have changed the way that financial services are provided. These changes provide many benefits to consumers and the economy, but they also raise challenges for regulators in monitoring and constraining the new actors in order to promote the key goals of finance in our society. In order to improve financial regulation in light of fintech, this Article has argued that a new, fintech-focused financial regulatory structure must be created. This "law of fintech" must focus on increasing the dissemination of accurate and comprehensive information about fintech products. It also must bolster cybersecurity measures within the industry. At the same time, given the disaggregated nature of fintech industries and the predominance of small, dispersed actors, regulators must identify and defend the tradeoffs they are making between efficiency, fairness and stability when they enact new rules.

---

of the Blockchain Lexicon (And the Law), 36 REV. BANKING & FIN. L. 713 (2017); Douglas W. Arner, Janos Barberis & Ross P. Buckley, *The Evolution of Fintech: A New Post-Crisis Paradigm*, 47 GEO. J. INT'L L. 1271 (2016).

With these outlines of the law of fintech now established, it is worth considering a set of potential objections to the approach proposed here. This Part addresses two prominent critiques in the financial regulation literature that, if fully accepted, would require significant changes to the regulatory regime set forth in this Article. First, it is often argued that disclosure-oriented reforms are ineffective because information-forcing laws are either unnecessary—markets will naturally lead actors with valuable information to disclose that information to those lacking it—or unhelpful—consumers and investors are unlikely to change their behavior based on new information. Second, many scholars have argued that there is a tradeoff between cybersecurity and national security, and where the two conflict, national security must trump. These objections raise important questions about the wisdom of a project to establish a regulatory regime for fintech based on greater information, better security, and more open weighing of priorities, and this Part will address them in turn.

A. *The Ineffectiveness of Information*

As described above in Part III.A, information asymmetries are a powerful source of market failure. If one party to a transaction cannot fully assess the costs and benefits of that transaction, then the party lacking information may be deceived into poor deals or, just as likely, refrain from engaging in the market in the first place.[183] In either scenario, the scope for mutually beneficial agreements in the market is narrowed, thereby creating a situation ripe for market failure.[184]

For this reason, many financial regulations adopt a disclosure-oriented approach to market reform.[185] For example, the Securities Exchange Act requires companies that seek to issue securities to the public to provide extensive disclosure about the companies' business, past operations, and risks.[186] The Sarbanes Oxley Act requires companies to disclose off-balance sheet items that had allowed companies like Enron to hide the true costs of their business and present

---

[183] *See* Easterbrook & Fischel, *supra* note **Error! Bookmark not defined.**, at 670 (noting that the securities laws were justified by the need to prevent fraud on the market, ensure that investors received the returns they expected, and prevent people from withdrawing their capital due to such behavior).

[184] *See* Stiglitz, *supra* note 92, at 1445.

[185] *See* Easterbrook & Fischel, *supra* note **Error! Bookmark not defined.**, at 670 ("The dominating principle of securities regulation is that anyone willing to disclose the right things can sell or buy whatever he wants at whatever price the market will sustain.").

[186] *See* Charles R. Korsmo, *The Audience for Corporate Disclosure*, 102 IOWA L. REV. 1581, 1590-99 (2017).

an overly optimistic portrait of their prospects for profit.[187] The Dodd-Frank Act authorizes the Securities Exchange Commission to issue "point-of-sale" disclosure rules requiring broker-dealers to include information about costs and conflicts of interest whenever investors bought financial products.[188] The rationale behind these information-forcing rules is to improve the functioning of markets by preventing fraud and empowering investors.

But in recent years, disclosure-oriented reforms have come under harsh criticism. A number of scholars have argued that increasing the quantity of disclosure to investors and consumers is an ineffectual response to the problems that regulators care about. Information-forcing rules, in this view, tend to inhibit market efficiency, not promote it.[189]

The criticisms of disclosure-oriented regulation can be categorized into two groups. First, one group of scholars, who might usefully be termed "disclosure optimists," argue that markets will naturally lead to an efficient level of disclosure.[190] Disclosure optimists

---

[187] *See* Jeffrey N. Gordon, *Governance Failures of the Enron Board and the New Information Order of Sarbanes Oxley*, COLUM. L. & ECON. WORKING PAPER NO. 215 (2003).

[188] *See* Nicholas S. Di Lorenzo, *Defining a New Punctilio of an Honor: The Best Interest Standard for Broker Dealers*, 92 B.U. L. Rev. 291 (2012).

[189] *See* Geoffrey A. Manne, *The Hydraulic Theory of Disclosure Regulation and Other Costs of Disclosure*, 58 ALA. L. REV. 473, 474 (2007) (arguing that "mandatory disclosure in certain circumstances will have undesirable consequences—costs born by shareholders—that could outweigh its perceived benefits").

[190] *See* Michael C. Jensen & William H. Meckling, *Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure*, 3 J. FIN. ECO. 305, 306 (1976) (arguing that firm managers voluntarily provide accounting reports and hire independent auditors in order to, among other things, attract investors to their firms; Stephen A. Ross, *The Economics of Information and the Disclosure Regulation Debate*, in ISSUES IN FINANCIAL REGULATION 177, 184-85 (Franklin R. Edwards ed., 1979) ("[I]n a competitive market (with no mandated disclosure), the managers of firms . . . will have a strong self-interest in disclosing relevant information . . . .");; Paul M. Healy & Krishna G. Palepu, *Information Asymmetry, Corporate Disclosure, and the Capital Markets: A Review of the Empirical Disclosure Literature*, 31 J. Accounting & Econ. 405, 411 (2001) ("Absent market imperfections or externalities, firms have incentives to optimally trade off the costs and benefits of voluntary disclosure, and to produce the efficient level of information for investors in the economy."); Troy A. Paredes, *Blinded by the Light: Information Overload and Its Consequences for Securities Regulation*, 81 WASH. U. L.Q. 417, 421 (2003) ("Critics . . . argue that a company will voluntarily disclose information that investors demand in order to reduce its cost of capital and avoid any discount that the market might apply to the company's stock price if investors think that they have too little information to evaluate the company and its securities properly or, worse yet, if investors think that the company is hiding something."); Pablo Kurlat & Laura Veldkamp, *Should We Regulate Financial Information?*, 158 J. ECON. THEORY 697 (2015); Jonathan R. Macey, *Efficient Capital Markets, Corporate Disclosure and Enron*, 89 CORNELL L.

view information asymmetries as problems that are entirely resolvable through private-sector mechanisms. The logic is as follows. Buyers that lack information about the relative quality of financial products (say, asset management services) will refrain from buying those products until they have received credible information about their value. While providers of low-quality financial products will have an interest in maintaining information asymmetries between themselves and buyers, providers of high-quality financial products will not.[191] These "reputable" financial services firms will be willing to provide the necessary amount of information to signal to prospective buyers that their products are of high quality. This disclosure will eliminate any material and harmful information asymmetries in the market. Thus, in this view, markets will naturally correct any information asymmetries that are harmful to consumers and investors. According to disclosure optimists, then, disclosure-oriented regulation will either be duplicative (to the extent that it requires firms to disclosure information they already are providing) or harmful (to the extent that it require firms to disclosure information that counterparties neither need nor desire).

But a second group of "disclosure pessimist" scholars have criticized disclosure-oriented financial regulation on another front: consumers and investors do not have the cognitive capacity to process the information that is disclosed.[192] In this view, markets may well *not* lead to effective disclosure to counterparties, but enacting mandatory

---

REV. 394, 411 (2004) ("Economic theory as it relates to disclosure dictates that high-quality corporations seeking to attract capital have strong incentives to distinguish themselves from rivals because investors that cannot distinguish high- from low-quality issuers will not pay more for securities from high-quality issuers.").

[191] Of course, the low-quality providers might have an interest in providing *false* information to investors and consumers, but, under the optimistic theory of disclosure, prohibitions against fraud should prevent this kind of behavior. In addition, high-quality providers could remedy this problem even in the face of fraudulent disclosure by hiring independent auditors to confirm the accuracy of their own, true disclosures.

[192] *See* Omri Ben-Shahar & Carl E. Schneider, *The Failure of Mandated Disclosure*, 159 U. PA. L. REV. 647, 705 (2011) (arguing that mandated disclosure's assumptions "that people want to make all the consequential decisions about their lives, and that they want to do so by assembling all the relevant information, reviewing all the possible outcomes, reviewing all their relevant values, and deciding which choice best promotes their preferences" . . . "so poorly describe[] how human beings live that mandated disclosure cannot reliably improve people's decisions and thus cannot be a dependable regulatory mechanism"); BEN-SHAHAR & SCHNEIDER, *supra* note 154, at 33-54; Henry T.C. Hu, *Too Complex to Depict? Innovation, "Pure Information," and the SEC Disclosure Paradigm*, 90 TEX. L. REV. 1601, 1607 (2012) (arguing that "the complexities of financial innovation may be so daunting that no one at the [company] understands such complexities"); Paredes, *supra* note 190, at 419 (arguing that investors may be "overloaded with information and make worse decisions than if less information were made available to them").

disclosure rules will not solve the problem either. First, consumers and investors face an acquisition problem: they may not be aware of the existence or availability of much relevant information, such as OCC guidelines or SEC alerts or NIST frameworks, even if this information is disclosed.[193] Second, consumers and investors face an overload problem: many of the disclosures they are provided are so detailed and complex—consider, for example, the extensive information provided in the most basic SEC disclosure document, the annual report on Form 10-K—that they are unable to understand and analyze these disclosures.[194] Finally, consumers and investors face an accumulation problem: they have access to so much information from so many different sources that, given limited time and cognitive resources, it is impossible for them to review and understand all of the information that is provided to them.[195] All of these issues are part of a larger conceptual problem related to the *use* of disclosure. After all, the purpose of disclosure is to prevent substantive problems, such as information asymmetries or fraud. If mandated disclosure does not lead to better decisionmaking, then it is both an ineffectual use of scarce regulatory resources and a harmful imposition of burdensome regulatory costs.

The arguments against mandated disclosure leveled by both disclosure optimists and disclosure pessimists provide compelling reasons for regulators to be cautious in enacting broad information disclosure rules on markets. Without a detailed understanding of existing, privately-negotiated disclosures, and the behavioral tendencies and capacities of disclosure recipients, lawmakers may well be wise to refrain from intervening in well-functioning industries. Intervention in such cases may end up exacerbating the problems that disclosure is intended to solve.[196] But, for a number of reasons, the critiques of the disclosure optimists and the disclosure pessimists are less compelling in the fintext context.

The argument of disclosure optimists that markets will naturally lead to efficient levels of disclosure in fintech demonstrates a misunderstanding of the dynamics within fintech industries. First, market mechanisms for information work less well for the kinds of complex products that fintech offers.[197] It is one thing to expect homebuyers to demand information about defects in their homes (one

---

[193] *See* Ben-Shahar & Schneider, *supra* note 192, at 689-90.

[194] *See id*., at 687-89.

[195] *See id*., at 689-90.

[196] *See id*., at 690.

[197] *See* John C. Coffee, Jr., *Market Failure and the Economic Case for a Mandatory Disclosure System*, 70 VA. L. REV. 717 (1984); Merritt B. Fox, *Retaining Mandatory Securities Disclosure: Why Issuer Choice Is Not Investor Empowerment*, 85 VA. L. REV. 1335 (1999)

common example given of market demand for information to resolve information asymmetries). It is another to expect investors in virtual currency platforms to demand information about the risks of blockchain—even computer scientists disagree about the functioning of the technologies underlying many virtual currencies. Even knowing the right questions to ask requires significant levels of technical knowledge that most investors do not have. Second, even if the dynamics of supply and demand will eventually lead to better disclosure of the quality of fintech products, this process takes time and will itself involve significant transaction costs. In a sector where new fintech products are launched, and new actors are created, on a nearly daily basis, transaction costs for information production are likely to be high. Third, even if market mechanisms function properly, and transaction costs can be minimized, it is unclear that proper levels of information will be disclosed by fintech actors. The information that investors will demand, and that companies will provide, will be determined based on the investment concerns of participants in the market. But, as described above, fintech also presents systemic risk concerns that affect the economy more broadly and not just the immediate participants in the industry. These externalities are potentially large and likely growing. By leaving out the interests of third parties, market mechanisms for disclosure will lead to suboptimal levels of information from the perspective of society more generally. Thus, there are several reasons to believe that market mechanisms for information will function poorly in fintech.

What, then, to make of the argument of disclosure pessimists, who view consumers as generally incapable of using disclosures to improve their decisionmaking? This is certainly a powerful critique of disclosure as a panacea for undesirable behavior in an industry. It seems quite clear that it is beyond the capacity of most, if not all, consumers to review the extensive amount of disclosure provided to them in nearly every aspect of their online lives, from terms of service pages to clickwrap to dispute resolution agreements. But to say that disclosure is sometimes ineffective, or even that it may lead to worse behavior than if no disclosure had existed, is not to say that it cannot be useful in areas in which large information asymmetries exist. More importantly, a number of insights from behavioral psychology suggest that there are ways to improve disclosure in order to make it more effective in altering consumer behavior. For example, consumers may be "primed" to review disclosures in a more analytical light through a variety of debiasing methods aimed at mitigating or eliminating cognitive shortcomings.[198] These might include "consider the opposite"

[198] *See* Christine Jolls & Cass R. Sunstein, *Debiasing Through Law*, 35 J. LEGAL

disclosures asking consumers or investors to assess their decision under differing assumptions[199] or "pros and cons" requirements forcing consumers to proactively list both the benefits and costs of their financial transactions.[200] Additionally, consumers and investors could be encouraged to make better use of disclosures through legal obligations on firms to use certain "framing" techniques.[201] These framing obligations might require firms to provide consumers and investors with immediate and repeated disclosures about the potential negative consequences of their behavior.

All of this is not to say that mandated disclosure can completely eliminate cognitive biases or uninformed decisionmaking by consumers. It certainly cannot. But given the large information asymmetries currently existing in the industry, even a marginal improvement in the capability of outsiders to assess the benefits and risks of their financial transactions could provide significant benefits in the efficiency, fairness and stability of these markets.

Perhaps just as importantly, information forcing is not solely about improving the decisionmaking of actors within fintech markets. It is also about enabling and strengthening the capacity of regulators to monitor and constrain those markets. And while regulators are not immune to the types of behavioral biases that afflict private sector actors, their role as governmental actors puts them in a unique position to correct misbehavior as it develops. Improving information disclosure

---

STUD. 199, 201 (2006) (providing a general account of how law may debias people's boundedly rational behavior); Carla C. Chandler et al., *It Can't Happen to Me...Or Can It? Conditional Base Rates Affect Subjective Probability Judgments*, 5 J. EXPERIMENTAL PSYCHOL.: APPLIED 361, 365-67 (1999) (; Linda Babcock & George Loewenstein, *Explaining Bargaining Impasse: The Role of Self-Serving Biases*, 11 J. ECON. PERSP. 109, 110 (1997); Alexander J. Rothman & Marc T. Kiviniemi, *Treating People with Information: An Analysis and Review of Approaches to Communicating Health Risk Information*, 25 J. NAT'L CANCER INST. MONOGRAPHS 44, 45 (1999); Alexander J. Rothman et al., *Absolute and Relative Biases in Estimations of Personal Risk*, 26 J. APPLIED SOC. PSYCHOL. 1213, 1213-36 (1996). *But see* Sean Hannon Williams, *Sticky Expectations: Responses to Persistent Over-Optimism in Marriage, Employment Contracts, and Credit Card Use*, 84 NOTRE DAME L. REV. 733 (2009) (arguing that there are multiple reasons to doubt that debiasing strategies would be effective in a number of areas of law); Neil D. Weinstein & William M. Klein, *Resistance of Personal Risk Perceptions to Debiasing Interventions*, 14 HEALTH PSYCHOL. 132 (1995) (finding that the use of certain debiasing methods with respect to health risks led to increased prevalence and magnitude in cognitive biases).

[199] Charles G. Lord et al., *Considering the Opposite: A Corrective Strategy for Social Judgment*, 47 J. PERSONALITY & SOC. PSYCHOL. 1231, 1231 (1984)

[200] Karen Pezza Leith & Roy F. Baumeister, *Why Do Bad Moods Increase Self-Defeating Behavior? Emotion, Risk Taking, and Self-Regulation*, 71 J. PERSONALITY & SOC. PSYCHOL. 1250, 1264 (1996).

[201] *See* RICHARD H. THALER & CASS R. SUNSTEIN, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS 8 (2009).

for regulators may well involve mechanisms that are not typically seen in the private sector. One proposal that has seen growing support internationally is the creation of "regulatory sandboxes" for fintech firms.[202] These governmental initiatives would encourage (or potentially require) fintech firms to launch new financial products under the active supervision of financial regulators. In return, fintech firms would receive reduced regulatory burdens and registration requirements. The benefits of a sandbox approach to fintech regulation are multifold, including, perhaps most importantly, that it would allow regulators to gain insight into the workings of financial products and do at an early stage, before risks materialize into real-world losses.

B. *Cybersecurity and National Security*

A second objection often lodged against efforts to improve the cryptographic power of technologies is that these efforts may raise national security concerns. This Article has argued that financial regulators must enact rules requiring fintech firms to adopt a set of best practices for cybersecurity to ensure that their systems are protected from unauthorized intrusions. Such a rule, this Article has argued, would promote efficient markets, protect consumers, and strengthen stability. But cybersecurity is not an unalloyed good. Governments may at times perceive an interest in "breaking" or penetrating the security protocols of financial firms in order to gain access to valuable information. Such governmental interests may clash with privacy and system integrity goals. In these scenarios, it is unclear that cybersecurity should always win out. Indeed, if all financial services were to have fully anonymous and impenetrable systems, it would be impossible for regulators to discover wrongdoing in the financial system.

The tradeoff between cybersecurity and national security has risen to national prominence following several recent disclosures about the ability (or in some cases inability) of governments to access information stored or transmitted on computers, mobile phones or other online platforms. In one incident that received substantial coverage in the media, the Federal Bureau of Investigation sought to access data stored on the iPhone of one of the terrorists in the 2015 attack in San

---

[202] *See* Max Colchester & Rachel Witkowski, *U.K. Takes Novel Approach on Fintech*, WALL ST. J., Apr. 11, 2016; Michelle Chen & Michelle Price, *Hong Kong to Launch Banking Fintech "Sandbox" As Rivals Pull Ahead*, REUTERS, Sept. 6, 2016; Clare Dickinson, *Bank of England Gathers Minds for Fintech Salon*, FIN. NEWS, Mar. 17, 2017. For a discussion of how regulatory sandboxes might be implemented in the United States, see Hilary J. Allen, *A US Regulatory Sandbox*, unpublished manuscript, available at www.ssrn.com/abstract_id=3056993.

Bernardino that killed 14 people and injured 22 others.[203] Apple, the maker of the phone, protested that the FBI's demands that it create such a backdoor into the phone by breaking its encryption would have harmful and unintended effects for future privacy, noting that "[i]n the physical world, it would be the equivalent of a master key, capable of opening hundreds of millions of locks — from restaurants and banks to stores and home."[204] Eventually, the FBI relented on its demand after it found hackers that managed to break the encryption on their own, at a reported cost of under $1 million.[205]

The dispute between FBI and Apple is symptomatic of the basic tension between cybersecurity and national security.[206] Efforts to strengthen encryption within a system will naturally tend to increase privacy and stability, thus protecting the system from hacking or other unauthorized intrusions. But those same efforts will also tend to reduce the ability of national governments to gain access to those systems. And there are legitimate reasons for national governments to do so. These reasons include, but are certainly not limited to, a desire to monitor communications by criminals and terrorists, prevent money laundering and other illicit activities, locate assets and accounts of citizens that are evading taxes, and protect consumers from fraud. In each of these areas, the government's ability to pursue its policy priorities comes squarely into conflict with basic cybersecurity priorities.

This tension is particularly visible in fintech for several reasons. First, many fintech industries, and in particular the virtual currency market, focus on providing both confidentiality and irreversibility for the transactions executed on their networks. Bitcoin has been the currency of choice for hackers, drug cartels and human traffickers because of its anonymity.[207] New virtual currencies such as monero

---

[203] *See* Daisuke Wakabayashi, *U.S. and Apple Dig In for Court Fight Over Encryption*, WALL ST. J., Feb. 17, 2016.

[204] *See* Ellen Nakashima, *Apple Vows to Resist FBI Demand to Crack iPhone Linked to San Bernardino Attacks*, WASHINGTON POST, Feb. 17, 2016.

[205] *See* Mark Hosenball, *FBI Paid Under $1 Million to Unlock San Bernardino iPhone*, REUTERS, Apr. 28, 2016.

[206] *See* Neal Kumar Katyal, *Criminal Law in Cyberspace*, 149 U. PA. L. REV. 1003, 1047-71 (2001); Jay P. Kesan & Carol M. Hayes, *Bugs in the Market: Creating a Legitimate, Transparent, and Vendor-Focused Market for Software Vulnerabilities*, 58 ARIZ. L. REV. 753 (2016); Martha Finnemore, *Constructing Norms for Global Cybersecurity*, 110 AM. J. INT'L L. 425 (2016); Amanda N. Craig, Scott J. Shackelford & Janine S. Hiller, *Proactive Cybersecurity: A Comparative Industry and Regulatory Analysis*, 52 AM. BUS. L. J. 721 (2015); Derek E. Bambauer, *Ghost in the Network*, 162 U. PA. L. REV. 1011 (2014); McKay Cunningham, *Privacy in the Age of the Hacker: Balancing Global Privacy and Data Security Law*, 44 GEO. WASH. INT'L L. Rev. 643 (2012).

[207] *See* Joshua Bearman & Tomer Hanuka, *The Rise and Fall of Silk Road*, WIRED, May 2015.

promise even greater anonymity to their users.[208] Second, the vulnerability of fintech to hacking, and the potential harm from intrusions into fintech systems, makes cybersecurity an essential component of fintech's business model. If robo-advisors or e-payment services were known to have had breaches of their services, it could potentially destroy the companies involved, especially if those breaches led to customer losses.[209] Consumer confidence about the strength of cybersecurity is, thus, of tremendous value to fintech firms.[210] Third, the governmental interest in accessing fintech networks is high. As greater and greater proportions of financial transactions are handled by fintech firms, governments seeking to regulate and monitor the world of finance will seek ways to gain greater insight into its functioning. They may well attempt to break the encryption in virtual currencies and payment systems in order to identify wrongdoers and track down illicit funds.[211] They may also try to force robo-advisors around the world to provide information on customer accounts.[212]

Thus, any legal regime that aims to strengthen fintech's encryption protocols risks weakening governments' ability to pursue other policy priorities.[213] Society may be better served by creating a financial system that is easily accessible and monitorable than in ensuring its resilience and impenetrability from cyberattacks. If the cost of increasing fintech's cybersecurity is that governments can no longer track illicit flows of capital, then government may well prefer to prohibit (not encourage) such developments.

This dichotomy between cybersecurity and national security is unsurprising. It has been seen over and over again in debates about civil liberties, government powers, public safety, and the war against terrorism.[214] The proper balance between protecting the privacy of individuals and empowering the government to prevent harm to the public is still a matter of controversy, and it will likely continue to be one.

But the position that cybersecurity necessarily comes at a cost to

---

[208] *See* Evelyn Cheng, *Dark Web Finds Bitcoin Increasingly More of a Problem Than a Help, Tries Other Digital Currencies*, CNBC, Aug. 29, 2017.

[209] *See* Clare O'Hara, *A Robo-Adviser's Best Defence Against Cyber Threats? The In-House Hacker*, GLOBE & MAIL, May 15, 2017.

[210] *See* BBVA, DATA AND CYBERSECURITY, KEYS TO GENERATE CONFIDENCE IN A DIGITAL BANK (2017).

[211] *See* John Bohannon, *Why Criminals Can't Hide Behind Bitcoin*, SCIENCE MAGAZINE, Mar. 9, 2016.

[212] *See* Tracy A. Kaye, *Innovations in the War on Tax Evasion*, 2014 B.Y.U. L. REV. 363 (2014).

[213] *See* Sean Kanuck, *Sovereign Discourse on Cyber Conflict Under International Law*, 88 TEXAS L. REV. 1571, 1590 (2010).

[214] *See* Katyal, *supra* note 206, at 1047-71.

national security is untenable. There are many commonsense rules that can both allow financial transactions to be processed securely and protect important national security interests. For example, incentivizing financial firms to identify flaws in software that would allow unauthorized intrusions makes sense regardless of whether our goal is to protect privacy or prevent crime. Requiring fintech firms to report when they have been the subject of a hacking attack (whether successful or not) contributes to consumer privacy interests and alerts law enforcement to potentially unlawful activity. Creating a set of cybsecurity best practices and offering "cyber-hygiene" scans to fintech firms would help ensure financial stability and mitigate concerns about criminal intrusions.

Of course, difficult questions about particular fintech technologies will arise—and indeed, already have.[215] Should governments have the power to seize virtual currency assets that are known to have been the product of criminal activity, even if doing so requires changes to the virtual currency's underlying code? Must online payment systems create backdoors that allow prosecutors to identify the senders and recipients of financial transactions? Can governments prohibit the creation of fintech technologies that are truly impossible to decrypt or intercept? Creating a truly comprehensive law of fintech will require answers to these questions. But as with any emerging technology of the size and importance of fintech, regulation will never be able to perfectly satisfy all stakeholders. Instead, it should aim to effectively achieve its primary goals—in this case, efficiency, fairness, and stability. Better cybersecurity would be a good start.

CONCLUSION

The rise of the Bitcoin era has reshaped the landscape of finance. Fintech firms have challenged the conventional wisdom about the way that financial services are provided and how financial institutions must look. They have pioneered innovations in the world of wealth management, capital formation, and virtual currencies. In all of these areas, fintech firms have relied a set of core characteristics to compete with longstanding incumbents—they utilize disaggregated networks to provide financial services to consumers and investors; their services are

[215] It has been reported, for example, that the FBI, the Drug Enforcement Administration, and other U.S. law enforcement agencies spend hundreds of thousands of dollars annually attempting to track virtual currency transactions through private, third-party contracts. Perhaps the most prominent example of law enforcement authorities stripping anonymity protections from a virtual currency occurred in the Silk Road case, in which the infamous online black market was shut down and its users identified by the FBI. *See* Bearman & Hanuka, *supra* note 207.

heavily automated and often delegated to algorithms; and their industries are highly adaptable, responding rapidly to changes in demand. These features are in many ways a boon to the financial world, as they allow for lower costs and broader access to financial products. But they also present thorny problems for financial regulation. Fintech industries reduce the ability of financial markets to promote the efficient allocation of capital in the economy. They create greater opportunities for consumer abuse and investor fraud. And finally, they present a set of systemic risks that are distinct from, and in certain aspects greater than, the risks presented by traditional financial institutions. For all of these reasons, the Bitcoin era will require us to engage in a comprehensive rethinking of financial regulation. This reconceptualization of financial regulation must focus much more closely on improving information production in fintech markets, bolstering cybersecurity procedures among fintech participants, and balancing core priorities. If financial regulators use these guideposts to hone their regulatory mechanisms in coming years, they will do much to make financial regulation relevant again.