FINTECH LAW

THE CASE STUDIES

BY HOWELL E. JACKSON AND MARGARET E. TAHYAR

Copyright © 2020 President and Fellows of Harvard University.

All rights reserved. This book or any portion thereof may not be reproduced or used in any manner whatsoever without the express written permission of the publisher except for the use of brief quotations in a book review.

ISBN: 978-0-578-72584-0

Cover art by Shir Warr.

Author Biographies

Howell E. Jackson

Howell E. Jackson is the James S. Reid, Jr., Professor of Law at Harvard Law School. Since joining the Harvard faculty in 1989, he has authored numerous scholarly articles and other publications on financial regulation. He has also advised government officials on regulatory policy in the United States and around the world. Jackson is the founding editor of the SSRN Regulation of Financial Institutions eJournal and a member of the academic advisory panel for the Cambridge University Press financial and corporate law series. Since 2005, Jackson has been a trustee of CREF and affiliated TIAA-CREF mutual funds. He is also on the board of Commonwealth, a non-profit focused on improving financial security of low and moderate income households. Professor Jackson occasionally serves as consultant to or expert witness for U.S. regulatory authorities and other governmental bodies. During the 1983 October Term, he was a law clerk for Associate Justice Thurgood Marshall. Additional information on Professor Jackson's activities is available at http://hls.harvard.edu/faculty/directory/10423/Jackson.

Margaret E. Tahyar

Margaret E. Tahyar is a partner in the Financial Institutions Group at Davis Polk & Wardwell LLP. Since joining Davis Polk in 1989, she has advised financial institutions on a wide range of regulatory reform, enforcement, and transactions. In addition to her full-time law practice, Tahyar teaches part-time at Harvard Law School (Bruce W. Nichols Lecturer in Law) and has also taught as an adjunct at Columbia Law School. She writes and speaks frequently and is recognized as a leading lawyer in the area of financial regulation (band 1 in Chambers and National Law Journal's Outstanding Women Lawyers 2015). After becoming a partner in 1997, she spent twelve years in Europe, first in London and then in Paris. During the 1988 October Term, she was a law clerk for Associate Justice Thurgood Marshall. Additional information on Ms. Tahyar's activities is available at http://www.davispolk.com/lawyers/margaret-tahyar.

Preface

Whether in response to roboadvising, artificial intelligence, or digital assets and cryptocurrencies, policymakers around the world have made it a top policy priority to supervise the exponential growth of financial technology (or "Fintech") in today's economy.

But regulating financial innovation is hard, in part because the field of Fintech law is inherently beset by a "trilemma" that has confounded the regulatory community for generations. (*See* Chris Brummer and Yesha Yadav, *Fintech and the Innovation Trilemma*, 107 GEORGETOWN L. J. 235, 2019.) When seeking to provide clear rules, maintain market integrity, and encourage financial innovation, regulators have long been able to achieve, at best, only two out of these three goals. The history of financial regulation reveals cycles over the course of which various combinations of priorities are emphasized. Adding in the inherent interdisciplinarity and tradeoffs involved in deploying and supervising new financial technology, Fintech law has become so complex that more than a few experts have come to wonder quietly whether or not the emerging field is in fact "unteachable."

Yet, this wonderful volume of case studies—covering fourteen diverse nooks and crannies of the Fintech ecosystem—proves this is far from the case. Exploring the technology and rationales underpinning different policies and the nuanced spectrum of formality and jurisdictional boundaries guiding financial services providers, the authors compile a unique overview of the industry through snapshots of the difficult work of policymaking. They then encourage the reader to think hard about not only the path taken, but also the paths available, when encountering the portfolio of technical and regulatory challenges presented in each scenario.

As such, *Fintech Law: The Case Studies* is an essential to the understanding of Fintech law—for students, scholars, and practitioners in the field. It highlights not only the contingency of rulemaking, but also the need for flexible and agile decision-making if indeed law is to keep pace with the transformational changes reshaping finance.

Chris Brummer, JD, PhD
Washington, DC
July 2020

Table of Contents

Teaching the Law of Fintech

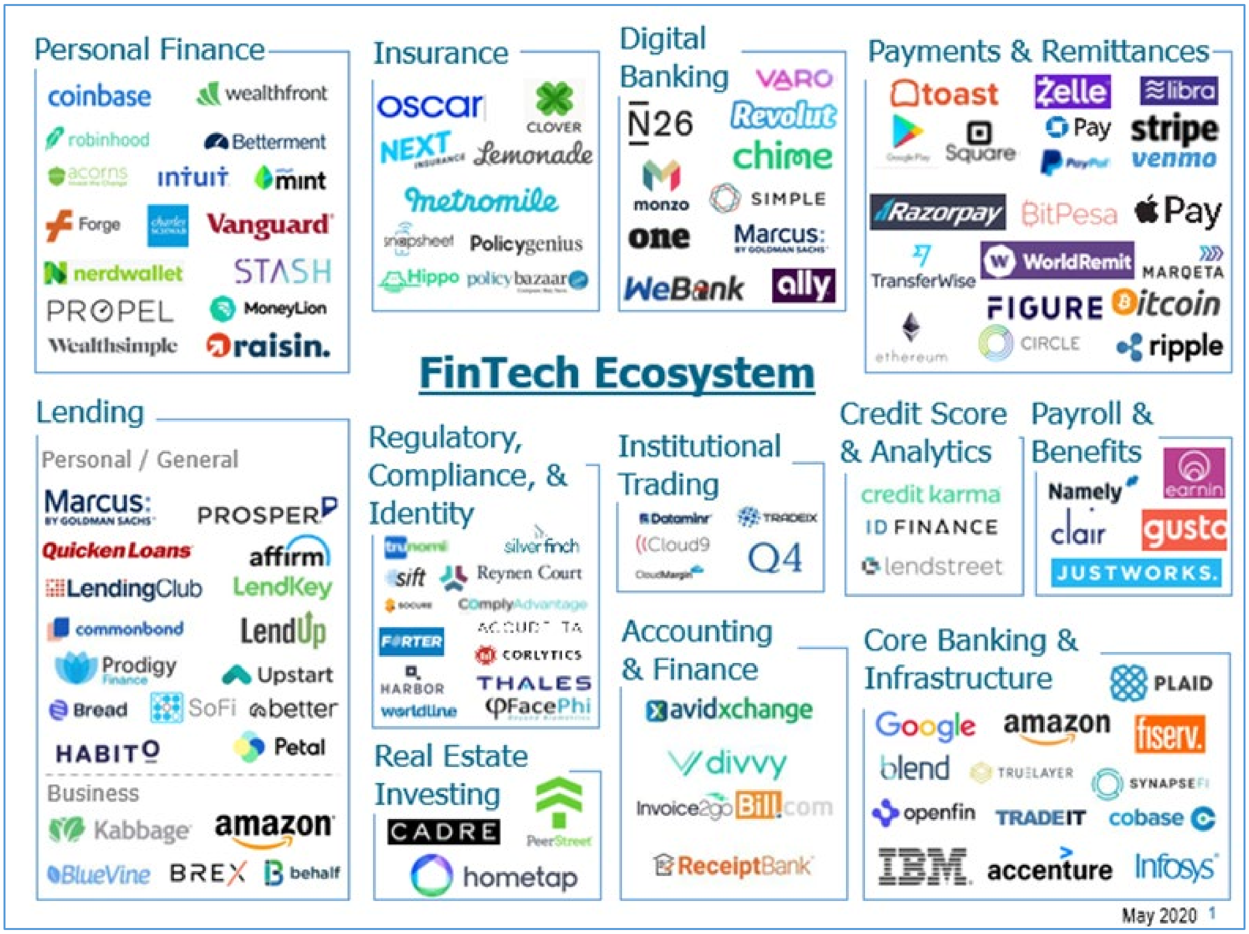
HOWELL E. JACKSON AND MARGARET E. TAHYAR

We developed the case studies in this book over the course of two years in teaching a pair of Fintech modules at Harvard Law School. Our goal with these modules was to introduce our students to the digital transformation of financial services now underway. From the start, we have taken the view that Fintech is an umbrella term covering many different phenomena and a wide range of business models. The law of Fintech is nothing like the bodies of law typically associated with law school courses such as property, contracts, or torts. Fintech itself is the by-product of on-going innovations in digital technologies including communications networks, computational power, and data analysis. Fintech's influence is not limited to a single set of financial products or a particular area of legal doctrine or regulatory policies. Instead, Fintech touches every corner of the world of finance and implicates every line of business. The law of Fintech is similarly broad. To introduce students to this new domain, we chose to develop a series of case studies modeled on the Harvard Business School case study method, but adapted for the teaching of law. In each case study, students are put into an institutional context that a young lawyer might face at a law firm, government agency, congressional office, or other setting in which practicing attorneys might expect to confront problems of law and policy with respect to innovations in Fintech.

The Fintech Ecosystem

Given the pervasive character of Fintech innovation, some have suggested the term Fintech, while catchy, is so broad and covers so much that it loses its meaning. Certainly, Fintech as an umbrella term refers to the many different innovations with the potential to disrupt or challenge the legacy financial services firms and existing regulatory practices. It refers to those who partner with the legacy financial services sector and it refers to investments made by the financial sector in new technologies. Fintech encompasses at least a dozen different areas of innovation—so far.

It includes marketplace and algorithmic lenders, robo-advisors and high-frequency trading strategies, an entire range of payments, both businesses-to-business and business-to-consumer, as well as insurance by app, digital banks, cryptocurrencies, central bank digital assets, credit scoring and analytics, payroll and benefits systems, real estate investing, compliance software and other forms of Regtech, blockchain, core infrastructure, bank services, and many more products and services still to emerge. There is not a Fintech, but an ecosystem of Fintechs. In the figure below, we lay out one possible taxonomy for organizing how many of the most familiar current Fintech brands fit into this rapidly evolving ecosystem.



The uniting thread in each of the many different innovations is the use of data, automation, interconnectivity, and, sometimes, artificial intelligence. It is in essence one manifestation of the digital transformation that we are experiencing on a global scale throughout society.

Our Approach to the Law of Fintech

The wide range of the Fintech ecosystem means that the law of Fintech and the public policy issues relevant to its regulation are as varied as Fintech innovations themselves. At a theoretical level, one could ask three basic questions about the law and polices relevant to Fintech innovations:

1. With which aspects of our current, and highly fragmented, system of financial regulation must a particular Fintech innovation comply? In other words, where within the existing regulatory perimeters does the innovation fall?
2. Once the applicable regulatory perimeters have been identified, a separate question arises as to whether the current legal framework provides for effective and equitable governance of the Fintech in question or is the current legal framework in some ways inadequate or inappropriate?
3. Finally, and often critically, what is the impact of a Fintech innovation on incumbent firms and other stakeholders and does that impact raise public policy concerns or points of political or bureaucratic resistance that a Fintech entrepreneur must be prepared to overcome?

The case studies in this eBook are designed to explore these questions in fourteen different contexts and the answers to the questions vary from context to context and are often hotly contested. In some cases, the applicable regulatory perimeters are clear but in other cases the application of jurisdictional boundaries are highly uncertain. Existing legal frameworks work passably well for some Fintech innovations, but in other contexts the alignment between current requirements and innovations are poor, in some cases already prompting legal changes. Some Fintech innovations face laws that are not adapted to their business model and some are able to rely upon existing legal frameworks in ways that are new and unanticipated. Some Fintechs pose existential challenges to incumbent firms and other stakeholders, and face considerable political resistance. Many share data governance and privacy issues. Some Fintech innovations—especially in the payments space—raise deep questions about sovereign powers and the appropriate division of responsibilities between public entities and private parties. As we developed the case studies, we also discovered that sophisticated practitioners of the law of Fintech must also possess the classic skill sets of business law, including knowledge of contract law and the art of negotiation, as well as the capacity to navigate supervisory interactions along with more formal investigations and enforcement actions plus the ability to advocate for client interests before regulatory leadership as well as legislative bodies. In short, to be an effective and responsible Fintech lawyer, one must be an effective and responsible lawyer.

For those unfamiliar with the Harvard Business School case study method, a few words of introduction may be helpful. Do not be confused by the similarity in names with the famous Langdell case study method that dominates legal teaching. Dean Langdell revolutionized the study of law by abandoning the traditional lecture and asking students to read excerpts from a limited number of judicial decisions and then distill underlying common law principles from those readings. It emphasized reasoning by analogy and thinking like a lawyer. The Harvard Business School case study is entirely different. It presents students with a real life business scenario with ample institutional context and asks students to make and defend choices about what the actors in the scenario should do next. The case studies developed in this book similarly present institutionally rich and realistic business, legal, and policy scenarios for law students. We have attempted to structure these scenarios to provide a good reflection of ongoing issues in the Fintech ecosystem today.

Each of the fourteen case studies in this book are designed to illustrate a different part of the Fintech ecosystem. Typically, the case studies consist of a 20- to 30-page cover memo along with a limited number of attachments that provide an overview of the issues to be explored. Each case study gives students a specific assignment. Almost all of the case studies also include a number of links to online resources providing additional details on each major issue. In our Fintech modules, we typically assign one team of three to five students to take the lead in presenting the case study to the rest of the class with the expectation that the team members would work through all of the relevant online links. In many cases it is also possible to break up the assignments among several different student teams, with each team addressing a subset of issues and reviewing only a portion of the online resources. We expect all students to read through the cover memo and attachments and be prepared to engage in class discussions. (A separate teacher's manual for instructors provides the pedagogical goals for each case study and suggestions on assignment options.)

In our view, the student presentations—typically made with a limited number of PowerPoint slides—are a critical component of the case study pedagogy. PowerPoint presentations are an increasingly important skill set for practicing attorneys. Even though not yet a standard component of legal education, most young attorneys will make many more PowerPoint presentations to clients than they will make oral arguments of the sort practiced in moot court exercises. We have found that our students have welcomed the opportunity to learn more about making presentations to clients and senior attorneys and we try to give advice about basic presentation skills before each team's presentations as well as feedback sessions to debrief on what went well and what might be improved thereafter. In our experience, these interactions are an important and welcomed aspect of experiential learning and are necessary for courses of this sort to qualify as experiential learning for purposes of bar requirements.

These case studies were largely developed before the COVID-19 pandemic triggered the move to remote learning. In the Spring of 2020, we did, however, have a chance to experiment with a few of the case studies in a Zoom classroom setting. The basic structure worked quite well as student teams were able to collaborate on presentations before class and the Zoom screen sharing function accommodates student presentation. For professors comfortable with Zoom breakout sessions, this feature allows groups of students to confer amongst themselves during class sessions and offer more considered reactions to student presentations.

Turning to the contents of the case studies themselves, here is a brief overview:

In Part I, we explore topics related to marketplace lending and the Fintech charters. The first case study explores challenges that Lending Club experienced very early in its business life in negotiation of the jurisdictional boundaries between loans and securities. In addition to offering a helpful introduction to regulatory perimeters, the Lending Club: 2008 case study introduces students to marketplace lending. The Strategic Options and Legal Risks for Elite ReFi, Inc. case study uses the backdrop of the *Madden* case to bring into relief the legal risk decisions a startup marketplace lender might need to make. The Fintech Charters case study places students into the role of Senate staffers (both Democratic Senators and Republican), Federal Reserve staffers, and state banking agency staffers to brief on whether the Senate Banking Committee should pass a bill authorizing a Fintech charter.

In Part II, we tackle topics related to capital markets. The Robo-Advising case study puts students in the role of attorneys working at the SEC and FINRA asking them to consider how these agencies should respond to a young entrepreneur's proposal for a robo-advising startup with only one employee. The case study Market Manipulation: Definitional Approaches considers whether and how the SEC might revise the definition of manipulation in light of developments in algorithmic trading. The Algorithmic Trading Strategies case study addresses problems associated with algorithmic trading and a possible initiative by the CFTC to require firms to disclose confidential information about their algorithms. The last case study in Part II, Regulating Crypto Assets: Securities and Commodities, explores the allocation of regulatory responsibilities between the SEC and CFTC over digital assets from the perspective of a bipartisan think tank attempting to develop a policy position on the issue.

In Part III, we consider a number of consumer products. The Employee Benefits – Emergency Savings Account case study, which has been prepared in conjunction with the non-profit Commonwealth, explores how a new automated product that encourages emergency savings can be created and employers encouraged to adopt it. Machine Learning in the Underwriting of Consumer Loans explores the issues of disparate impact in artificial intelligence and credit decisions and the students act as a team of staff attorneys briefing the CFPB leadership on potential legal frameworks for supervising and enforcing algorithmic accountability in credit lending.

Part IV deals with payments. The case study on Mobile Payments for the Developing World examines what advice the World Bank should give to developing countries interested in promoting new mobile payment systems, while the Digital Currencies scenario explores the pros and cons of establishing a central bank digital currency from the perspective of Federal Reserve Board staff.

Part V takes up issues of customer information and privacy. The first case study, Regulating Consumer Permissioned Access to Financial Data, explores from the perspective of a presidential campaign the ability of consumers to control the sharing of personal financial information with Fintech startups in the face of restrictions on data sharing often put in place by incumbent firms. The next case study, Anti-Money Laundering and Blockchain Technology, asks students to take the perspective of FinCen lawyers reviewing industry proposals to modify AML requirements to facilitate the use of blockchain and other data sharing arrangements in order to reduce compliance costs and improve efficiencies. CLOUD Act Enforcement, the final case study, puts students in the position of attorneys in the U.S. Justice Department considering the application of the CLOUD Act to the collection of financial data located in the European Union and subject to the requirements of the GDPR.

Legal Background & Academic Literatures

One of the challenges of devising a course built around case studies is making sure that students have a sufficient grounding of the legal structures that govern the business activities in question. Given the broad scope of the Law of Fintech, this is a nontrivial matter. We attempt to address the concern in several ways.

First, most of the case studies contain a large number of supplemental on-line sources that often include a good deal of legal context. These materials are especially important for students on teams making presentations as they require good bit of background for their work. As a group, these appendices include some of the most influential and helpful academic articles written on Fintech issues in recent years.

Second, we make available to students more general treatments of financial regulation. We typically begin each semester with a review of the history of financial regulation in the United States and an explanation of its regulatory architecture both at the Federal and State level. We rely heavily on Chapters 1.2 and 1.3 of Barr, Jackson & Tahyar*, Financial Regulation: Law and Policy* (Foundation Press, 2d ed. 2018), the individual chapters of which can be purchased digitally from the publisher. In the Spring of 2020, we also assigned students chapters from Chris Brummer's most excellent *Fintech Law in a Nutshell* (West Academic Publishing 2019), which offers good coverage for many of the legal issues explored in our case studies.

Third, and as a second chapter of these Introductory Materials, we have included a slightly expanded version of a short conference piece: Howell E. Jackson, *The Nature of the Fintech Firm*, 61 WASH. U. J. LAW & POL'Y 9 (2020). This essay offers a Coasean analysis of Fintech innovations, explaining recent developments as the product of new technologies for dealing with information and uncertainty. The essay offers one way of conceptualizing the Fintech revolution, making references to many of the innovations explored in our case studies. The essay also includes citations to many of the most influential recent Fintech articles by other legal scholars and thus offers a gateway into scholarship in the area for students interested in pursuing a more academic perspective on the subject.

Finally, we have provided at the end of the book a link to an online bibliography of a more comprehensive list of recent academic work on Fintech law. We hope to update this bibliography from time to time and suggestions for additional publications to include are most welcome.

Acknowledgements

In putting together this eBook we have had the assistance and support of many colleagues and students.

We start by thanking the many practitioners and government officials who took the time to review earlier drafts of these case studies and, in most instances, to travel to Cambridge, Massachusetts, to sit in on our classes and play the role of senior partners or agency officials in responding to student presentations. The presence of outside visitors – many who have actually served as policy makers, business leaders or lawyers in comparable or even identical settings – was invaluable and in almost every case allowed us to refine the case studies and enhance the experiential learning component of the course. The role-play has made for some interesting and dynamic classroom discussions, both within the role-play itself and in the after-action wrap up discussions. To the extent that other professors can entice outside participation of this sort – whether in person or virtually – we would strongly encourage you to do so. Our honor list of outside contributors for whom we are deeply grateful include: Todd Baker; Isaac Boltansky; Elsa Broeker; Sylvia Brown; Christopher Brummer; Albert Chang; Leimin Chen; Jessie Cheng; Robert Cohen; Thomas Curry; Fred Davis; Elizabeth Davy; Mary Dent; Jason Ewas; Tim Flacke; Reuben Grinberg; Boris Khentov; Sharon Cohen Levin; Timothy Massad; Jai Massari; Nick Maynard; Annette L. Nazareth; Keith Noreika; Eric Pan; Will Paterson; Steven Polansky; Alan Rozenshtein; David Silberman; Paul Watkins; and Dirk Zetzsche.

We also are appreciative of the many students who participated in our two Fintech modules at Harvard Law School, suffering through the inevitable bumps and glitches that go with any new teaching materials. Their willingness and good humor in taking on novel assignments of considerable complexity were much appreciated. As always, undertakings of this sort are a gift from past students to future students.

We are especially grateful for the large number of research assistants and colleagues who contributed to the drafting and redrafting of the case studies and accompanying teaching notes. This work has stretched over multiple years and often entailed extensive revisions and reorientations. We are humbled by the effort and professionalism all of our co-authors have contributed to this effort. Our deep felt thanks to Nafisa Adama; Ryan Chan-Wei; Zachary Dearing; Christina Drakeford; Adam Fovent; Talia Gillis; Jonathan Greenacre; Kendall Howell; Chung-Chia Huang; Anzhelika Ishkhanyan; Craig Kennedy; Yinan Liu; Jai Massari; Carolina Rabinowicz; Madison Roberts; Carol Rodrigues; Anooshree Sinha; Corrine Snow; Adam Spiegel; Sebastian Steuer; Asher Trangle; Connor Tweardy; and Amy Zhang.

Finally, the team that helped us through the challenges of converting teaching materials into a publishable eBook deserve special thanks. The staff of the Harvard Law School Library as well as support personnel at Davis Polk have done yeoman's work on this book and without their contributions none of this would be possible. Our thanks to Nancy Cuevas-Martinez, Serena Doubleday, Sheri Keniston, Jocelyn Kennedy, Mary O'Rourke, Carolina Rabinowicz, and Vincenza Rico. Ryan Chan-Wei's final review of the entire manuscript and accompanying teaching notes was heroic and invaluable.

July 2020

The Nature of the Fintech Firm and its Implications for Financial Regulation

HOWELL E. JACKSON [*]

This chapter explores recent Fintech innovations through the lens of Ronald Coase's classic article: The Nature of the Firm. Applying a transaction cost analysis, the chapter argues that developments in computer technology, data processing, and information networks are reshaping the manner in which financial services are produced, unsettling the boundaries separating regulated firms from outside vendors and open market transactions. These changes raise challenging questions as to the appropriate contours of regulatory perimeters as well as the structure of regulation and supervision in the many areas of financial regulation. Fintech innovations also have the potential to be harnessed to serve public purposes, including expanding access to financial services and improving supervisory practices. At a minimum, Fintech innovations and most especially machine learning and artificial intelligence complicate the application of legal doctrines based on human intentionality. More broadly, the scale and scope of these technological developments may lead to a fundamental rethinking of the appropriate goals of regulatory policy for financial firms and the economy, particularly with respect to privacy and the accumulation of personal information in private and public hands.

Table of Contents

[*] James S. Reid, Jr., Professor of Law, Harvard University. This chapter draws on the work of and discussions with my students at Harvard Law School and is an elaboration of an earlier essay that appeared in a symposium issue of the *Washington University Journal on Law and Policy* on Regulating Emerging Financial Technologies. Howell E. Jackson, *The Nature of the FinTech Firm*, 61 Wash. U. J. Law & Pol'y 9 (2020). My thanks to Professor Dirk Andreas Zetzsche, Jai Massari, Todd Baker, and participants in a Harvard Law School Faculty Workshop on June 25, 2020, for helpful comments and suggestions.

Introduction

The title of this chapter is an homage to Ronald Coase's classic work, *The Nature of the Firm*, in which Professor Coase offered up a pithy, but profound, exposition of the question why some business activities are located within the discretionary control of corporate management, while others are exchanged through arm's length transactions in the marketplace.[1] As explicated decades later in the press release announcing the award of Professor Coase's Nobel Prize in the Economic Sciences, the Royal Swedish Academy of Sciences highlighted the article's focus on transaction costs for market transactions, as well as production costs for activities organized within the firm, as being of "critical importance":

> If these circumstances are taken into account, it may be concluded that a firm originates when allocative measures are carried out at lower total production, contract and administrative costs within the firm than by means of purchases and sales on the market. Similarly, a firm expands to the point where an additional allocative measure costs more internally than it would through a contract on markets. If transaction costs were zero, no firms would arise. All allocation would take place through simple contracts between individuals.[2]

For years, Professor Coase's article has inspired theorists of organizational design and earned a place in the pantheon of corporate law scholarship. In this chapter, I return to *The Nature of the Firm* to explore the Fintech revolution and the challenges that aspects of this revolution have posed for regulatory authorities. Several of the examples I discuss concern the distinction between activities located within a firm and those arranged through market transactions often supplied through new and specialized Fintech entities. Later, I focus on the expanded production possibilities that Fintech innovations facilitate, especially in regards to big data, personal and otherwise. This aspect of Fintech raises hard questions for regulatory policy with respect to privacy, institutional design, and cross-border jurisdiction. The expanded use of machine learning and artificial intelligence in business practices also complicates our understanding of what it means to exercise managerial discretion and may require adjustments to several bodies of legal doctrine, including fair lending and market manipulation. While much of this chapter focuses on the question of how existing legal structures should apply to Fintech innovations, lingering in the background throughout, and addressed briefly in the conclusion, is the possibility that the changes wrought by Fintech innovations are so profound that it is our regulatory structure itself that must now be reimagined and reformed.

[1] Ronald H. Coase, *The Nature of the Firm*, 4 Economica 386, 392 (1937). I am hardly the first to make a connection between Professor Coase's classic article and the impact of technological developments on optimal models of productions. *See, e.g.*, Yochai Benkler, *Coase's Penguin, or, Linux and The Nature of the Firm*, 112 Yale L.J. 369 (2002) (exploring the potential for peer production in a technologically advanced economy). *See also* Yueh-Ping Yang & Cheng-Yun Tsang, *RegTech and the New Era of Financial Regulators: Envisaging More Public-Private-Partnership Models of Financial Regulators*, 21 U. Pa. J. Bus. L. 354 (2018) (applying transaction cost analysis to Fintech developments). In a related vein, Luca Enriques & Dirk Zetzsche, *Corporate Technologies and the Tech Nirvana* (July 2019) (available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3392321) has recently engaged in a similarly spirited exercise exploring (with some skepticism) the capacity of artificial intelligence and other Fintech innovations to revolutionize corporate governance.

[2] Press Release, Royal Swedish Academy of Sciences (Oct. 15, 1991) (available at https://www.nobelprize.org/prizes/economic-sciences/1991/press-release/).

Finance and Fintech

While other scholars have offered a number of plausible definitions of Fintech,[3] my own preference is to define the phenomenon as encompassing a wide range of private and regulatory innovations that have become possible through the rapid decline in the cost of computing, accompanied by the widespread availability of reliable, high-speed connectivity (typically over the internet), and an explosion of newly collected data about a broad swath of personal and commercial characteristics and behaviors. This technological transformation has potentially huge implications for the domain of finance, which, to paraphrase Professors Merton and Bodie, can be helpfully demarked as "the movement of value across time and space under conditions of uncertainty that are not fully knowable by other private parties or government agents."[4] The critical concept here is "conditions of uncertainty," which includes, among other things, the uncertainty whether a borrower will repay their loan, the uncertainty whether an insured risk (like an earthquake) will come to pass, the uncertainty whether providers of liquidity (like repurchase counterparties or market-makers for bonds) will withdraw unexpectedly from their markets, or the uncertainty whether interest rates will rise or fall as expected. On many dimensions, Fintech allows for these and other uncertainties (i.e., risks) to be managed in new, more efficient, and more expeditious ways. Moreover, as I explain below, Fintech innovations allow for the management and oversight of many risks and associated operations to be contracted out of regulated entities and into new Fintech firms or market transactions. Sometimes, Fintech innovations create the possibility of entirely new kinds of market transactions, as is the case with the introduction of new networks such as payment platforms or clearing systems.[5] That is, the rise of Fintech increases the set of viable arrangements for producing financial services, potentially relocating significant amounts of activities that were previously based within the regulated firm and subject to management discretion in a well-supervised environment.[6] Similarly, technological developments also have the potential to improve the ability of government agents to monitor financial activity and identify more rapidly emerging risks.

A secular erosion of regulated financial firms' franchise substantially predates the rise of the internet or the introduction of distributed ledgers and actually was well underway when Steve Jobs was

[3] *See, e.g.*, Chris Brummer & Yesha Yadav, *Fintech and the Innovation Trilemma*, 108 GEO. L.J. 235, 241 (2019) ("the use of digital technologies in finance"); William Magnuson, *Regulating Fintech*, 71 VAND. L. REV. 1167, 1174 (2018) ("the new breed of companies that specialize in providing financial services through technologically enabled mobile and online platforms"); Rory Van Loo, *Making Innovation More Competitive: The Case of Fintech*, 65 UCLA L. REV. 232, 239 (2018) ("Fintech is used here to refer to the relatively new category of companies whose business models are based on digital products[, but] leaves out legacy banks…which may now offer similar products but whose services originally lacked a digital component."). In its recent report on Fintech and related developments, the U.S. Treasury Department did not offer a precise definition, but organized its discussion of Fintech in a manner analogous to my own, embracing both innovations within traditional financial firms and the emergence of new technology based firms. *See* U.S. DEP'T OF TREASURY, A FINANCIAL SYSTEM THAT CREATES ECONOMIC OPPORTUNITY: NONBANK FINANCIALS, FINTECH, AND INNOVATION 5 (2018). Professor Dirk Zetsche and his many co-authors have refined the concept of Fintech to distinguish "regtech," the emergence of regulatory technologies, and "techfin," the entrance of primarily technology companies (like Google or Apple) into the world of finance. *See, e.g.*, Dirk A. Zetzche, Douglas W. Arner, Ross P. Buckley & Rolf H. Weber, *The Future of Data-Driven Finance and Regtech: Lesssons from EU Big Bang II* (Eur. Banking Inst. Working Paper Series No. 35, 2019) (available at https://ssrn.com/abstract=3359399); Dirk A. Zetzche, Ross P. Buckley, Douglas W. Arner & János N. Barberis, *From FinTech to TechFin: The Regulatory Challenges of Data-Driven Finance,* 14 N.Y.U. J.L. & BUS. 393 (2018). *See also* Douglas W. Arner, János Barberis & Ross P. Buckley, *The Evolution of FinTech: A New Post-Crisis Paradigm*, 47 GEO. J. INT'L L. 1271, 1272 (2015-2016) (defining Fintech as "the use of technology to deliver financial solutions").

[4] Zvi Bodie & Robert C. Merton, Finance 2 (2000).

[5] *See* Enriques & Zetzsche*, supra* note 1, at 11-13.

[6] In "The Nature of the Firm," Professor Coase identified technological developments—then, telephones and telegraphs—as having the potential for changing the scope of efficient firm size, though he interpreted these changes as creating the potential for larger firms rather than the shrinking of incumbent firms contemplated in the text. *See* Coase, *supra* note 1, at 397.

still working out of his garage.[7] At least as early as the 1970s, the expansion of commercial paper was an early example of disintermediation: short-term funding for high-quality corporate issuers moved from intermediated bank loans into disintermediated commercial paper issuances. The process accelerated in the 1990s with the explosion of securitization practices whereby many other commercial and consumer loans found funding through capital market transactions, and banks and thrifts adopted new originate-to-distribute business models. The emergence of marketplace lending in the new millennium—and the first illustration in this chronology that might properly be labeled "Fintech"—allowed yet more kinds of consumer borrowing to be disintermediated, and in some cases crowdsourced with retail funding, but more commonly now through funding from institutional investors. Moving away from credit markets, one can also observe over the past several decades how swaps and other derivatives moved interest rate risk, foreign exchange risk, credit risk, and even weather risk into the capital markets and off the balance sheets of regulated entities. Innovations in information processing, including the development of options-pricing models and technological developments such as the Bloomberg terminal, as well as the work of the now often maligned—but still historically important—rating agencies, made these advances in finance possible. Now, Fintech is starting to produce similar effects, only more, better, faster, and more economical.

At the same time, some aspects of Fintech—especially those that reward economies of scale and pre-existing network effects—can serve to entrench incumbent firms. Financial institutions have long accumulated information about existing customers and advances in digital technologies, if exploited aggressively and creatively, can serve to shore up legacy firms and increase market share. In many contexts, a battle is currently underway between, on the one hand, nimble insurgents exploiting digital technologies to create new market niches and, on the other hand, major financial institutions scrambling to upgrade operations through a combination of investments, new hires, and opportunistic acquisitions. In some cases, the insurgencies come from tech firms discovering that their core digital competencies are well suited to expansion into financial services markets. While the lines of expansion differ, what is common to all of these contexts is that technological innovations are transforming the ways in which financial services can be delivered.[8] Some analysts interpret these developments as weakening the capacity of legacy firms to extract rents at the expense of their customers,[9] while others worry that, without careful government oversight, Fintech innovation could, instead, lead to a more dangerously concentrated market, dominated either by Wall Street giants or West Coast technology firms or some unholy bicoastal alliance of the two.[10] Still, others envision Fintech innovations as a pathway for community banks and mid-size financial services firms to recapture the market through strategic alliance with Fintech vendors to gain technological services that are impossible to produce economically on a limited scale.[11] So, while the endpoint of these developments in terms of eventual market structure is very much in doubt, there is a consensus that changes in the means of production that Fintech innovations represent is poised to alter the face of the financial services industry.

[7] The history of the developments discussed in this paragraph are reviewed in MICHAEL S. BARR, HOWELL E. JACKSON & MARGARET E. TAHYAR, FINANCIAL REGULATION: LAW AND POLICY 207-13, 372-74, 457-61 & 1237-68 (2nd ed. 2018) (Foundation Press) (hereinafter BARR, JACKSON & TAHYAR).

[8] For an insightful exploration of these issues, *see* Loo, *supra* note 3.

[9] Jeremy Kidd, *Fintech: Antidote to Rent-Seeking?,* 93 CHI.-KENT L. REV. 165 (2018).

[10] Loo, *supra* note 3.

[11] *See, e.g.,* Independent Community Bankers Association and Hunton & Williams, Fintech Strategy Roadmap for Community Banks (Mar. 2018).

Entities Versus Activities and the Challenge of Fintech

A classic—and in many areas still dominant—approach to financial regulation is based on the regulation of entities. If a firm engages in some core financial function—like banking, insurance, or the securities business—then the firm itself (often along with all affiliated entities) is subject to strict regulation, such as activities restrictions and capital requirements, as well as supervisory oversights, typically reporting, examination, and an enforcement regime. Once subject to entity-based regulation, a financial firm also enjoys certain benefits not available to other firms. For example, certain aspects of the U.S. payments system are available only to insured depository institutions. Similarly, insured depositories are the only entities that are permitted to "export" interest rates from their home jurisdictions, thereby preempting local usury laws and other state-based consumer protections in other jurisdictions.

Faced with a burdensome and costly system of entity-based regulation, the Fintech firm has every incentive to organize its behaviors to stay outside the relevant regulatory perimeters and simply contract for the provision of critical functions, like access to payment systems, through market transactions with already-regulated entities. So, for example, when Apple wanted to launch Apple Pay, it simply entered into contracts with existing banks and credit card providers to use their payment access and monetized its payments interface through a share of interchange fees.[12] Similarly, when marketplace lenders wanted the advantages of relaxed usury rules and uniform consumer protection statutes, they negotiated with existing banks located in business-friendly jurisdictions through a process known as "rent-a-charter," whereby the contracting bank formally originates all loans and then transfers them to the marketplace lenders for permanent funding and servicing.[13] Or, to put it in Coasean terms, as the domain of market-based transactions increased with technological developments, fewer activities had to be located within the discretionary (and costly) management of the regulated firm itself.[14] One of the reasons for the low enthusiasm surrounding the Office of the Comptroller of the Currency's (OCC) much publicized efforts to develop a new Fintech charter that would attract Fintech firms into the regulated space—aside from legal challenges from entrenched interests[15]—has been the simple fact that Fintech firms have many paths to gaining access to regulatory benefits without the burdens of direct regulation and supervisory control.[16] Some analysts have taken to calling these firms "synthetic" banks.[17]

[12] *See* Brummer & Yadav, *supra* note 3, at 277 & n.189.

[13] *See* Noah Buhayar, *Where Peer-to-Peer Loans Are Born*, BLOOMBERG BUSINESSWEEK (Apr. 16, 2015), https://www.bloomberg.com/news/articles/2015-04-16/webbank-where-peer-to-peer-loans-are-born [https://perma.cc/49LQ-P8G4].

[14] In his essay, Professor Coase identified government polices as having the potential to influence the location of economic activity. His example concerned sales taxes, which applied primarily to market transactions and thus encouraged the location of activities to within the firm. See Coase, *supra* note 1, at 393. With respect to the examples discussed in the main text, government requirements imposed on regulated firms—or example capital requirements or activities restrictions—operate as a tax on those firms, thereby encouraging the movement of activities to market transactions with unregulated firms.

[15] Rachel Witkowski, *Google and PayPal Explored OCC's Fintech Charter, Then Walked Away*, AM. BANKER (July 19, 2019), https://www.americanbanker.com/news/google-and-paypal-explored-occs-Fintech-charter-then-walked-away [https://perma.cc/LZA9-2R9H]. *See also* Vullo v. Office of the Comptroller of the Currency, 378 F. Supp. 3d 271, 292 (S.D.N.Y. May 2, 2019) (finding that New York state banking regulator had standing to challenge the Fintech charter, and that it appeared to at least partially exceed OCC's authority), *final judgment entered sub nom.* Lacewell v. Office of the Comptroller of the Currency, No. 18-cv-8377 (S.D.N.Y. Oct. 21, 2019) (permanently enjoining OCC from regulating any "Fintech applicant[]...that do[es] not accept deposits").

[16] Lea Nonniger, *Tech and Fintech Firms Aren't Interested in the OCC's Fintech Charter*, BUSINESS INSIDER (June 18, 2019), https://www.businessinsider.com/google-paypal-not-interested-in-occ-Fintech-charter-2019-6 [https://perma.cc/Z8WJ-NERJ].

[17] See, e.g., Todd H. Baker, Charter or not, Fintechs are Already 'Banking," AM. BANKER (Nov. 22, 2019).

While new Fintech entrants have incentives to tap into the regulated sector for the bare minimum of activities, regulated entities also have incentives to "push out" new Fintech services into unaffiliated firms operating beyond the regulatory perimeter. Such push-out strategies allow for innovations outside the constraints of supervisory controls while providing a potentially cost-effective mechanism for diversifying revenue streams and customer services of regulated entities. Prominent examples would include efforts of established firms to provide customer access to crypto-currencies, but without assuming full responsibility for custody and other customer protections typically required of broker-dealers.[18] The role of several major financial firms in supporting Facebook's Libra initiative for a new stable-value cryptocurrency (a stablecoin), but locating it in a new legally distinct non-U.S. entity, offers another still unfolding illustration of a push-out strategy to accommodate Fintech innovations beyond traditional regulatory perimeters, posing questions (among other things) with respect of the enterprise's ability to ensure compliance with anti-money laundering requirements.[19]

Mounting an Effective Defense to Regulatory Perimeters

Drawing an effective line between activities that must be brought within the regulatory perimeter for entity regulation and those activities that can remain outside of direct supervisory oversight is a fraught task.[20] Too bright a line invites evasion through complicated contracting terms with licensing and profit-sharing arrangements that are difficult to interpret and police. Too loose a definition (if backed by the threat of credible enforcement) will discourage innovation and add to compliance burdens. Oftentimes, innovations will occur and contractual arrangements will be put in place before regulatory officials have even focused on the issue, leaving regulators in the unenviable position of having to retrieve the horses once they are out of the barn and already lent out for hire.[21]

To be sure, Fintech firms have not always been able to escape the scrutiny and oversight of financial regulation. Many Fintech innovators in the payments space have evaded direct regulation as banks, but must still comply with state money transmitter requirements. The U.S. operations of PayPal offer one example of this approach.[22] Marketplace lenders that do not rely on the rent-a-charter tactic will also generally be subject to state consumer lending laws.[23] In some instances, regulatory authorities may attempt to gain control over Fintech firm activities as a result of their contractual relationships with

[18] For an overview of these issues including a reference to "non-custodial models," see Div. of Trading & Mts., Sec. & Exch. Comm'n & Office of Gen Counsel, Fin. Indus. Regulatory Auth., *Joint Staff Statement on Broker-Dealer Custody of Digital Asset Securities* (July 8, 2019), SEC. & EXCH. COMM'N, https://www.sec.gov/news/public-statement/joint-staff-statement-broker-dealer-custody-digital-asset-securities [https://perma.cc/4Q3J-6BHT]. For a more general treatment of the subject, see Timothy G. Massad, *It's Time to Strengthen the Regulation of Crypto-Assets*, BROOKINGS (Mar. 2019), https://www.brookings.edu/research/its-time-to-strengthen-the-regulation-of-crypto-assets/ [https://perma.cc/H4Y5-766G].

[19] *See* Timothy Massad, *Is Facebook Libra a Betrayal of Satoshi Nakamoto's Vision?*, FORTUNE (July 15, 2019), https://fortune.com/2019/07/15/facebook-libra-coin-cryptocurrency-hearing/ [https://perma.cc/FM95-6ER7]. *See also*, Dirk A. Zetzsche, Ross P. Buckley & Douglas W. Arner, Regulating Libra (July 2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3414401.

[20] For an insightful discussion of the perils of entities-based regulation for policing systemic risk, *see* Jeremy C. Kress, Patricia A. McCoy & Daniel Schwarcz, *Regulating Entities and Activities: Complementary Approaches to Nonbank Systemic Risk*, 92 S. CAL. L. REV. 1455 (2019).

[21] For an insightful characterization of these problems as an irreconcilable trilemma, *see* Brummer & Yadav, *supra* note 3.

[22] *See* Van Loo, *supra* note 3, at 239.

[23] For an overview of the overlapping system of federal and state oversight of marketplace lending, see DAVID W. PERKINS, CONG. RESEARCH SERV., R44614, MARKETPLACE LENDING: FINTECH IN CONSUMER AND SMALL-BUSINESS LENDING 12-22 (2018), https://fas.org/sgp/crs/misc/R44614.pdf [perma.cc/AJC8-6YFS].

regulated firms.[24] As the regulated entities must be attentive to supervisory concerns, there are a variety of ways in which public officials can leverage that influence into indirect control over Fintech entrepreneurs.[25] For example, recent efforts to define the ways in which regulated securities firms can maintain custody arrangements for cryptocurrencies can be seen as an effort on the part of government actors to establish some degree of supervisory oversight of cryptocurrencies beyond their direct control.[26]

In addition, if the manipulation of regulatory perimeters becomes too blatant, the legal system has ways of counteracting innovations that appear egregious. Several courts, for example, have disregarded interest-rate terms set through rent-a-charter arrangements when the practices seemed especially abusive.[27] Similarly, the Federal Reserve Board has been reluctant to admit into the payment system a new bank charter whose entire business plan was based on giving unregulated third parties the functional equivalent of access to interest bearing accounts at Federal Reserve Banks.[28] So, there are limits on the extent to which Fintech firms can contract into key financial functions. But, with a very large number of existing banks and other kinds of financial firms available to provide a port of entry, there are ample opportunities for Fintech firms with a new way of managing uncertainty or accessing customers to find a regulated entity willing to partner up for a modest fee.[29]

Sometimes, regulators have a hard time even realizing that a regulatory perimeter has been breached. Here, the rise of robo-advisers offers an object lesson.[30] Robo-advisers are typically organized as broker-dealers and investment advisers under the supervision of the Securities and Exchange Commission (SEC), Financial Industry Regulator Authority (FINRA), and, in certain respects, state securities officials. Robo-advisers use investment algorithms to invest client assets in regulated mutual funds, including exchange-traded funds (ETFs), based on a limited number of characteristics, such as risk-return preference, investment period, and tax status. Robo-advisers are subject to regulation, but a relatively lax form that consists primarily of open-ended fiduciary duties and soft disclosure standards. The product that robo-advisers offer, however, is functionally quite similar to "fund-of-funds" mutual funds, which are subject to much more stringent regulatory requirements, including independent board oversight, well-defined disclosure rules about performance and fees, plus stringent portfolio restrictions. Robo-advisers

[24] For example, the Bank Service Corporation Act has been interpreted to provide federal agencies the authority to obtain information with respect to, and in some instances actually examine, Fintech firms providing important services to regulated entities. *See* Fed. Deposit Ins. Corp., FIL-19-2019, Financial Institution Letter on Technology Service Provider Contracts (Apr. 2, 2019), https://www.fdic.gov/news/news/financial/2019/fil19019.pdf [perma.cc/NWD9-K6BR].

[25] *See* BARR, JACKSON & TAHYAR, *supra* note 7, at 216-21 (exploring other instances in which regulatory officials used supervisory authority to constrain the activities of regulated firms).

[26] *See supra* sources cited note 18. See also Letter of Dalia Blass, Director, SEC Division of Investment Management (Jan. 18, 2018), https://www.sec.gov/divisions/investment/noaction/2018/cryptocurrency-011818.htm. (exploring custody and other regulatory aspects of cryptocurrency holdings in investment funds).

[27] For a critical overview of the principal legal cases setting aside efforts of lenders to contract out of usury limits, *see* Davis Polk White Paper: Federal Banking Regulators Can and Should Resolve Madden and True Lender Developments (Aug. 14, 2018), https://www.davispolk.com/files/madden-true-lender-federal-regulatory-fix-whitepaper_final.pdf. The OCC and FDIC have since finalized rules that seek to pre-empt the ability of courts to make such decisions. See FDIC Press Release on Rule to Codify Permissible Interests on Transferred Loans (June 25, 2020); OCC News Release on Rule to Clarify Permissible Interest on Transferred Loans (May 29, 2020).

[28] *See* Carolyn Duren & Rucha Khole, *'Narrow Bank' Challenges Traditional Industry Model, But Fed Pushes Back*, S&P GLOBAL MKT. INTELLIGENCE (Mar. 27, 2019), https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/49204495 [https://perma.cc/JYQ6-K2EN].

[29] *Cf.* Kidd, *supra* note 9 (envisioning the rise of Fintech firms as having the potential for reducing rent-seeking in the financial service industry).

[30] The points made in this paragraph are elaborated upon in Howell E. Jackson, *Limits of Fiduciary Protections for Investors in Mutual Funds and Other Collective Investment Vehicles*, *in* FIDUCIARY OBLIGATIONS IN BUSINESS (Arthur Laby & Jacob H. Russell, eds., Cambridge Univ. Press, forthcoming 2020).

replicate mutual fund activities through a combination of algorithmic models and client agreements. While they contract into the mutual fund industry for their underlying investments, their outer wrappers (and associated fee arrangements and disclosure requirements) are substantially different than those imposed on functionally similar fund-of-fund mutual funds. To date, robo-advisors arguably constitute a successful illustration of regulatory arbitrage.

Systemic Risk and Fintech Innovations

Another area of uncertainty with respect to Fintech innovations are the implications for financial stability and systemic risks, that is, the possibility that an exogenous shock to one part of the financial system could lead to serious disruptions to the broader economy.[31] Like many things related to Fintech, this possibility is contested. On the one hand, to the extent that Fintech innovations lead to greater competition in the financial services industry, one might imagine that the introduction of new technologies will reduce the significance of dominant market actors and thereby ameliorate too-big-to-fail concerns. Of course, this perception proceeds under the assumption that Fintech innovation will reduce the dominance of major players, a prediction which, as discussed above, itself remains contested. But, even if technological innovations do not increase traditional measures of concentration, it is possible that these new technologies could create concerns for financial stability.[32]

For example, to the extent that marketplace lending supersedes intermediated finance as a source of funding for small and medium-size enterprises in the United States, there are questions as to how this funding mechanism will operate in periods of financial instability. Without direct ties to central-bank support and lender of last resort facilities, marketplace lenders may be more vulnerable to funding interruptions in times of financial stress, a weakness that could become manifested in the course of the pandemic of 2020. In addition, there are other pathways whereby Fintech innovations could accelerate the transmission of exogenous shocks to the broader economy. For example, if algorithmic trading programs lead capital market participants to pursue trading strategies based on common models, then trading responses to unexpected information could enhance volatility beyond what would have been experienced with more traditional trading practices based on human decision-making. Computer software, that is, may be even more susceptible to herd behavior than human beings. It is also possible that the new information networks and mechanisms of interconnectivity can themselves become sources of systemic risks of the sort experienced in the unregulated OTC derivatives markets of 2008. Perhaps the greatest potential source of systemic risk is the development of new payment systems, either expanding upon public models supported by the Federal Reserve and other central banks or created by private entities such as the Libra Foundation. In addition to problems inherent in the creation of any new complex system, these mechanisms for the safe and easily accessible storage of value pose the possibility of new forms of runs out of the commercial banking sector in times of financial stress.

[31] Howell E. Jackson, *Introduction: Thinking Hard about Systemic Risk*, *in* SYSTEMIC RISK IN THE FINANCIAL SECTOR: TEN YEARS AFTER THE GLOBAL FINANCIAL CRISIS 1, 8 (Douglas Arner, Emilios Avgouleas, Danny Busch & Steven L. Schwarcz, eds., Centre for International Governance Innovation, 2019). *See also* BARR, JACKSON, & MARGARET E. TAHYAR, *supra* note 7, at 738-46.

[32] For one view of these concerns, *see* William Magnuson, *Regulating Fintech*, 71 VAND. L. REV. 1167 (2018) (exploring systemic risks from a decentralized Fintech market). *See also* Douglas W. Arner, Ross P. Buckley, and Dirk Zetsche, *Fintech, Regtech and Systemic Risk: The Rise of Global Technology Risk*, in SYSTEMIC RISK IN THE FINANCIAL SECTOR, *supra* note 31, at 69.

Anticipating actual sources of systemic risk as opposed to purely theoretical ones, is extraordinarily difficult, especially in early stages of innovation. But as our experience from the authorization of money market mutual funds many decades ago demonstrates, what originally appears as an incrementally and procompetitive innovation can grow over time into a major market segment built on profoundly unstable foundations.[33] Whether today's Fintech innovations have similar potentials for market instability in the future, remains to be seen.

Exploiting the Potential of Fintech for Public Purposes

While it is easy—and perhaps natural for a law professor—to focus on the extent to which Fintech innovations pose challenges to regulatory regimes, Fintech and its ability to reduce transaction costs and expand the range of contractual options also can offer possibilities to promote the public interest. I offer here a brief account of two examples: one ongoing and one hypothetical.[34] I then comment briefly on the possibility that Fintech innovations could be incorporated into the regulatory and supervisory process itself.

Emergency Savings in the Workplace

One of the greatest sources of financial vulnerability for low- and moderate-income individuals is the absence of emergency savings. To invoke an oft-quoted statistic, some nearly forty percent of Americans do not have immediate access to four hundred dollars of funds in the event of an emergency need.[35] Much regulatory effort has gone into policing abusive short-term lending practices, like some payday lending programs, to address a consequence of the absence of meaningful emergency savings, but another more direct solution would be to increase emergency savings balances. A good place to start such an effort is with major employers with large numbers of low- and moderate-income employees.[36] For the most part, these employers are not financial institutions and, while they may offer various kinds of fringe benefits (like health care and retirement savings plans), emergency savings is not yet typically on the menu of most employee benefit plans. There are, however, a number of Fintech firms that provide a range of linkages between employer payrolls and regulated emergency savings vehicles. One could easily imagine a combination of nonprofit leadership with limited government support to promote Fintech linkages and employer nudges to steer workers into emergency savings programs. Here, Fintech firms might exploit technological innovations to accumulate funds in a manner that has proven unprofitable and therefore unattractive to regulated firms operating on their own.

[33] *See* BARR, JACKSON & TAHYAR, *supra* note 7, ch. 12.3.

[34] For additional discussions in a similar vein, *see* Ross P. Buckley, Douglas W. Arner, & Dirk A. Zetzsche, Sustainability, FinTech and Financial Inclusion (EBI Working Paper Series, no. 41, 2019).

[35] *See* BD. OF GOVERNORS OF THE FED. RESERVE SYS., REPORT ON THE ECONOMIC WELL-BEING OF U.S. HOUSEHOLDS IN 2018 21-22 (May 2019), https://www.federalreserve.gov/publications/files/2018-report-economic-well-being-us-households-201905.pdf, [https://perma.cc/829Y-LFPU].

[36] The concepts presented in this paragraph are illustrated by a recent initiative, funded by BlackRock, to promote emergency savings. *See* BLACKROCK'S EMERGENCY SAVINGS INITIATIVE, https://savingsproject.org/ [https://perma.cc/R2PZ-A96K].

Safe, Low-Cost Accounts for the Unbanked

Finding safe and cost-effective savings vehicles for other unbanked individuals poses a related problem that may also allow a Fintech solution. Many kinds of depository institutions operating in the United States today have historical roots in efforts to promote savings among working Americans: savings banks, thrifts, and credit unions all share these common roots. And recent efforts to revive a U.S. Postal Bank also are rooted, at least in part, on the view that such a bank would provide increased access to savings for the presently unbanked.[37] But all of these approaches are entity-centric and focus on the creation of a well-motived legal entity to issue deposits to underserved communities and reinvest those assets through the entity's own balance sheet.

However, it is entirely possible to create safe savings without the balance sheet of a new legal entity.[38] The U.S. Treasury issues trillions of dollars of safe assets each year. Even putting aside the large volumes held on the Federal Reserve's balance sheet, there are ample Treasuries available for public purchase in a variety of maturities. There is even an internet portal—Treasury Direct—where the general public can purchase Treasuries directly, albeit with an interface that is currently quite clunky.[39] One could easily imagine, however, a refreshed Treasury Direct portal, supported through open-access APIs that would allow Fintech firms to market safe savings products to a range of consumers. The Treasury Department already has statutory authority to adjust the terms of Treasury securities to accommodate such a program. And, to appease industry resistance, the size of permissible balances could be set at a level to avoid competition with private firms, just as the Obama Administration did with its now terminated myRA program.[40] The product would solely be targeted at customers with account balances beneath commercially viable levels. Fintech entrepreneurs would provide all of the necessarily linkages, including (perhaps) offloading programs to private banks when Treasury accounts reach high enough balances.[41]

Incorporating Fintech into Regulatory and Supervisory Processes

Fintech innovation are not limited to private agents, and a number of academic commentators have speculated as to the possibility that regulatory agencies might themselves exploit new technologies

[37] *See* MEHRSA BARADARAN, HOW THE OTHER HALF BANKS: EXCLUSION, EXPLOITATION, AND THE THREAT TO DEMOCRACY 183-225 (Harvard Univ. Press 2015); *see also* Mehrsa Baradaran, *It's Time for Postal Banking*, 127 HARV. L. REV. F. 165 (2014); Mehrsa Baradaran*, How the Poor Got Cut out of Banking*, 62 EMORY L.J. 483 (2013).

[38] *See* Commonwealth, Increasing Access to U.S. Savings Bonds: Recommendations for Bond Innovations (Dec. 9, 2016). The legal issues summarized in this paragraph are presented more fully in a Memorandum from Kathleen Shelton, Harvard Law Sch. Class of 2018, to Howell Jackson (Mar. 16, 2017) (on file with author). The adaptation of the Treasury Direct Program in this manner is functionally similar to The Narrow Bank approach discussed above, *see supra* text accompanying note 28, albeit targeted at low and moderate income individuals in need of a safe saving vehicle rather than the wholesale institutional market.

[39] *See Guided Tour*, TREASURYDIRECT, https://www.treasurydirect.gov/indiv/TDTour/default.htm [https://perma.cc/K4W3-CRAD].

[40] *See* Richard Eisenberg, *R.I.P. myRA Retirement Account, Gone Too Soon*, Forbes (July 28, 2017), https://www.forbes.com/sites/nextavenue/2017/07/28/r-i-p-myra-retirement-account-gone-too-soon/#73c1db0a7885 [https://perma.cc/KB5G-DP6Y].

[41] For a recent paper fleshing out a proposal along very similar lines, see Robert C. Hockett, Digital Greenbacks: A Sequenced "Treasury Direct" and "FedWallet" Plan for the Democratic Digital Dollar (May 18, 2020), (avail. at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3599419).

to improve supervisory capabilities and refine regulatory standards.[42] Just as private firms utilize Fintech to reduce uncertainty with respect to market risks and borrower creditworthiness, regulatory officials might employ similar innovations to detect more efficiently potential problems in regulated firms and financial markets as well as to deploy more efficiently supervisory resources. A 2017 report from the Toronto Centre identified five potential areas for such "SupTech" applications:

- Real-time supervision, by looking at data as it is created in the regulated institutions' operational systems;
- Exceptions-based supervision, in which automated checks on institutions' data and other information automatically collected and analyzed by the supervisory agency identify "exceptions" or "outliers" to pre-determined parameters for expected behavior, triggering supervisory action; Automated implementation of supervisory measures, such as sending a (automatically created) direction for capital increases based on automated data analysis, and decision-making;
- Algorithmic regulation and supervision in areas such as high-frequency trading, algorithm-based credit scoring, robo-advisors or any service or product that automates decision-making;
- Dynamic, predictive supervision by using machine learning, which could move supervisors to take supervisory actions in a preemptive manner based on predictive behavioral analysis.[43]

While the challenges of developing and maintaining regulatory expertise in these areas are considerable and much work would need to be done to integrate automated supervision with the operating systems of financial firms (with non-trivial issues with respect to privacy and trade secrets needing to be worked through), Fintech innovations do offer the possibility of improved regulatory and supervisory processes for the future.

On Discretion & Intentionality

In *The Nature of the Firm*, Professor Coase identified managerial discretion as a critical strength of the firm and a principal justification for moving activities away from market transactions and into firm control. But, Fintech and, most especially, the emergence of artificial intelligence based on machine learning offer new ways of organizing activities within the firm but outside the control of managerial discretion, at least as the concept has traditionally been understood. This phenomenon has many important implications—among other things, for personal privacy and intellectual property[44]—but the one that I want to explore here concerns state-of-mind requirements in various legal regimes. In many contexts, legal liability turns on the state of mind of a legal actor, requiring in some cases a showing of

[42] *See, e.g.,* Douglas W. Arner, Jànos N. Barberis & Ross P. Buckley, *The Emergence of Regtech 2.0: From Know Your Customer to Know YourData*, 44 J. FIN. TRANSFORMATION 79 (2016); Yueh-Ping Yang & Cheng-Yun Tsang, *RegTech and the New Era of Financial Regulators: Envisaging More Public-Private-Partnership Models of Financial Regulators*, 21 U. PA. J. BUS. L. 354 (2018).

[43] See Toronto Centre Global Leadership in Financial Supervision. FinTech, RegTech and SupTech: What They Mean for Financial Supervision 12-13 (Aug. 2017). See also Dirk Broeders & Jermy Prenio, Innovative Technology in Financial Supervision (Suptech): The Experience of Early Users 1 (July 2018) (BIS Financial Stability Institute Insights on Policy Implementation No. 9) ("Suptech is currently found in two areas of applications: data collection and data analytics.").

[44] For an overview of the issues with an emphasis on financial stability, *see* Financial Stability Board, Artificial Intelligence and Machine Learning in Financial Services: Market Developments and Financial Stability Implications (2017). *See also* William Magnuson, *Artificial Financial Intelligence*, Harv. Bus. L. Rev. (forthcoming 2020) (available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3403712).

negligence and in others a finding of intentionality. Much of the first-year law school curriculum and a fair bit of jurisprudence explores the justifications for different state of mind requirements, but—put crudely—the law tends to impose intentionality requirements when the social desirability of some activity is ambiguous and doctrine has evolved to limit liability to those cases where the likelihood of social harm is greatest and the culpability of the defendant clearest. With artificial intelligence, however, firms now have the opportunity to move activities away from the kinds of discretionary management that can give rise to a finding of human intentionality and into the domain of machine learning, where the concept of intentionality becomes opaque if not evanescent.[45]

Market Manipulation and High-Frequency Trading

A good example of this phenomenon can be seen in the area of market manipulation and high-frequency trading (HFT). One potential concern with high-frequency trading is that its trading practices are often reminiscent of traditional forms of manipulation.[46] For example, HFT strategies often entail the posting of large numbers of trade orders, the vast majority of which are withdrawn before execution. This practice could be seen as analogous to fictitious trading proscribed under traditional market manipulation doctrine. Another example would be trading strategies in which HFT firms detect the presence of large "buy" orders—typically from institutional investors—and then seek to place orders ahead of the institutional buyer, pushing prices away from the large purchaser and allowing the HFT trader to earn quick profits by placing itself between the orders in the marketplace. In certain respects, this practice is analogous to front-running.[47]

A robust and insightful body of academic literature and policy papers have recently explored the question as to how traditional anti-manipulation rules should be applied to these new concepts. One component of this literature is an examination of how intentionality—traditionally a key element of manipulation cases—should be applied in these concepts where human intentionality is not directly at issue in the trading, but arguably something akin to intentionality might be found in the design of the code that supports the trade.[48] Of course, to the extent the HFT trading algorithms have their own elements of machine learning, it is quite easy to imagine the algorithms themselves developing trading practices wholly unanticipated by the humans that generated the underlying code in the first place.

[45] *But cf.* Enriques & Zetzsche, *supra* note 1 (emphasizing the challenges in delegating discretion to algorithms in the contest of corporate governance).

[46] For a good overview of the differences between old manipulation practices and new manipulation practices, see Tom C.W. Lin, *The New Market Manipulation*, 66 EMORY L.J. 1253, 1280-94 (2017).

[47] *See* Alan Chan, *Do High Frequency Traders Front-Run the Market by Using Their Speed Advantage?*, FORBES (Apr. 3, 2014, 1:41 P.M.), https://www.forbes.com/sites/quora/2014/04/03/do-high-frequency-traders-front-run-the-market-by-using-their-speed-advantage/#4c0442fb25a0 [https://perma.cc/548V-CD62].

[48] For an overview of sources on this topic, *see* Lin, *supra* note 46, at 1300-03. *See also Id.* at 1303-06 (advocating intermediary integrity obligations as an alternative approach); Merritt B. Fox & Kevin S. Haeberle, *Evaluating Stock-Trading Practices and Their Regulation*, 42 J. CORP. L. 887 (2017) (advocating that legal doctrine focus on the second market impact of trading practices). For a more general, but still quite helpful, proposal for the analysis of manipulation, *see* Merritt B. Fox, Lawrence R. Glosten & Gabriel V. Rauterberg, *Stock Market Manipulation and its Regulation*, 35 YALE J. ON REG. 67 (2018).

Artificial Intelligence and the Enforcement of Fair Lending Rules

Another example of this phenomenon occurs in the area of antidiscrimination law defining the boundaries of fair lending practices. Traditionally, the Equal Credit Opportunity Act (ECOA) and related antidiscrimination laws prohibit discrimination in lending through a doctrinal structure that includes a combination of disparate treatment and disparate impact analysis.[49] The doctrines that evolved in this area look to whether a lending firm intentionally discriminated on the basis of protected characteristics (such as race), or made use of factors that had a disparate impact on protected groups without there being a legitimate business justification for the lender's underwriting practices. Cases arising under these provisions often turn on the state of mind of the lender for both intentional use of race and business justifications for the use of other factors.[50]

Increasingly, lenders today and, most particularly, many Fintech lenders, rely on algorithms and machine learning to make credit decisions. In this context as well, the use of algorithms does not easily map on to traditional doctrinal test of intentionality and, as my colleague Talia Gillis has explored in several recent articles, advanced machine learning techniques seek to find variables correlated with creditworthiness and profitability, acting without the intervention of any human state of mind or discretionary authority to make pricing or credit allocation decisions.[51] One of the great debates of consumer financial regulation today is how to align these new lending practices with traditional fair lending doctrine.

To put these two examples into the Coasean framework, underwriting decisions and trading strategies were typically organized within the operations of a regulated firm because of the advantages of delegating to expert personnel the discretion to decide to whom to make loans or by which trading strategies to execute transactions. While lending algorithms and HFT strategies may formally remain within the regulated firm, the discretionary component and also the possibility of ascertaining human intentionality have disappeared. Traditional legal doctrines are incapable of providing relief unless regulatory officials devise new approaches to enforcement and detection. Efforts of these sorts are underway, but for the purposes of this chapter the need for such refinement of legal doctrines is further evidence that Fintech innovations are challenging the boundaries of regulated firm behavior.

Fintech and the Endogeneity of Regulatory Goals

A final question to consider, one that is implicit in much of the earlier discussion, is whether Fintech innovations themselves warrant change in the way we define our goals in the field of regulation or possibly in the structure of our supervisory system. In the Nature of the Firm, Professor Coase was not concerned with this question and accepted legal requirements as a fixed and exogenous constraint. But,

[49] *See* Equal Credit Opportunity Act, 15 U.S.C. §§ 1691-1691f (2018).

[50] *See, e.g.,* Anderson v. Wachovia Mortg. Corp., 621 F.3d 261, 269-79 (3d Cir. 2010) (performing detailed analysis of alleged intentional discrimination and business justifications); Golden v. City of Columbus, 404 F.3d 950, 963-65 (6th Cir. 2005) (affirming dismissal of ECOA disparate-impact claim regarding utility fees, in part relying on legitimate business justification that measuring unit-by-unit consumption was impracticable).

[51] *See* Talia Gillis, *False Dreams of Algorithmic Fairness: The Case of Credit Pricing* (Working Draft of Sept. 26, 2019) (available at https://scholar.harvard.edu/gillis/job-talk-paper); *see also* Talia B. Gillis & Jann L. Spiess, *Big Data and Discrimination*, 86 U. CHI. L. REV. 459 (2019).

for legal scholars and policy analysts this constraint is appropriately lifted, at least from time to time. This approach is nicely illustrated in Chris Brummer and Yesha Yadav's article *Fintech and the Innovation Trilemma,* in which they raise the possibility that Fintech developments might prompt us to recalibrate what they define as an enduring trilemma of regulatory design: tradeoffs among the provision of clear legal rules, the maintenance of market integrity, and the encouragement of financial innovation.[52] Whether or not one accepts this trilemma as embracing the full set of tradeoffs in our system of financial regulation, Professors Brummer and Yadav are undoubtedly correct that technological developments could necessitate a more profound rethinking of our regulatory structure than mere redefining of regulatory perimeters or adjustments in legal doctrine. And, the emergence of regulatory "sandboxes" to foster Fintech innovations is simply one manifestation of this intuition.[53]

This possibility is perhaps nowhere better illustrated than in the case of the regulation of big data and personal privacy more generally. The collection and manipulation of data is at the heart of many Fintech innovations and it has been the subject of considerable attention in recent academic literature.[54] One of the recurring questions that arise in this literature is the question of whether data utilized in the context of financial services should be treated as distinct from data regulation more generally. Historically, at least in the United States, financial services firms have been subject to specialized regulation of data, such as title V of the Gramm-Rudman-Hollings Act regarding personal financial information, the Fair Credit Reporting Act for information used to determine the credit-worthiness of borrowers, and a wide range of requirements governing impermissible uses of information in insurance and credit underwriting. Europe, in contrast, has adopted more general and far-reaching data protection rules, creating both substantial challenges for cross-border compliance as well as an alternative model for the supervision in this area of the law. The centrality of data in the modern economy has led some observers to argue that the United States should create an new uber-privacy authority to oversee data protection measures through the economy.[55] This would certainly be a plausible approach to the overarching problem of data protection and privacy, but also one that would create further fragmentation in our oversight of financial services and potentially limit the capacity of financial regulators to address core regulatory concerns within their jurisdiction, such as the promotion of financial stability or the preservation of competitive markets.

The larger point—and the point that readers should bear in mind as they work through the case studies that follow—is that Fintech innovations and the technological developments upon which they rest may necessitate a fundamental rethinking of the regulatory goals of financial authorities and the most appropriate institutional structures through which those goals should be achieved.

[52] Brummer & Yadav, *supra* note 3.

[53] Ross P. Buckley, Douglas W. Arner, Robin Veidt, and Dirk A. Zetzsche, *Building FinTech Ecosystems: Regulatory Sandboxes, Innovation Hubs, and Beyond*, 61 WASH. U. J. L. AND POL'Y 55 (2020). For a similarly motivated proposal to increase the use of internal compliance mechanisms to address problems associated with the use of artificial intelligence in credit underwriting, see Katja Langenbucher, *Responsible A.I.-Credit Scoring – A Legal Framework*, 31 EUROPEAN BUS. L. REV. 527 (2020).

[54] *See e.g.,* Dirk A. Zetzsche, Douglas W. Arner, Ross P. Buckley & Rolf H. Weber, The Future of Data-Driven Finance and RegTech: Lessons from EU Big Bang II (EBI Working Paper Series, no. 35, 2019). *See also* Douglas W. Arner, Jànos N. Barberis & Ross P. Buckley, *The Emergence of Regtech 2.0: From Know Your Customer to Know Your Data*, 44 J. FIN. TRANSFORMATION 79 (2016).

[55] Rory Van Loo, *Rise of the Digital Regulator*, 66 DUKE L. REV. 1267, 1267-1329 (2017).

PART I

MARKETPLACE LENDING & BEYOND

HARVARD LAW SCHOOL | The Case Studies

CSP028
MAY 2020

Lending Club: 2008

ANOOSHREE SINHA, CORRINE SNOW, AND HOWELL E. JACKSON

Memorandum

DATE: January 2008

TO: Partner, XYZ LLP

FROM: Associate ABC

RE: Lending Club

Lending Club is an online peer-to-peer lending (P2P lending) site. It is currently in the process of considering changes in its current business model and a question has arisen whether its funding of consumer loans may result in issuance of "securities" rather than "loans" and therefore be subject to registration requirements under Section 5 of the Securities Act of 1933 ("1933 Act").[1] Before moving ahead with any changes in its business model, Lending Club seek clarity regarding the application of federal securities laws to its operations. This memorandum outlines the legal framework to determine if a product is a security, and if so, who is the issuer of the security. It also discusses the risks associated with Lending Club's options.

Background

Lending Club's initial business model allowed qualified borrower members to obtain unsecured loans from its lender members. Lending members could indirectly fund specific loans to borrower members by purchasing promissory notes from Lending Club. Under the firm's first model, Lending Club was the lender of record. Borrowers executed promissory notes directly to Lending Club, and then Lending Club immediately assigned the rights to payment under these promissory notes to the lending members

[1] Securities Act of 1933, 15 U.S.C. § 77a et seq. (2008).

Written by Anooshree Sinha and Corrine Snow under the supervision of Howell E. Jackson, James S. Reid, Jr., Professor of Law of Harvard Law School. Case development at Harvard Law School is partially funded by a grant from Dechert LLP. Cases are developed solely as the basis for class discussion. They are not intended to serve as endorsements, sources of primary data, legal advice, or illustrations of effective or ineffective management.

Copyright © 2020 President and Fellows of Harvard University. No part of this publication may be reproduced, stored in a retrieval system, used in a spreadsheet, or transmitted in any form or by any means—electronic, mechanical, photocopying, recording, or otherwise—without permission. To order copies or permissions to reproduce materials please visit our website at casestudies.law.harvard.edu or contact us by phone at 617-496-1316, by mail at Harvard Law School Case Studies Program, 1545 Massachusetts Avenue – Areeda 507, Cambridge, MA 02138, or by email at HLSCaseStudies@law.harvard.edu.

indirectly funding the loan. As the lender of record, Lending Club was required to comply with lending guidelines, usury laws, and licensing requirements for each state in which it operated. Because complying with these varying rules was administratively cumbersome, costly, and economically infeasible, Lending Club established its current funding model with WebBank in December 2007.[2] Within the company, this funding model is sometimes referred to as Version 2.0.

WebBank is a state-chartered industrial bank organized under the law of Utah. Partnering with WebBank allowed Lending Club to provide uniform and advantageous interest rates across all states where Lending Club operates.[3] Under this current lending model, WebBank issues loans to borrower members and then endorses the promissory notes underlying those loans to Lending Club. Lending Club then assigns each note to a number of lender members. Lending Members are entitled to a pro rata share of the proceeds of the underlying promissory note from the borrower members. Borrowers enter into a loan agreement with WebBank. WebBank processes the loans, manages the money coming in from the lender members to fund the loans, and remits the monies to the corresponding borrower members. Funds from lending members go, in this way, to borrowing members.

Under both the initial and current lending models, Lending Club is responsible for screening borrowers, determining loan terms, computing interest rates, and servicing the loans.[4] Lender members choose in which loans they want to participate and pay a 1% service fee during the life of the loan for these services. Under both models, the notes held by lending members are essentially illiquid, because lender members must retain the notes until the principal and interest are repaid by the corresponding borrower member.

Looking into the future, Lending Club now wants to create a secondary market to provide greater liquidity for these notes. Under the proposed new business model that the firm is now exploring, lender members would not make loans directly to borrower members. Instead, Lending Club would hold the promissory notes from borrower members and then issue “Member Payment Dependent Notes” (MPD Notes). Lender members purchase MPD Notes issued by Lending Club, which would entitle the lender members to the proceeds of the specific promissory note backing the MPD Notes. These MPD Notes would be issued in series to lender members. Each series would correspond to a single loan. Lending Club expects these MPD Notes to be traded on a daily basis, thereby providing lending members liquidity. Lending Club would only be required to make payments to holders of the MPD Notes when it received payments on the corresponding loan. This new funding model is called “Version 3.0” among company executives. Aside from providing lending members a degree of liquidity, Version 3.0 is functionally identical to Version 2.0, as the MPD Notes are effectively non-recourse with respect to Lending Club and lending members thus bear all of the credit risks on the MPD Notes. Since their emergence several years

[2] Lending in certain states was essentially impossible because the states stipulated very low thresholds for interest rates. *See* Peter Tufano and Howell Jackson, LENDING CLUB CASE STUDY, Harvard Business School N9-210-052, 12 December 17, 2010, (avail at web.archive.org/web/20071015042928/www.usurylaw.com/state [perma.cc/5XPS-4VAY]).

[3] *See* Marquette National Bank v. First of Omaha Service Corporation, 493 U.S. 299 (1978) (allowing Nebraska bank to “export” higher interest rates to credit cardholders in Minnesota despite the host state’s usury laws). The “exportation doctrine” has been expanded through legal changes, administrative decisions and case law.

[4] Though Lending Club requires minimum credit scores for its borrower members, loans obtained via the Lending Club platform are more accessible than loans offered by financial institutions, which typical require better credit scores and more documentation and often additional forms of collateral.

ago, Prosper and other leading peer-to-peer entrepreneurs have not been subject to supervision under the federal securities laws.[5]

Before launching Version 3.0, Lending Club has requested an independent analysis of whether the Securities and Exchange Commission (SEC) might take a contrary position with respect to the firm's practices. Federal securities laws impose extensive disclosure requirements on the public issuance of securities, imposing substantial costs and potential liabilities on firms subject to SEC jurisdictions. So, in addition to considering whether Lending Club's funding models entail the creation of a security, we have also been asked to consider who the SEC would consider to be the issuer or perhaps co-issuer of any securities: Lending Club, WebBank, or possibly the individual borrowing members themselves.

Legal Background

Do Lending Club's Funding Models Create "Securities" for Purposes of the Federal Securities Laws?

The 1933 Act and the Securities Exchange Act of 1934 ("1934 Act")[6] have substantially similar definitions of a security. The 1933 Act defines a security as:

> any note, stock, treasury stock, security future, bond, debenture, evidence of indebtedness, certificate of interest or participation in any profit-sharing agreement, collateral-trust certificate, preorganization certificate or subscription, transferable share, investment contract, voting-trust certificate, certificate of deposit for a security, fractional undivided interest in oil, gas, or other mineral rights, any put, call, straddle, option, or privilege on any security, certificate of deposit, or group or index of securities (including any interest therein or based on the value thereof), or any put, call, straddle, option, or privilege entered into on a national securities exchange relating to foreign currency, or, in general, any interest or instrument commonly known as a "security", or any certificate of interest or participation in, temporary or interim certificate for, receipt for, guarantee of, or warrant or right to subscribe to or purchase, any of the foregoing.[7]

Traditional financial instruments like stocks and bonds are well established "securities" under federal law. The definition of a security evolves, however, with the introduction of each new financial product. The SEC may determine that Lending Club's promissory notes are either "investment contracts" or "notes" and therefore securities.

Might the Funding Models Constitute an Investment Contract?

In *S.E.C v. W. J. Howey Co.,* the Supreme Court held that an investment contract exists when there is "an investment of money in a common enterprise with profits to come solely from the efforts of

[5] For an overview of the industry, see Brad Slavin, Peer-to Peer Lending – An Industry Insight (June 21, 2007) (avail. at http://www.bradslavin.com/wp-content/uploads/2007/06/peer-to-peer-lending.pdf). Lending Club executives have heard rumors that a forthcoming student written law review note may take a different view of this issues. It is unclear, however, whether the authors of the piece are well informed as to the business models that peer-to-peer firms actually employ.

[6] Securities Exchange Act of 1934, 15 U.S.C. § 78a et seq. (2008).

[7] 15 U.S.C. § 77a(1) (2010).

others."[8] In *Howey*, the defendant offered units of a citrus grove development. The investors had no right of entry into, or management of, their specific units or to specific fruit. Instead, they were entitled to receive a share of the net proceeds of the grove on a pro rata basis.[9] The Court determined that the contracts and deed created an investment contract within the meaning of Section 2(1) of the 1933 Act.[10] The Court emphasized that economic reality should take precedence over form when assessing the nature of a contract.[11] In *Howey*, the primary purpose of the contracts was to determine each investors' share of the profits; the rights to the land were purely incidental. The "economic reality" of the arrangement was therefore akin to a profit seeking business where the investors brought in capital and shared in the profits, but did not manage, control, or operate the enterprise.[12]

Whether or not an instrument is an investment contract depends on both the nature of the instrument and the circumstances surrounding its sale. As a result, the exact same instrument may be a security in some circumstances, but not in others. For example, in *Marine Bank v. Weaver*, the Court held that a certificate of deposit (CD) was not a security because it was unique, would have different value to different investors, and was unsuitable for public trading.[13] In contrast, the CDs in *Gary Plastic Packaging Corp. v Merrill Lynch, Fenner & Smith Inc.,* were securities because of Merrill Lynch's repackaging actions.[14] As the Court explained in Marine Bank, "not all certificates of deposit invariably fall outside the definition of a 'security' as defined by the federal statutes. Each transaction must be analyzed and evaluated on the basis of the content of the instruments in question, the purposes intended to be served, and the factual setting as a whole."[15]

In *Marine Bank*, the Weavers pledged a CD in exchange for a share in Columbus Packing Company's net profits, the right to use Columbus' barn and pasture, and veto rights on future borrowings by Columbus.[16] The Court explained that the arrangement with the Weavers was a unique contract and a private transaction, whereas the transaction in *Howey* involved an offering to a large number of investors.[17] The Court defined a security as an instrument that is "commonly traded," has an equivalent values to most persons, and could be traded publicly.[18] The Court also emphasized that the Weaver's investment was already protected under existing laws, "[there are] important differences between a certificate of deposit purchased from a federally regulated bank and other long-term debt obligations... the purchaser of a certificate of deposit is virtually guaranteed payment in full, whereas the holder of an ordinary long term debt obligation assumes the risk of the borrower's insolvency."[19]

[8] 328 U.S. 293 (1946).

[9] *Id.* at 296–97.

[10] *Id.* at 300–01.

[11] *Id.*

[12] *Id.*

[13] 455 U.S. 551 (1982).

[14] 756 F.2d 230 (2nd Cir. 1985).

[15] *Weaver*, 455 U.S. at n. 11.

[16] *Id.* at 560.

[17] *Id.*

[18] *Id.*

[19] *Id.* at 558–59

In *Gary Plastic*, Merrill Lynch investigated a firm that marketed and created a secondary market for its CDs.[20] Unlike ordinary CDs, which are not freely redeemable prior to maturity and carry substantial penalty for early redemption, Merrill Lynch allowed investors a high degree of liquidity by giving them the option of selling the CDs back to Merrill Lynch if prevailing interest rates dropped. Merrill Lynch was therefore engaged in activities that were significantly greater than that of an ordinary broker or sales agent and investors expected profits derived solely from the efforts of Merrill Lynch.[21] Investment was motivated by the expectation of a return on cash investment, the potential for price appreciation due to interest rate fluctuations, and the liquidity of these highly negotiable instruments. The court therefore concluded that the CDs were securities.[22]

The instruments issued under Lending Club's current model may meet *Howey's* definition of an investment contract. Under the current model, lending members invest money through the purchase of a loan. The lenders bear the risk of loss because the loans are uncollateralized. Like the investors in *Howey*, lending members lack direct contact or control over borrower members.[23] As in *Howey*, the lending members hope to gain profit from the efforts of others.

Under the *Howey* test, Lending Club must be engaged in a "common enterprise." To determine whether or not a "common enterprise" exists, the court focuses on whether the promoter's activities (here, Lending Club) is the controlling factor in ensuring the success or failure of the investment.[24] These courts emphasize the "efforts" undertaken by the promoters.[25] Unlike Merrill Lynch in *Gary Plastics*, Lending Club merely provides intermediate services to facilitate borrowing between members. Lending Club's services are not instrumental in enabling the lender members to earn a profit, which is ultimately dependent on the borrower members repaying the underlying loans. The profits earned by lender members are not dependent on the entrepreneurial or managerial efforts of Lending Club. Instead, repayments come from the activities of the borrower members.

Other courts have determined that a common enterprise exists when promoters and investors share the risk of the investment.[26] Risk sharing occurs most commonly when investors rely on the expertise of intermediaries and those intermediaries earn commissions irrespective of the investor's gains or losses. Lending members, rather than Lending Club, bear almost all of the risk if the borrowing member defaults on their note. However, Lending Club charges a 1% servicing fee, but does not receive this fee if the borrower defaults on their payments. As a result, both Lending Club and the lending member bear some risk if a borrowing member defaults.

If Lending Club creates a secondary market for the MPD Notes, Lending Club's additional efforts will make their model look more analogous to the CDs issued in *Gary Plastics* than those in *Marine Bank.* Lending Club could still argue that the *Howey* test is too simplistic to apply to the notes in P2P lending because P2P lending is not designed solely to generate profits for lending members. Instead, P2P provides

[20] *See Gary Plastic*, 756 F.2d at 232–35.

[21] *Id.* at 240.

[22] *Id.*

[23] Ashta, Arvind and Assadi, Djamchid, *Do Social Cause and Social Technology Meet? Impact of Web 2.0 Technologies on Peer-to-Peer Lending Transactions* (October 9, 2008), (avail. at ssm.com/abstract=1281373 [http://perma.cc/YYN9-SMEZ]).

[24] *See* James D. Cox, Robert W. Hillman, and Donald C. Langevoort, SECURITIES REGULATION CASES AND MATERIALS, 38 (6th ed. 2008).

[25] SEC v. ETS Payphones Inc., 408 F.3d 727 (11th Cir. 2005).

[26] SEC v. Alliance Leasing Corp, 2000 US Dist LEXIS 5227 (S.D. Cal. Mar. 17, 2000).

optimal rates both to lenders and borrowers. Lending Club could also emphasize the active role lending members play in selecting which Notes to fund. Unlike the investors in *Howey*, who recovered profits on a pro rata basis, lending members receive profits from the individual loan that they specifically select. Still, the MPD Notes proposed under the new model closely resemble securities issued by Merrill Lynch.

Might the Funding Models Create a "Note"?

In *Reves v. Ernst & Young, Inc.*, a farmer's cooperative sold promissory notes to raise money for its general business operations.[27] The notes were uncollateralized, uninsured, and paid a variable rate of interest. The Court held that the notes were securities, and explained that there is a rebuttable presumption that a note is a security, unless it fits into a specific category of non-securities.[28] *Reves* specifically identified several types of non-securities, including (1) notes delivered in a consumer financing, (2) notes secured by a mortgage on a home, (3) short-term notes secured by a lien on a small business or its assets, (4) short-term notes evidenced by accounts receivable, (5) notes evidencing "character" loans to bank customers, (6) notes formalizing open account debts incurred in the ordinary course of business, and (7) notes evidencing loans from commercial banks for ordinary operations.[29] The Court held that a note is a security unless it falls into one of these categories, or bears a "strong family resemblance" to the notes in one of these categories.[30]

The Court then established a four-part "family resemblance" test for notes outside of the categories explicitly mentioned in *Reves*. In assessing these notes, courts should consider: (i) motivations of the buyer and seller—a note is more likely to be a security when the sellers' purpose is to raise money for the general use of the business, or to finance substantial investments, and the buyers' interest is in the profit of the business. Conversely, if the note's purpose is to "facilitate the purchase and sale of a minor asset or consumer good, to correct for the seller's cash-flow difficulties, or to advance some other commercial or consumer purpose... the note is less sensibly described as a 'security;'"[31] (ii) the plan of distribution to determine whether there is common trading for speculation or investment; (iii) the reasonable expectations of the investing public; and (iv) the existence of an alternate regulatory regime.[32] The Court held that the notes at issue in *Reves* were securities because the seller's motivation was to raise capital, the investors sought a profit from their investment, the notes were offered and sold to a broad segment of the public, and they were advertised as "investments," which created a general perception of a security. Finally, the uncollateralized and uninsured notes had no risk-reducing factors to suggest that they were not securities.[33] When applying the *Reves* test, courts also consider whether notes are offered to sophisticated buyers or members of the general public.

Lending Club's products do not fall into any of the enumerated categories of non-security notes and may fail the family resemblance test. To analyze the expectations of the lending members, courts

[27] 494 U.S. 56 (1990).

[28] *Id.* at 65.

[29] *Id.*

[30] *Id.* at 64–65.

[31] *Id.* at 66.

[32] *Id.* at 66–67.

[33] *Id.* at 67–69.

consider what a reasonable lender would believe about the character of the transaction. The manner in which a transaction is projected in advertisements or on the client's website can influence expectations. For instance, in *Reves,* the instrument was advertised as a "valuable return on an investment, which undoubtedly includes interest."[34] Lending members are motivated by the desire to obtain a better return on their money.

Lending members may therefore view their funding activities as an investment rather than a loan. Lending Club can argue that its own purpose is merely to facilitate a lending platform and that the money raised from lender members is used to finance general business purposes. Borrower members' motivations will vary from loan to loan. Lending Club could argue that many of the loans are "consumer finance" and therefore a non-security for "general business" purposes. Their model promissory note does stipulate that the loans are for personal finance rather than commercial purposes.[35] Lending Club's online marketing, however, does not limit itself to such a closed group. Instead, it reaches out to the general public. Lending Club's intention to create a secondary market available to the general public may further exacerbate this issue.

In *Banco Español de Credito v. Security Pacific National Bank*, the Second Circuit applied the *Reves* test and concluded that the notes were not securities. In *Banco Español*, Security Pacific extended a line of credit permitting Integrated Resources, Inc. to obtain short term unsecured loans.[36] Security Pacific then sold these loans to various institutional investors.[37] The court looked to the second factor in the *Reves* test and concluded that the plan of distribution was a limited solicitation to sophisticated financial or commercial institutions and not to the general public that specifically prohibited resales of the loans without the express written permission of Security Pacific. This limitation prevented the loan participations from being sold to the general public, thus limiting eligible buyers to sophisticated investors capable of acquiring information about the debtor.[38] In contrast, Lending Club offers its products over the internet to the public at large. The current model does not stipulate any special level of financial sophistication, expertise, or high income level akin to that of an accredited investor in order for a person to qualify as a lender member.[39] This wide dissemination and solicitation to the public may lead the SEC to conclude that the notes are securities.[40]

The third part of the *Reves* test assesses whether the reasonable public views the notes as an investment or a loan. The lender members seek higher returns on their investment in the notes. However, Lending Club promotes itself as a social lending network where members can borrow and lend money among themselves and Lending Club explains to lender members that our client does not itself guarantee the notes.

[34] *Id.* at n. 4.

[35] *See* Tufano, Jackson & Ryan, *surpa* note 1 at Exhibit 9.

[36] 973 F.2d 51 (2nd Cir 1992).

[37] *Id.* at 53.

[38] *Id.* at 55 (internal citations omitted).

[39] *See* the discussion under Regulation D of the '33 Act, *infra* Part III.

[40] *See* Reves, 494 U.S. at 68 (the notes "were...offered and sold to a broad segment of the public, and that is all we have held to be necessary to establish the requisite 'common trading' in an instrument.").

The absence of regulation, collateral, or insurance to protect against the risks associated with an instrument is an important factor in determining that an instrument is a security.[41] The SEC may determine that there are currently no appropriate regulatory safeguards for the lending members against misleading statements by a borrower member about their employment and income, identity, or against misleading statements by our client with respect to marketing or issuance of the notes.

Lending Club is already subject to substantial regulation. Applicable state laws regulate interest rates and charges, and require certain disclosures. In addition, state laws, public policy, and general principles of equity relating to the protection of consumers, unfair and deceptive practices, and debt collection practices apply to the origination, servicing and collection of the notes. The notes are also subject to federal laws, including the federal Truth-in-Lending Act and Regulation Z,[42] Equal Credit Opportunity Act and Regulation B,[43] Fair Credit Reporting Act,[44] Fair Debt Collection Practices Act, and similar state debt collection laws.[45] Failure to comply with the laws and regulatory requirements subjects our client to damages, lawsuits, administrative enforcement actions, and civil and criminal liability.

However, these laws aim to protect the borrower members but not the lender members in respect of the risks associated with the notes. WebBank is an FDIC-insured state-chartered industrial bank. State licensing statutes impose a variety of regulatory compliances such as (1) recordkeeping, (2) restrictions on loan origination and servicing practices, (3) disclosure, examination, and financial reporting requirements, (4) restrictions on advertising, and (5) review requirements for loan forms.[46]

Lending Club can also argue that the services it provides bear a closer semblance to the activities of banking institutions rather than those of an investment company. The current lending model is more akin to providing a lending platform and the promissory notes are more similar to loans rather than securities. This argument will be weakened under the proposed model, as a secondary market will make Lending Club appear more like an investment company.

Lending Club could also analogize its product to viatical agreements. In *SEC v. Life Partners Inc*, the viatical agreements were not securities.[47] A viatical settlement is an investment contract in which an investor acquires an interest in the life insurance policy of a terminally ill person. When the insured dies, the investor receives the benefit of the insurance. The investor's profit is the difference between the discounted purchase price paid to the insured and the death benefit collected from the insurer, less transaction costs, premiums paid, and other administrative expenses. Life Partners, Inc. (LPI), arranged these transactions and performed certain post-transaction administrative services. The court concluded that LPI's contracts were not securities because LPIs efforts did not have a predominant influence on investor profits. The court distinguished between pre-investment and post-investment services.[48]

[41] Bass v. Janney Montgomery Scott Inc., 210 F. 3d 577, 585 (6th Cir. 2000) (notes not securities in part because they were collateralized with assets and stock of borrower and its subsidiary).

[42] 15 U.S.C. § 1601 (2010); 12 C.F.R. § 226 (2010) (requiring certain disclosures to the Borrowers regarding the terms of the notes).

[43] 15 U.S.C. § 1691 (2010); 12 C.F.R. § 202 (2010) (prohibiting discrimination on the basis of age, race, color, sex, religion, marital status, national origin, receipt of public assistance or the exercise of any right under the Consumer Credit Protection Act, in the extension of credit).

[44] 15 U.S.C. § 1681 (regulating the use and reporting of information related to each Borrower's credit history).

[45] 15 U.S.C. § 1692 (regulating debt collection practices by "debt collectors" and prohibit debt collectors from engaging in certain practices in collecting, and attempting to collect, outstanding consumer loans).

[46] *See* 12 U.S.C. § 1813 (2010).

[47] 87 F.3d 536, 537–39 (D.C. Cir. 1996).

[48] 408 F.3d 737 (11th Cir 2005).

If Lending Club's Funding Models Create Securities, Who Is the Issuer?

Securities regulations place high disclosure requirements, costs, and liabilities on the issuer of a security. It is important to determine whether WebBank or borrower members will be treated as "co-issuers" under the current or proposed lending models. It is unlikely that WebBank would be agreeable to act as a co-issuer and there is a substantial risk that WebBank would withdraw from the present arrangement. Providing the financial details for every borrower member would be administratively difficult, would increase the chances of liabilities arising from misstatements, and discourage borrower members from participating in the business.

The 1933 Act defines an "issuer" as:

- "Every person who issues or proposes to issue any security...",
- "the person or persons performing the acts and assuming the duties of depositor or manager pursuant to the provisions of the trust or other agreement or instrument under which such securities are issued…", "the person by whom the equipment or property is or is to be used…", and
- "the owner of any such right or of any interest in such right (whether whole or fractional) who creates fractional interests therein for the purpose of public offering…".[49]

The term "person" includes corporations.[50]

Ordinarily, an issuer sells ownership in itself in order to raise capital. Under the current and proposed models, Lending Club holds the promissory notes from the borrower member. Rather than giving these promissory notes to lending members, Lending Club gives lending members a note which entitles them to the principal and interest from the specific loan that they chose to fund. As a result, the firm hopes Lending Club would be an issuer under either model should the notes be deemed securities.

In *Prudential Ins. Co. v. SEC*, an insurer set up separate accounts to fund variable annuities, which it then offered to the public.[51] The value of the annuity was dependent on the value of the securities in these separate accounts. Even though the accounts were not separate business entities, the court held that they were still "investment companies" and "co-issuers" of the securities under the 1940 Act.[52] Guarantors, on the other hand, were not considered co-issuers, although they must still fulfill lesser regulator's requirements.[53] Under its new approach, Lending Club could argue that the Notes are analogous to the separate accounts, and that WebBank and the borrowing members are more analogous to the guarantors. Like the separate accounts, the value of the Notes is dependent on the value, or repayment, of the underlying loans.

Lending Club can also analogize its product to a form of municipal securities known as industrial development revenue bonds (IDRBs). IDRBs are government-issued bonds used to raise capital for private sector companies who are undertaking specific projects that the government wants to see financed. These

[49] 15 U.S.C. § 77b(a)(4) (exemptions omitted).

[50] United States v. Rachal, 473 F.2d 1338 (5th Cir. 1973).

[51] 326 F.2d 383 (3d Cir. 1964).

[52] *Id.*

[53] Guarantors must sign and include their financial statements in the registration statement but are not required to make periodic reports. *See* American Home Assurance Company, SEC No-Action Letter (Oct. 17, 2005).

bonds are tradable on secondary markets. For example, a city could issue bonds for Company A to build a bridge. The city issues bonds to investors, and uses the capital to fund Company A's work on the bridge. The city is then responsible for repaying bond holders, but its obligation to repay the bonds is limited to proceeds received from the bridge's operations. The SEC treats the city, rather than the private company undertaking the project, as the sole issuer of the bonds. Just as IDRBs allow citizens to invest in a specific project (the bridge), lending members can invest in a specific loan. [54]

Even if Lending Club can demonstrate that its product *looks* similar to IDRBs, there is still a risk that the SEC will be unwilling to *treat* the MPD Notes like IDRBs. First, the Securities Act gives municipal securities special status, exempting them from registration requirements.[55] The primary purpose of the securities law is to protect investors. Because municipal securities are overseen by a government entity, the law has far greater confidence in the trustworthiness of the issuer, and the likelihood that the investor will get the expected return on their investment. The same is not true when the sponsoring entity is a private company, like Lending Club.[56]

Business Considerations

Assessing the Registration of Securities Offerings Under the Securities Act of 1933

The decision to register with the SEC involves a number of risks and costs which could impact the competitiveness of Lending Club's business model. If it is determined that Lending Club's funding model creates securities, the firm (and any other co-issuers) would be required to register any public offering of those securities under the Securities Act of 1933; the firm would also have considerable ongoing disclosure obligation under the Securities Exchange Act of 1934. While compliance with SEC registration requirements might enhance the firm's reputation and possibly increase confidence in the firm's services, SEC registration entails substantial initial and on-going costs for compliance, as well as the risk of litigation regarding Notes already issued prior to registration. At a minimum, registration would require the firm to interrupt its operations for a quiet period that might last for a few months, forcing it to fall further behind Prosper, which already has a dominant position in the peer-to-peer space. If Lending Club registers, it also risks that the SEC will treat WebBank or lending members as issuers or co-issuers.

To elaborate a bit more: Section 5 of the 1933 Act restricts the ability of issuers and their underwriters to promote the offering or soliciting of purchase orders until the registration statement is filed with the SEC (quiet period) and it bars any sale of securities until the registration statement becomes effective. Any activity that is likely to promote investor interest in the offering is likely to violate Section 5.[57] Lending Club would therefore have to stop allowing lender members to fund any loans and any borrowings sanctioned during the quiet period. Though the Act states that the registration statement becomes effective within a limited number of days after it is filed with the SEC, the registration statement

[54] *See* Louis Loss, Joel Seligman and Troy Paredes, SECURITIES REGULATION 23–24 (4ed. 2008).

[55] 15 U.S.C. § 77(c)(2) (2010).

[56] *See* Robert S. Amdursky, *Creative State and Local Financing Techniques*, 249 PLI N4-4429, 347 (1984) ("Traditionally, municipal securities have been considered the most secure category of investments second only to obligations of the federal government.").

[57] *See* Cox, Hillman, and Langevoort, *supra* note 24 at 147, 159.

is subject to review and comment from the SEC, which may substantially lengthen the process.[58] Under Section 8 of the 1933 Act, the SEC may refuse to permit a registration statement from becoming effective,[59] issue a stop order, or institute any public proceeding or examination arising out of any deficiencies or misleading information in the registration statement.[60] The process may take several rounds of correspondence and amendments, especially given the unique nature of Lending Club's business models.

After filing a registration statement, Lending Club will become subject to anti-fraud liability under federal securities law for information provided in the statement and on its website. This poses a challenge for our client, because the federal Gramm-Leach-Bliley Act ("GLBA") limits the disclosure of nonpublic personal information about a consumer to nonaffiliated third parties, requires financial institutions to disclose certain privacy policies and practices with respect to information sharing with affiliated and nonaffiliated entities, and obligates financial institutions to safeguard personal customer information. Several states have similarly enacted privacy and data security laws requiring safeguards to protect the privacy and security of consumers' personally identifiable information and requiring notification to affected customers in the event of a breach. However, some of the information regarding the member borrowers may require investigation and disclosure in order to comply with the anti-fraud provisions of the Act.

Once the securities are offered pursuant to Section 5 of the 1933 Act, Lending Club would become a public company. This will result in significant legal, accounting, and other expenses that Lending Club did not incur as a private company. A substantial amount of time would need to be allocated towards public company compliance requirements. Some of these may include obtaining better coverage for D&O liability insurance, given that the liability of directors and executive officers of the company would increase. As a public company, Lending Club will be subject to the Sarbanes-Oxley Act, which requires effective internal controls over financial reporting, disclosure controls, and procedures.[61] This would require our client to put in place systems that meet the Act's requirements, incurring substantial accounting expense, expending significant management time on compliance-related issues, and hiring additional accounting and financial staff with appropriate public company experience and technical accounting knowledge. Failure to do so would subject our client to sanctions or investigations by the SEC or other regulatory authorities.

Three Options Under Consideration

Lending Club's top executives have identified several different possible courses of action going forward. In light of your analysis of the legal issues, they would like your assessment of the pros and cons of each approach as well as a recommendation as to which approach you would suggest they pursue:

First, Lending Club could take a "wait and see" approach, forgo the secondary market, and continue to operate under the current lending model. This option carries with it a risk of sanctions if the

[58] *See* 15 U.S.C. § 77a(8)(a) (2010).

[59] *See* 15 U.S.C. § 77a(8)(b) (2010).

[60] *See* 15 U.S.C. § 77a(8)(d) (2010).

[61] *See* Sarbanes Oxley Act, 15 U.S.C. § 7201 (2002).

SEC determines that the notes under the current model are unregistered securities. The SEC has broad-ranging powers to issue cease-and-desist orders and to impose civil monetary penalties for violations of federal securities laws.[62] Any violation of a cease-and-desist order is punishable by a civil penalty in addition to a mandatory injunction directing compliance with the order. The SEC has further powers to suspend trading of a security or stop further issuances of new securities. As a result, Lending Club could face substantial legal and business costs should the SEC decide to proceed against it. On the other hand, as other peer-to-peer lenders, notably Prosper, have a much larger market share than Lending Club, it may be unlikely that the Commission staff would target Lending Club for an initial enforcement action, especially if it keeps its head down.

Second, Lending Club could approach the SEC for a no-action letter from the staff. Under this approach, Lending Club would seek to persuade the staff its new Version 3.0 funding model does not create securities for purposes of federal securities laws and, on that basis, the staff would then recommend to the Commission that no enforcement action be taken with respect to Version 3.0. No-action letters of this sort are often issued in response to requests made when the legal status of an activity is not clear, as is arguably the present case. A no-action letter would only provide partial certainty: the letter indicates the SEC's intentions, but is not binding in the courts. If Lending Club requests a letter, it also risks drawing the SEC's attention to its current practices. If the staff is unwilling to provide a no-action letter, the Company would almost certainly have to register with the Commission if it were to pursue Version 3.0, and – indeed – the company may effectively be committing to pursue Version 3.0 through SEC registration if it opens up a dialog on a no-action letter. This option thus also presents non-trivial regulatory risks and costs, as there is no industry precedent to serve as a benchmark for the probability of the SEC approving our client's registration. Should the notes be deemed securities, the registration and compliance requirements may substantially increase overhead and business costs, which may drive up the fees charged by our client, ultimately hurting the viability of the business.

Another option is to make a joint representation to the SEC with other P2P lenders operating in the United States, arguing that the notes issued under the P2P lending business models should be exempt from registration requirements under Section 5 of the 1933 Act. While this strategy would allow Lending Club to continue to use its current lending model, it may prevent Lending Club from creating a secondary trading platform for the MPD Notes. A joint representation to the SEC may help lay industry standards, save considerable costs and compliance burdens—should they get the exemption. However, coordinating a joint effort may be time consuming and our client could lose out on the significant competitive advantage as a "first mover" gained by acting independently and successfully registering with the SEC.

Appendix

1. Brad Slavin, Peer-to Peer Lending – An Industry Insight (June 21, 2007). http://www.bradslavin.com/wp-content/uploads/2007/06/peer-to-peer-lending.pdf

[62] *See* Cox, Hillman, and Langevoort, *supra* note 24 at 814.

HARVARD LAW SCHOOL | The Case Studies

CSP043
JUNE 2020

Strategic Options and Legal Risks for Elite ReFi, Inc.

HOWELL E. JACKSON, MARGARET E. TAHYAR, AND JAI MASSARI

Memorandum

DATE:	June 2020
TO:	Associate Team
FROM:	Partner, XYZ Law LLP
RE:	Strategic Options and Legal Risks for Elite ReFi, Inc.

I received a call last night from Katie Harris, the former associate who left our team two weeks ago to become the first general counsel of Elite ReFi, Inc. (*ReFi*). As you will recall from Katie's goodbye dinner, ReFi is a socially-responsible marketplace lender that operates an online platform for the refinancing of student loans. I am going to be on a plane for most of the day, but can chat with you this evening right before we have a face-to-face meeting with ReFi's general counsel and senior management. I'll be coming directly from the airport, so let's meet at the coffee shop across the street from Elite ReFi's offices about a half hour before the meeting. Representatives of Finventures Capital Group LLP (*Finventures*), a small Fintech-focused investment fund and current investor in ReFi, and RedRock LLP (*RedRock*), a large private equity fund considering investing in ReFi, will be at the meeting as well. We are under some time pressure and the budget is tight.

What follows are my quick notes from my call with ReFi's general counsel. Don't be afraid to point anything out that you think I might have gotten wrong – I jotted these down in haste while on the call and haven't had the time to review.

ReFi offers student loan refinancing nationwide, but only to those with a graduate professional degree (e.g. M.D., J.D., M.B.A., or D.M.D.) and who are currently employed in their professional field. ReFi takes advantage of the fact that many federal student loans to graduate students in recent years carried higher than market interest rates, with the result that refinancing can lower the interest rate on student loans for this target demographic. ReFi also offers the option to stretch out payments.

Written by Margaret E. Tahyar & Jai Massari of Davis Polk & Wardwell, with the assistance of Howell E. Jackson, James S. Reid Jr., Professor of Law, Harvard Law School. An earlier version of this case study benefited from substantial work by Adam Fovent and Madison Roberts. Cases are developed solely as the basis for class discussion. They are not intended to serve as endorsements, sources of primary data, legal advice, or illustrations of effective or ineffective management.

Copyright © 2020 President and Fellows of Harvard University. No part of this publication may be reproduced, stored in a retrieval system, used in a spreadsheet, or transmitted in any form or by any means—electronic, mechanical, photocopying, recording, or otherwise—without permission. To order copies or permissions to reproduce materials please visit our website at casestudies.law.harvard.edu or contact us by phone at 617-496-1316, by mail at Harvard Law School Case Studies Program, 1545 Massachusetts Avenue – Areeda 507, Cambridge, MA 02138, or by email at HLSCaseStudies@law.harvard.edu.

ReFi suddenly grew much more quickly than anticipated after their much larger competitor suffered both platform issues and a scandal around whether its algorithm contained racial bias and was shut down for several weeks. Accordingly, most of ReFi's management's attention in the past year has been on making sure that its online platform remained operational in light of the increased traffic.

Given its success with the graduate professional demographic, ReFi has decided to begin offering student loan refinancing to those with undergraduate computer science and certain other undergraduate STEM degrees. ReFi's premise is that it will continue to work only with those who are currently employed in their field and with respect to whom ReFi's algorithm signals a very low default risk.

Opening up the platform to this wider pool will require additional funding. Finventures was an early investor in ReFi and has been quite pleased with the recent unexpected growth. As a result, Finventures recently participated in a new round of financing for ReFi, realizing that further investment will soon be needed. The funds from the recent round have not yet been deployed, but as a business matter they must be soon. ReFi has hired a consulting firm (*McBain*) and a boutique investment bank (*ZerpBank*) to evaluate its options for deploying the recent round and to help it find additional investors. One of these potential additional investors is RedRock, a large private equity fund.

ReFi was started by several graduate students only three years ago who originally operated it part-time. The company's budget for legal services has been very slim – in the beginning, ReFi's founders relied upon part-time help from their law school classmates. Once the company took off, ReFi hired a retired lawyer who had specialized in securitization to advise on the impacts of the Second Circuit's decision in *Madden v. Midland Funding, LLC*[1] and recent true lender litigation for ReFi's business model. That lawyer, who in retirement was operating as a solo practitioner, delivered ReFi a memorandum adopting the view that the *Madden* case and true lender cases are limited in application strictly to their facts and apply only to debt collectors and other predatory lenders, like payday lenders. Because of its tight legal budget, ReFi did not revisit that advice over the past three years, instead relying on updates from general news, its investment bankers, and informal discussions with consultants. The memorandum was made available to Finventures when it did its diligence during its investment rounds and has been made available to RedRock.

In light of its recent growth, and after discussions with its investors, ReFi and its founders realized that they had reached the stage where they needed in-house counsel and compliance capabilities. They hired Katie Harris, our former associate, as their first general counsel the week after the last financing from Finventures closed. Upon reviewing the three-year-old memorandum analyzing the implications of *Madden* and the true lender cases, one of her first actions as general counsel was to suggest the memorandum's analysis was out of date and might have always underestimated the legal risks that *Madden* and the true lender cases present to ReFi's business model. Finventures and the founder management are convinced that the new general counsel is overstating the risks.

ReFi, Finventures, and RedRock have decided to split the cost of hiring us. They all seek our views on the risks that *Madden* and the true lender cases pose to ReFi's business model. We may need to set up a call with our general counsel's office here at XYZ Law LLP to make sure they don't see any problems with this arrangement.

[1] *Madden v. Midland Funding, LLC*, 786 F.3d 246 (2d Cir. 2015), *cert. denied*, 136 S. Ct. 2505 (2016). Attached as Appendix I.

McBain and ZerpBank have already prepared a slide deck with strategic expansion options for ReFi, a copy of which has been given to us to help speed along our analysis and which is attached as Appendix II.[2] I flipped through this quickly and noticed a few things we will need to think carefully about.

ReFi's Business

ReFi was incorporated in Delaware in 2016 and operates an online marketplace lending website specializing in the refinancing of student loans. ReFi is a strong proponent of responsible lending and has adopted a range of internal policies and practices in order to facilitate greater access to student loan refinancing in a manner informed by a holistic understanding of customers' present and ongoing ability to repay.

Customers interested in refinancing their student loans submit an application through ReFi's online platform, which is open to customers nationwide. A decision on whether or not to approve the application for refinancing is made on the basis of the information provided in the customer's application and on ReFi's internal proprietary data analytics and credit assessment tools. ReFi does not itself extend credit to the relevant customer, which would subject ReFi to state and federal regulatory burdens, such as the need to obtain state lending licenses and to comply with state usury laws, which would limit on a state-by-state basis the interest rates ReFi can charge. Instead, once an application has been approved, the refinanced loan is originated by Elite ReFi's partner bank, Squarestream, a state-chartered digital bank that specializes in being a bank partner to market place lenders. Elite ReFi has just renegotiated an exclusive 3-year contract with Squarestream at very favorable pricing. Squarestream is not subject to any limit on the interest rates they charge.

The loans approved through ReFi's marketplace lending platform and originated by Squarestream do not remain on the banks' books. In fact, the bank immediately sells 100% of the loans to ReFi. In the past, ReFi has relied on equity capital to finance these purchases. However, in order to maximize the availability of refinancing through its platform, and thereby also maximize the commission-based revenue it earns through the platform, ReFi also on-sells the loans to fixed income investors. ReFi has employed a range of funding models in this regard, including selling whole loans to institutional investors, securitizing loans, and selling pass-through interests in loans to retail investors under a peer-to-peer lending program.[3]

This bank partnership model was critical in ReFi's expansion over the past three years. It allowed ReFi to provide uniform and advantageous interest rates nationwide as interpreted by the Supreme Court's *Marquette* decision and 12 U.S.C. §85, which allows a federally-chartered bank headquartered in one state to charge interest on any loan at the rate allowed by the laws of the state in which it is headquartered.[4] A similar provision applies to state-chartered banks.[5] Together, by the operation of federal preemption, these provisions allow a bank to export interest rates which are permissible based on the location of the bank's headquarters or the state in which it is chartered, even when transacting with

[2] McBain and ZerpBank, STRATEGIC EXPANSION OPTIONS: ELITE REFI. Attached as Appendix II.

[3] **Note:** Students do not need to consider any securities law issues associated with these funding sources.

[4] 12 U.S.C. § 85; Marquette Nat'l Bank v. First Omaha Serv. Corp., 439 U.S. 299 (1978).

[5] 12 U.S.C. § 1831d(a).

customers in states where such rates would not be permissible were the bank located or chartered there. This ability to export rates throughout the country is particularly important given that usury laws, which set the maximum rate of interest that lenders may charge on consumer loans, vary substantially from state to state.

As understood during ReFi's operations to date, the ability of Squarestream to export rates permissible based on the location of their headquarters not only ensured the validity of refinancing loans when initially originated by those banks, but also ensured their ongoing validity and enforceability in the hands of subsequent assignees of the loans, including ReFi and the third parties to whom ReFi sells the loans. Given the funding sources relied on by ReFi, these legal features of ReFi's bank-partnership business model have been crucial to the company's operations and expansion.

Sources of Legal Risk

In the same three-year period in which ReFi rapidly expanded its nationwide operations, there were a series of legal developments challenging the above-described traditional understanding of rate exportation and preemption of state usury laws. We've done work in this area before, so I've pulled together this summary based on a past memorandum. I have summarized the main sources of legal risk I would like you to consider. I have also attached to this Memo as Appendices some of the relevant materials, and as Appendix VI a legal memorandum we prepared for another client which considers these legal risks in detail.[6] Note: This work was carefully vetted by a number of partners, so you should consider it a reliable reference when working through my rough summary below.

The "Valid-When-Made" Doctrine and Madden v. Midland Funding

The traditional understanding of rate exportation and preemption of state usury laws alluded to above is an application of the valid-when-made doctrine. The valid-when-made doctrine provides that a loan that is valid at its inception cannot become usurious upon subsequent sale or transfer to another person. This doctrine is one of long standing, having been recognized by the Supreme Court as early as 1828.[7] Indeed, in 1833, the Supreme Court described as a cardinal rule the proposition "that a contract, which, in its inception, is unaffected by usury, can never be invalidated by any subsequent usurious transaction."[8]

Application of the valid-when-made doctrine to ReFi's bank-partnership model would indicate that because of the ability of Squarestream under federal statute to charge interest rates permissible based on the location of its headquarters, any loan originated by it should be valid and not subject to challenge under conflicting state usury laws when in the hands of a subsequent non-bank purchaser or assignee. Notwithstanding the valid-when-made doctrine, recent legal developments have cast doubt on the enforceability of out-of-state interest rates in the hands of non-bank loan purchasers and assignees.

[6] Randall D. Guynn, Jai R. Massari & Margaret E. Tahyar, DAVISPOLK FINREG, MEMORANDUM FOR MARKETPLACE LENDING ASSOCIATION, "*Federal Banking Regulators Can and Should Resolve Madden and True Lender Developments*," Aug. 14, 2018, https://www.finregreform.com/single-post/2018/08/14/federal-banking-regulators-can-resolve-madden-true-lender-developments/. Attached as Appendix VI.

[7] Gaither v. Farmers & Mechs. Bank of Georgetown, 26 U.S. (1 Pet.) 37, 43 (1828).

[8] *Nichols v. Fearson*, 32 U.S. (7 Pet.) 103, 109 (1833).

In particular, the decision of the United States Court of Appeals for the Second Circuit in *Madden v. Midland Funding, LLC* has generated much uncertainty in the ongoing application of the valid when made doctrine.[9]

The plaintiff in that case, Saliha Madden, was a New York resident who opened a credit card account with Bank of America, a national bank.[10] In 2005, Madden's account was sold to another national bank, which later charged off the account as uncollectible, before itself selling the account to Midland Funding.[11] Through an affiliate, Midland Funding sought to collect Madden's debt at an interest rate of 27% per year, which was the rate chargeable pursuant to the terms of the credit card agreement with Bank of America.[12] Madden filed suit in the Federal District Court against Midland Funding and its affiliate, alleging a violation of New York's state usury law, which imposed a maximum interest rate of 25%.[13]

Judge Seibel in the United States District Court for the Southern District of New York held that because the underlying credit card loan was originated by a national bank, the National Bank Act preempted state usury law.[14] Citing authority from the Fifth and Eighth Circuits,[15] Judge Seibel reasoned that when examining the application of National Bank Act preemption in the context of loan assignments, courts look at the originating bank and not the subsequent assignee.[16]

On appeal, the United States Court of Appeals for the Second Circuit reversed, holding that the National Bank Act did not preempt Madden's state usury law claim because Midland Funding and its affiliates were not national banks, subsidiaries or agents of a national bank, or acting on behalf of a national bank, and thus were not entitled to the protection of National Bank Act preemption.[17] In so concluding, the Second Circuit did not analyze or address the valid-when-made doctrine.

Midland Funding petitioned for a writ of certiorari on the question whether the National Bank Act "continues to have preemptive effect after the national bank has sold or otherwise assigned the loan to another entity."[18] Midland Funding argued in its petition that the Second Circuit's decision was erroneous because it "allows state law to infringe the core enumerated power of national banks to set interest rates at the level allowed by their home States."[19] In this regard, Midland Funding argued that 12 U.S.C. §85 "incorporates the principle that an interest rate set by an originating bank cannot be invalidated by a subsequent assignment of the loan" and that "[t]he valid when made doctrine is essential to a national bank's ability to set interest rates."[20] Midland Funding further argued that the Second Circuit erred in failing to take into account the broader preemption by 12 U.S.C. §25b of state consumer financial laws that prevent or significantly interfere with the ability of national banks to exercise their powers.[21] Various

[9] Madden, supra Note 1.

[10] *Id.* 247.

[11] *Id.* 248.

[12] *Id.*

[13] *Id.*

[14] *See* Petition for a Writ of Certiorari, *Midland Funding, LLC v. Madden,* No. 15-610.

[15] *Id.* 8; *See, e.g., Phipps v. FDIC,* 417 F.3d 1006, 1013 (8th Cir. 2005).

[16] *See* Petition for a Writ of Certiorari, *Midland Funding, LLC v. Madden,* at 8.

[17] *Madden v. Midland Funding, LLC*, 786 F.3d 246, 249-253 (2d Cir. 2015).

[18] Petition for a Writ of Certiorari, *Midland Funding, LLC v. Madden,* at 2.

[19] *Id.* 15.

[20] *Id.* 16.

[21] *Id.* 17.

amicus briefs were filed in support of Midland Fund's petition for certiorari, including by industry groups such as the American Bankers' Association. On the Supreme Court's invitation, an amicus brief was filed by the Solicitor-General and the Office of the Comptroller of the Currency expressing the views of the United States. Although that brief characterized the Second Circuit's decision as "incorrect," including its failure to consider the valid-when-made doctrine, it described the case as a poor vehicle for resolution of the application of National Bank Act preemption to state usury law claims against a subsequent assignee.[22] The Supreme Court ultimately denied Midland Funding's petition for a writ of certiorari.

As a decision of the Second Circuit, *Madden* is binding only in Connecticut, New York, and Vermont. However, it appears that the reasoning in *Madden* is influencing courts in other parts of the country. For example, *Madden* was cited by Chief Judge Castillo in the Northern District of Illinois in reasoning that National Bank Act preemption did not apply and thus denying a motion to dismiss a state usury law action.[23][24]

We need to think about the potential legal risks for ReFi's business model and funding sources as a result of the *Madden* decision.

True Lender Developments

A further legal development posing potential risks to ReFi's business model is the emergence of "true lender" analyses under which courts have exhibited a willingness to look through bank-partnership arrangements and characterize nonbank partners as the true lender on loans in form originated by the bank partner. Courts applying this theory have increasingly applied a "predominant economic interest" test in determining whether a bank or its nonbank partner is the true lender in a particular transaction.

In *Consumer Financial Protection Bureau v. CashCall, Inc.*, attached to this Memo as Appendix IV,[25] the United States District Court for the Central District of California applied the true lender approach to a "tribal model" of lending. The defendant in that case, CashCall, was a Californian corporation operating in the payday lending industry. In 2006, in order to expand its operations beyond California, CashCall entered into partnerships with two banks under which loans were originated by the partner banks but then purchased from the banks and serviced on an ongoing basis by CashCall.[26] This bank partnership model was intended to take advantage of the pre-*Madden* understanding of federal preemption of state usury law claims against subsequent assignees of bank originated loans.

After CashCall's bank partners withdrew from this arrangement, CashCall entered into an agreement with Western Sky Financial, a South Dakota limited liability company formed by a member of the Cheyenne River Sioux Tribe (CRST) and licensed to do business by the CSRT.[27] Under the agreement, CashCall was under an obligation to purchase loans originated under the name of Western Sky Financial,

[22] Brief for the United States as Amicus Curiae, Midland Funding, LLC v. Madden, No. 15-610.

[23] *Eul v. Transworld Systems, Inc.*, 2017 WL 1178537 (N.D. Ill. Mar. 30, 2017).

[24] *OCC*, Permissible Interest on Loans that are Sold, Assigned, or Otherwise Transferred, May 29, 2020 (pending publication in the Federal Register). Attached as Appendix III.

[25] *Consumer Financial Protection Bureau v. CashCall, Inc.*, No. CV 15-7522-JFW (RAOx), 2016 WL 4820635 (C.D. Cal. Aug. 31, 2016). Attached as Appendix IV.

[26] *Id.* *1.

[27] *Id.* *2.

with the proceeds from these purchases funding the origination of further loans.[28] Loans applications were originally made through CashCall agents, or through a Western Sky website hosted on CashCall's servers in California.[29] As the partnership continued, Western Sky loan agents employed on the CSRT reservation handled an increasing amount of calls from prospective borrowers.[30] At all times, the loan agreement for loans originated under this partnership identified Western Sky Financial as the lender.

In March 2014, the Consumer Financial Protection Bureau (CFPB) initiated proceedings alleging that CashCall had engaged in unfair, deceptive, and abusive acts and practices in violation of the Consumer Financial Protection Act of 2010 by servicing and collecting on loans that were wholly or partially void or uncollectible under state licensing and usury laws.[31] In granting the CFPB's motion for partial summary judgment, Judge Walter agreed with the CFPB's contention that in order to identify the "true lender" under the loans, one "should consider the substance, not the form, of the transaction."[32] The Court explained that "[i]n identifying the true or de facto lender, courts generally consider the totality of the circumstances and apply a predominant economic interest [test], which examines which party or entity has the predominant economic interest in the transaction."[33] Judge Walter ultimately concluded that CashCall, and not Western Sky Financial, was the true lender, emphasizing that it was CashCall that placed its money at risk, that CashCall purchased each and every loan before any payment was made, and kept enough money on deposit with Western Sky Financial to fund two days of loans at any one time.[34] Judge Walter went on to conclude that the CFPB had established that the loans were void or uncollectible under the laws of most borrowers' states, and that CashCall, as the true lender on the loans, had therefore engaged in violations of the Consumer Financial Protection Act.[35]

Courts in New York,[36] West Virginia,[37] and Maryland[38] have applied the true lender theory to look through the bank partnership model in the payday lending context. Further, in a number of states, plaintiffs and regulators are now invoking the true lender theory in relation to marketplace lenders and other non-payday lenders that rely on the bank partnership model.[39] In Georgia, the true lender theory applies, at least in the payday lending context, as a matter of statute.[40] We need to think about the potential risk of ReFi being deemed the true lender on loans originated through the platform.[41]

[28] *Id.*

[29] *Id.* *3.

[30] *Id.*

[31] *Id.* *4.

[32] *Id.* *5.

[33] *Id.* *6 (internal quotation marks omitted).

[34] *Id.*

[35] *Id.* *9-*11.

[36] People ex rel. Spitzer v. Cty. Bank of Rehoboth Beach, Del., 846 N.Y.S.2d 436 (2007).

[37] *CashCall, Inc. v. Morrissey*, No. 12-1274, 2014 WL 2404300 (W.Va. May 30, 2014).

[38] CashCall, Inc. v. Maryland Comm'r of Fin. Reg., 139 A.3d 990 (Md. 2016).

[39] *See, e.g., Meade v. Marlette Funding, LLC*, No. 17-CV-00575-PAB-MJW, 2018 WL 1417706 (D. Colo. Mar. 12, 2018); *Meade v. Avant of Colo., LLC*, No. 17-CV-0620-WJM-STV, 2018 WL 1101672 (D. Colo. Mar. 1, 2018); *Indelicato v. Kabbage, Inc.*, No. 1:17- CV-11976 (D. Mass. Oct. 12, 2017).

[40] The Georgia Payday Lending Law codified a predominant economic interest test to determine when a "purported agent shall be considered a de facto lender" for purposes of applying state usury laws to payday loans.

[41] **NOTE:** Students should focus on the true lender aspects of the reasoning in *Consumer Financial Protection Bureau v. CashCall, Inc.,* and the legal risk of Refi, rather than Squarestream, being deemed the "true lender" on loans originated through Refi's platform. Students need not focus on the choice of law issues analyzed in *Consumer Financial Protection Bureau v. CashCall*, *Inc*.

Choice of Law Issues

At present, the loan agreements for student loan refinancing approved through ReFi's platform and originated by Squarestream contain a provision identifying the law of Utah as the governing law of the contract. Along with the federal preemption and true lender developments discussed above, there is a further potential risk that, depending on a borrower's state of residence at the time their loan was originated and/or at the time proceedings are brought on the loan, a Court may decide not to uphold the choice of Utah law as the governing law of the loan agreement.

Under choice of law principles, courts generally apply the law of the state chosen by the parties to govern their contract.[42] However, there are limited circumstances in which the courts will not uphold the parties' choice of law, such as where application of the chosen law would be contrary to public policy of the forum state.[43] Some courts have taken the view that state usury law limits reflect fundamental matters of public policy, such that a loan that is non-usurious under the governing law of the loan agreement may not be enforced by courts in other states based on the usury law of those states.[44] However, analysis of this source of legal risk is outside the scope of our retainer and so you should not dwell on these choice of law issues.[45]

Expansion Options

As set out in the pitch deck contained in Appendix I, McBain and ZerpBank have identified a number of strategic expansion options for the company.[46]

ReFi was started by five friends who were unhappy with the refinancing options for their own student loans. One of them, now almost 30, was criminally charged with the use of a false ID in a bar when he was 20 and was required to perform community service. Two of the other founders are from emerging market countries which have recently been identified by the Federal government as the source of government-sanctioned cyberattacks. The new general counsel of ReFi has advised that, in light of these facts, obtaining a bank charter would be more than usually complex. Senior management has decided that it would take far too long and be too risky for ReFi to seek a bank charter at this time. That option is off the table for strategic consideration.

Option 1 – Continue expansion plans unabated; modify documentation to avoid risk

Under McBain and ZerpBank's Option 1, ReFi would work with Squarestream to preclude any *Madden* or true lender issues by amendment of the loan documentation. In particular, the loan agreement for student loan refinancing approved through the ReFi Platform and originated by Squarestream would

[42] *See, e.g.,* Restatement (Second) of Conflict of Laws § 187 (1971).

[43] *Id.*

[44] *See, e.g., Madden v. Midland Funding, LLC.,* 237 F.Supp.3d 130, 151 (S.D.N.Y. 2017) (Concluding that "to apply Delaware usury law would violate a fundamental public policy of the state of New York").

[45] **NOTE:** Students need not dwell on the choice of law issues, nor on whether the choice of Utah law as governing loan agreements originated under the Refi platform would be respected.

[46] **NOTE:** Students should not assume that all information contained in the pitch deck is accurate. Nor should students assume that the client has given the partner all of the facts or understands the interconnections between all of the facts.

be amended so that borrowers agree (a) not to challenge the loan as usurious notwithstanding any future assignment;[47] and (b) that Squarestream, and no other party, is the true lender under the loan.[48]

I have not entirely thought through whether this would actually work. Please look into whether we could draft some contractual language to circumvent state usury statutes and the true lender analysis.

Option 2 – Continue expansion plans unabated; risk reducing actions not needed

Under McBain and ZerpBank's Option 2, ReFi would leverage its recent influx of capital from Finventures and future financing rounds to fund aggressive expansion plans in order to take advantage of the favorable current market conditions and lack of direct competition. Given that ReFi is facilitating borrowers refinancing at lower rates and adheres to responsible lending practices, ReFi would proceed on the basis that it is less likely than other lenders to be the target of class actions or regulatory scrutiny. The legal risks impact the entire marketplace lending sector and ReFi is less impacted than others. Given that there has been an influx of capital that must be deployed, there is no choice but to proceed while accepting the legal risks.

In any event, the OCC and FDIC have recently released for comment a proposed regulatory fix, an example of which is attached as Appendix V.[49] McBain and Zerpbank have advised senior management that they are confident final rules will be adopted in the near future that will completely address the *Madden* and true lender issues.[50]

It is my concern that McBain and Zerpbank are overconfident. There has been quite a bit of media response to the proposed rules, representative examples of which are attached as Appendix VII,[51] so we need to think carefully about what we can predict about the likelihood that these proposals will be adopted and the scope of what they actually cover. I have not read the proposals in full, so we'll also need to double check that they actually address legal risks from the perspective of both *Madden* and true lender litigation.

Option 3 – Expand strategically; take risk reducing actions

Under McBain and ZerpBank's Option 3, ReFi would seek to limit exposure to California, due to true lender risk, and to states within the Second Circuit, the most important of which commercially would

[47] *But cf.* New York Jurisprudence, 2d, Interest and Usury § 56 ("Usury is not a crime in itself or *malum in se*; it is merely *malum prohibitum*. Both as an offense against the laws and a defense in suits in court, it is dependent upon express statute, and in determining the rights and remedies of the parties to a usurious exaction of interest, reference must be made to the provisions of the statute involved…Lenders, with the money, have all the leverage; borrowers, in dire need of money, have none. Thus, the laws defining and prohibiting usury are intended to protect against a lender's overreaching."); *Trinity Fire Ins. Co. v. Kerrville Hotel Co.,* 103 S.W.2d 121, 128-129 (1937) ("[W]e have found no authority…which would sustain the proposition that estoppel against pleading usury may be worked by merely stating in the original instrument itself, which does not disclose the usury, that it constitutes the sole and only contract between the parties, or even by directly stating in such instrument that the contract is free from the taint of usury.").

[48] Recall that in *Cash Call,* Judge Walter agreed with the CFPB's contention that in order to identify the "true lender" under the loans, one "should consider the substance, not the form, of the transaction."

[49] Permissible Interest on Loans That Are Sold, Assigned, or Otherwise Transferred, 84 Fed. Reg. 64229 (proposed Nov. 21, 2019) (The OCC proposes to amend 12 CFR 7.4001 and 12 CFR 160.110 to provide that interest on a loan shall not be affected by the sale, assignment, or other transfer of the loan) (Attached as Appendix V.)

[50] **NOTE:** Students should assume the political and economic conditions in effect as of January 2020.

[51] *See* Appendix VII.

be New York, due to the *Madden* decision. ReFi has, to date, been very active in both California and New York, which are key markets for student loan refinancing. Under this option, ReFi would limit itself to providing refinancing to customers who currently live in states whose laws remain true lender and *Madden* friendly. In this regard, ReFi will focus its expansion efforts on markets with growing STEM-focused workforces, such as Austin, Charlotte, Nashville, and Phoenix.

Assessing the Risks

Evaluate the legal risks and how they impact the needed business decisions from the perspectives of ReFi, Finventures, and RedRock.

Assume that you do not have access to the partner for further information until half an hour before the meeting with the general counsel and senior management of ReFi, and representatives of Finventures and Redrock. Consider how you will brief the partner and how you ought to handle the meeting.

While ReFi and its business are fictional, in evaluating the legal risks with respect to the business and its expansion, students should assume the political and economic conditions in effect as of June 2020.

Do not consider any securities law violations that might have occurred in the fundraising. For current purposes, assume that Finventures was responsible for its own diligence and is not interested in abandoning the investment.

Appendices

1. Madden v. Midland Funding, LLC, 786 F.3d 246 (2d Cir. 2015), cert. denied, 136 S.Ct. 2505 (2016).
2. McBain and ZerpBank – Strategic Expansion Options for Elite ReFi (Davis Polk deck).
3. OCC, Permissible Interest on Loans that are Sold, Assigned, or Otherwise Transferred, May 29, 2020 (pending publication in the Federal Register). https://www.occ.gov/news-issuances/federal-register/2020/nr-occ-2020-71a.pdf
4. Consumer Fin. Prot. Bureau v. CashCall, Inc., No. CV 15-7522-JFW (RAOx), 2016 WL 4820635 (C.D. Cal. Aug. 31, 2016). https://static.reuters.com/resources/media/editorial/20180411/cfpbvcashcall--SJopinion.pdf
5. Permissible Interest on Loans That Are Sold, Assigned, or Otherwise Transferred, 84 Fed. Reg. 64,229 (Nov. 21, 2019). https://www.govinfo.gov/content/pkg/FR-2019-11-21/pdf/2019-25280.pdf
6. Memorandum for Marketplace Lending Association – Federal Banking Regulators Can and Should Resolve Madden and True Lender Developments" (Aug. 14, 2018). https://www.finregreform.com/wp-content/uploads/sites/32/2018/08/Madden-True-Lender-Federal-Regulatory-Fix-Whitepaper_Final.pdf

Adverse Media Coverage:

7. Neal Haggerty, OCC offers road map for banks to bypass 'Madden' ruling, AMERICAN BANKER (Nov. 18, 2019). https://www.americanbanker.com/news/occ-offers-roadmap-for-banks-to-bypass-madden-ruling
8. Evan Weinberger, Rate Fix for National Bank Loans Would Hurt Consumers, N.Y. Says, BLOOMBERG LAW (Dec. 19, 2019). https://news.bloomberglaw.com/banking-law/rate-fix-for-national-bank-loans-would-hurt-consumers-n-y-says
9. Pratin Vallabhaneni, Max Bonici, John Wagner & Margaux Curie, Bank Regulators' Proposals Won't Erase Madden Uncertainty, LAW360, LEXIS/NEXIS (Dec. 4, 2019). https://www.law360.com/articles/1224855/bank-regulators-proposals-won-t-erase-madden-uncertainty
10. David Dayen, Trump's Bank Regulators Open the Door to More Predatory Lending, THE AMERICAN PROSPECT (Nov. 19, 2019). https://prospect.org/power/trump%E2%80%99s-bank-regulators-open-the-door-to-more-predatory-lend/
11. Peter Conti-Brown, Can fintech increase lending? How courts are undermining financial inclusion, BROOKINGS CTR. ON REG. AND MKTS. (Apr. 16, 2019). https://www.brookings.edu/research/can-fintech-increase-lending-how-courts-are-undermining-financial-inclusion/.
12. Scott A. Cammarn, Mark Chorazak, Jonathan & Marshall G. Jones, Marketplace Lending Update #7: This and That, THE NAT'L LAW REV. (Oct. 23, 2019). https://www.natlawreview.com/article/marketplace-lending-update-7-and

HARVARD LAW SCHOOL | The Case Studies

CSP044
MAY 2020

Fintech Charters

HOWELL E. JACKSON, MARGARET E. TAHYAR, AND CAROL RODRIGUES

Memorandum

DATE:	February 6, 2020
TO:	Staffers to Senators Smith (R) and Roberts (D)
FROM:	Staff Counsel, Senate Banking Committee
RE:	Upcoming Committee Hearing on Fintech Charters

The Senate Banking Committee is holding a hearing next week to discuss the Office of the Comptroller of the Currency's "Fintech Charter." The Committee has been hearing about advances in this sector in other parts of the world, such as the United Kingdom and China, and is concerned that the United States is falling behind as a global financial services leader.

In July 2018, the Office of the Comptroller of the Currency (OCC) announced that it would begin accepting applications for a special purpose national bank charter, commonly known as the Fintech Charter. The OCC is the first prudential banking regulator to offer a pathway for non-banking firms to enter the banking system. The Fintech Charter is a national bank charter that is available to qualifying companies engaged in a limited range of banking activities, specifically providing payment services and/or lending money, but not taking deposits. Like traditionally-chartered national banks, companies that apply and receive a Fintech Charter would be subject to the statutes, regulations, guidance and federal supervision that apply to all national banks, with some exceptions and tailoring based on the company's business model. There have not yet been any applications for a Fintech Charter, 1 which is likely because of the uncertainty caused by pending litigation.

Since the OCC released its initial proposal for a Fintech Charter in December 2016, certain stakeholders have voiced significant opposition. The New York Department of Financial Services and the

[1] As of December 5, 2019.

Written by Carol Rodrigues, with assistance from Howell E. Jackson, James S. Reid Jr., Professor of Law at Harvard Law School and Margaret E. Tahyar of Davis Polk & Wardwell. Case development at Harvard Law School is partially funded by a grant from Dechert LLP. Cases are developed solely as the basis for class discussion. They are not intended to serve as endorsements, sources of primary data, legal advice, or illustrations of effective or ineffective management.

Copyright © 2020 President and Fellows of Harvard University. No part of this publication may be reproduced, stored in a retrieval system, used in a spreadsheet, or transmitted in any form or by any means—electronic, mechanical, photocopying, recording, or otherwise—without permission. To order copies or permissions to reproduce materials please visit our website at casestudies.law.harvard.edu or contact us by phone at 617-496-1316, by mail at Harvard Law School Case Studies Program, 1545 Massachusetts Avenue – Areeda 507, Cambridge, MA 02138, or by email at HLSCaseStudies@law.harvard.edu.

Conference of State Bank Supervisors have each sued the OCC to stop it from issuing Fintech Charters, arguing that the OCC lacks statutory authority to charter special-purpose national banks that do not accept deposits. In October 2019, the District Court for the Southern District of New York ruled in favor of the New York Department of Financial Services and held that the National Bank Act "unambiguously requires that, absent a statutory provision to the contrary, only depository institutions are eligible to receive national bank charters from [the] OCC."[2] The OCC appealed the decision to the U.S. Court of Appeals for the Second Circuit in 2020.[3] The District Court for the District of Columbia dismissed the lawsuit brought by the Conference of State Bank Supervisors in September 2019 for a lack of standing because the OCC has not yet granted a Fintech Charter.[4] This litigation seems likely to drag on for years, and the resulting uncertainty has clearly dampened investor enthusiasm for the Fintech Charter.

There is also uncertainty about the Federal Reserve's response to the Fintech Charter. National banks are required to be members of the Federal Reserve System,[5] but the Federal Reserve has refused, for almost four years, to clarify whether companies that receive an OCC Fintech bank charter will be given a Master Account at a Federal Reserve Bank, which grants direct access to the Federal Reserve's payment system.[6] As discussed in further detail in the background materials, access to the Federal Reserve's payment system will be crucial for certain business models so as to realize the full potential of a national charter.

The recent developments in the litigation against the OCC have increased pressure on Congress to act. Former Comptroller Thomas Curry, for example, has called on Congress to "consider a bipartisan legislative solution that builds on the home-and-host state framework established under [the law governing interstate banking]" because "we cannot wait one, two or more years for the federal courts to decide whether the OCC [Fintech Charter] is a means to offer a national option for Fintechs, while other countries develop competing and streamlined regulatory frameworks that are conducive to innovation."[7]

The Senate Banking Committee is considering legislation that would make abundantly clear that the OCC has the authority to issue a special purpose national bank charter for new entrants and clarify that entities that receive such a charter would be eligible for membership in the Federal Reserve System. The Committee would like to limit the legislation to these two issues and is not intending to change any other feature of the OCC's Fintech Charter. The Chairman of the Senate Banking Committee has signaled support for the bill. If passed, the Committee's goal would be to moot the ongoing litigation about the OCC's authority and reduce uncertainty in the sector. The upcoming hearing aims to assist the Committee in deciding whether it wants to introduce this bill.

[2] *Lacewell v. Off. of the Comp. of the Currency*, No. 18 Civ. 8377, 2019 U.S. Dist. LEXIS 182934, at *4 (S.D.N.Y. Oct. 21, 2019).

[3] For arguments in support of the OCC's appeal, *see Brief of David Zaring, Lacewell v. Off. of the Comp. of the Currency*, No. 19-4271 (Apr. 30, 2020).

[4] *Conf. of State Bank Supervisors v. Off. of the Comp. of the Currency*, No. 18-cv-24492019, U.S. Dist. LEXIS 149531 (D.D.C. Sep. 3, 2019).

[5] 12 U.S.C. § 282.

[6] Rachel Witkowski, *Fed Will Have the Say on Key Parts of OCC's Fintech Charter*, AM. BANKER (Sep. 18, 2018), https://www.americanbanker.com/news/fed-will-have-the-say-on-key-parts-of-occs-Fintech-charter. There is currently an open question regarding the Federal Reserve's discretion, or lack thereof, to grant direct access to the payments system for chartered depository institutions. *See* Michael S. Derby, *Bank Sues New York Fed Over Lack of Account*, WALL ST. J (Sep. 5, 2018), https://www.wsj.com/articles/bank-sues-new-york-fed-over-lack-of-account-1536185523.

[7] Thomas Curry, *Congress Can Work Around Court's Nixing of OCC Fintech Charter*, AM. BANKER (Nov. 18, 2019), https://www.americanbanker.com/opinion/congress-can-work-around-courts-nixing-of-occ-Fintech-charter.

In preparation for the hearing, the Senators would like you to brief them on the policy and political considerations surrounding the Fintech Charter. As you know, the Senators are new to the Committee, and Senator Smith (R) is up for re-election in 2020. In the interest of time, the Senators are requesting to be briefed together. A staff member from the Federal Reserve and a representative from the New York Department of Financial Services will also be briefing the Senators on their respective points of view. You need not concern yourself with legal questions surrounding the OCC's authority to grant such a charter, which would be resolved with the passage of the legislation. Instead, the Senators want to know whether they should take a position on the legislation and, if so, whether they should support or oppose it.

If the legislation passes, companies are much more likely to proceed with an application for a special-purpose national bank charter knowing that much of the legal uncertainty has been resolved. As discussed in further detail below, the Fintech Charter could be extremely valuable to various business models that would now be more inclined to become a chartered national bank.

This memorandum offers additional background on the Fintech Charter and related issues. Also included are a number of appendices with additional items that may be helpful in your analysis. The specific questions to be addressed are listed at the end of the memorandum.

What is the OCC's Fintech Charter?

The leading textbook on Financial Regulation describes the traditional bank charter as follows:

A bank needs a charter issued by a government authority before it can start taking deposits and making loans. The chartering process for a bank and a corporation are radically different. Anyone with access to the Internet and a credit card can fill out a few forms to incorporate a general-purpose corporation and begin business almost overnight. No state authority with discretionary authority to grant or deny the charter examines the moral character, the qualifications and experience of the investors, or whether the community needs the product offered by the new company. On the contrary, it is considered a virtue of the American capitalist system that two guys in a dorm room or a garage with no experience and an idea about a novel product can start a company.

The process could not be more different for those seeking to charter a new bank and there is no guarantee that the application will be approved. The Federal Reserve Board's website describes the process:

"Starting a bank involves a long organization process that could take a year or more and permission from at least two regulatory authorities. Extensive information about the organizer(s), the business plan, senior management team, finances, capital adequacy, risk management infrastructure, and other relevant factors must be provided to the appropriate authorities."[8,9]

Many Fintech companies that started out as two guys in a garage have now come face-to-face with the bank chartering process and are grappling with the costs and benefits of a bank charter, which vary based on the chartering institution involved. Bank organizers—people wishing to start a bank—have a choice of chartering agencies.

[8] *See How Can I Start a Bank?*, FED. RESERVE (last updated Aug. 2, 2013).

[9] Barr, Jackson & Tahyar, Financial Regulation: Law and Policy 165 (2nd ed. 2018).

The United States has a dual banking system, which means that banks can be chartered either at the state level by a state banking regulator, or at the federal level by the OCC. The choice of chartering institution is also a choice of the primary regulator. State-chartered banks are regulated primarily by state banking authorities and secondarily by the Federal Deposit Insurance Corporation (FDIC), while national banks are regulated primarily by the OCC. Institutions that are successfully approved for the OCC's Fintech Charter would be regulated primarily by the OCC.

The OCC's Fintech Charter began as a white paper titled *Supporting Responsible Innovation in the Federal Banking System* released in March 2016. After months of innovation initiatives, the OCC proposed a special purpose national bank charter in December 2016. Under that proposal, charter holders would be required to engage in at least one of the three core banking functions—receiving deposits, paying checks[10] or making loans. Following the end of the comment period on the proposed charter in January 2017, the final policy narrowed the scope of the charter to exclude deposit-taking institutions, thus removing the need for FDIC insurance. Excluding deposit-taking institutions also meant that a firm with a Fintech Charter would fall outside the definition of a "bank" under the Bank Holding Company Act (BHCA) and could be owned by a company that is also engaged in commercial or nonfinancial ventures. The BHCA, among other things, imposes significant restrictions on the types of activities that entities that control, are controlled by or share common control with a bank can engage in and subjects them to supervision by the Federal Reserve.

Applying the BHCA to Fintech companies could mean that if Amazon opens a traditional deposit-taking bank, for example, all of Amazon's activities, including those that have nothing to do with banking, such as Prime grocery services and Prime media content, would become subject to the activities restrictions of the BHCA and fall within the supervision of the Federal Reserve.

An alternative to a Fintech Charter might be an Industrial Loan Company (ILC) charter, which is issued in certain states, most commonly Utah. ILCs with assets over $100 million may accept certain forms of deposits and therefore must obtain FDIC insurance. ILCs are also exempt from the definition of a "bank" under the BHCA. In recent years, there have been attempts to block the use of the ILC charter, as described in the Financial Regulation textbook, as follows:

The popularity of the ILC charter began to dim in 2006 when the FDIC imposed a moratorium on deposit insurance for new ILCs. The moratorium was spurred by Walmart's attempt to form a Utah-chartered ILC, which generated widespread opposition from community bankers, the Federal Reserve Board, labor unions, retail stores and members of Congress. The primary activity of Walmart's proposed ILC was to "act as a sponsor for the processing and settlement of credit card payments, debit card payments, and check payments made by customers at Walmart stores."[11] The public outcry that resulted was unprecedented, especially considering that Target had been previously granted an ILC charter. In addition to the moratorium, many non-bank financial ILCs failed or were converted to bank holding companies during the Financial Crisis. As a result, by early 2017, only 25 ILCs remained, controlling a total of $152.4 billion in assets.

[10] The OCC considers issuing debit cards or engaging in other means of facilitating payments electronically the modern equivalent of paying checks. *See* Office of the Comptroller of the Currency, *Exploring Special Purpose National Bank Charters for Fintech Companies* 4 (Dec. 2016), https://www.occ.gov/topics/responsible-innovation/comments/special-purpose-national-bank-charters-for-Fintech.pdf.

[11] Arthur E. Wilmarth, Jr., *Wal-Mart and the Separation of Banking and Commerce*, 39 CONN. L. REV. 1539, 1541–42, 1544 (2007).

Nonetheless, the ILC charter still exists, together with its extremely valuable exception from the BHCA. Attempts to eradicate the charter as part of the 2010 Dodd-Frank Act failed. Congress instead imposed a three-year moratorium on the granting of any new FDIC insurance for ILCs, essentially preventing any new charters. The FDIC moratorium expired on July 21, 2013, and no new charters have been granted since 2009. The FDIC's informal moratorium on granting deposit insurance to new ILC charters has ended, with both FDIC staff and the Chairman Jelena McWilliams making statements that the FDIC will now consider such applications.[12]

As a state-chartered, FDIC-insured institution, an ILC provides many of the benefits of a national bank, as described in Section II, including preemption of state licensing and usury laws and access to the Federal Reserve's payments system. The existence of the ILC charter as a potential alternative to the OCC's Fintech Charter may diminish the urgency to resolve the lingering uncertainties around the OCC's Fintech Charter. In 2020, the FDIC granted deposit insurance to two proposed ILCs, Nelnet Bank and Square Financial Services, Inc., both Fintechs. These were the first such approvals by the FDIC since before the Financial Crisis, however.

Why Would a New Entrant Want a Fintech Charter from the OCC?

While a bank charter comes with a host of regulatory responsibilities—including frequent examination and reporting requirements as well as minimum capital requirements—it also provides a suite of benefits to institutions that want to engage in certain business lines. Because the OCC's Fintech Charter does not permit deposit-taking, the benefits of the charter will mainly accrue to institutions that engage in the business of "paying checks" or "lending money." The OCC has taken a broad interpretation of what it considers the business of "paying checks" or "lending money." The OCC's 2016 Charter Proposal stated, "discounting notes, purchasing bank-permissible debt securities, engaging in lease-financing transactions, and making loans are forms of lending money. Similarly, issuing debit cards or engaging in other means of facilitating payments electronically are the modern equivalent of paying checks."[13]

For non-bank institutions engaged in lending money, the key benefits of a national bank charter are the preemption of state usury laws, which limit how much lenders can charge in interest. National banks engaged in lending activities—a core banking function—are entitled to federal preemption of state usury laws so that a national bank is permitted to export the maximum interest rate allowed in the state where the bank is located and make loans in other states without regard to the usury laws of those states.[14] The power to use one state's interest and usury provisions for interstate lending activities are commonly referred to as the Exportation Doctrine. Most national banks engaged in nationwide lending choose a state with no or very liberal usury limits as the locus for such activities.

A firm receiving a special purpose charter, accordingly, would be similarly entitled to take advantage of the Exportation Doctrine. Since many state laws provide that a usurious loan is void, the benefits of the Exportation Doctrine are very important. Without such benefits, stand-alone nonbank

[12] Barr, Jackson & Tahyar, *supra* note 8, at 178.

[13] Office of the Comptroller of the Currency, *Exploring Special Purpose National Bank Charters for Fintech Companies* 4 (Dec. 2016), https://www.occ.gov/topics/responsible-innovation/comments/special-purpose-national-bank-charters-for-Fintech.pdf.

[14] 12 U.S.C. § 85; 12 C.F.R. §§ 7.4001, 7.4008.

lenders must comply with the usury laws in each state in which they provide loans to avoid such loans being deemed void under state law. This consequence has been especially concerning in light of the uncertainty of the bank partnership, or "rent-a-charter," model raised by recent court decisions such as *CashCall* and *Madden*.[15,16]

The key benefits of a national bank charter for institutions engaged in the business of facilitating payments are the ability to preempt state money transmitter license laws and the ability to directly access the Federal Reserve's payment system.[17] These benefits were explained in a Davis Polk & Wardwell LLP memorandum as follows:

National banks are entitled to federal preemption of state laws and regulations, including licensing requirements, when they conflict with a national bank's power to engage in a broad range of payment services.[18] National banks are able to avoid state-level money transmitter licensing requirements and, in turn, the expensive and time-consuming state-by-state money transmitter licensing process, in order to engage in such activities.[19]

Currently, virtually every state has some form of licensing requirement for businesses engaged in the transmission of money.[20] These laws, while certainly covering traditional money transmitters such as Western Union and MoneyGram, may also catch nonbank firms engaged in payment services — including online, mobile payment and virtual currency providers — subjecting them to an array of regulatory and compliance issues. The scope of activities considered to be money transmission varies by state,[21] Nonbank firms with multistate operations must comply with varying standards and complex licensing and registration requirements that typically include financial requirements, audits, bonding, investment limitations, and the like.

[15] Davis Polk & Wardwell LLP, *Beyond Fintech: The OCC's Special Purpose National Bank Charter* 3 (Dec. 9, 2016), https://www.davispolk.com/files/2016-12-9_occs_special_purpose_national_bank_charter.pdf.

[16] *See CashCall v. Morrisey*, No. 12-1274 (W. Va. 2014); *Madden v. Midland Funding, LLC*, 786 F.3d 246 (2d Cir. 2015). Under the "rent-a-charter" model, a marketplace lender typically enters into a contractual arrangement with an existing chartered bank pursuant to which the bank initially funds the loan but the marketplace lender purchases the loan from the bank at the time of or shortly after origination. The marketplace lender may also assume loan servicing, collection and other administrative functions of the original funding bank. Both *CashCall* and *Madden* called into question the viability of the rent-a-charter model by holding that the original funding bank must retain a predominant economic interest in the loan in order for preemption of state usury law to apply to the nonbank lender. While cases in other states have upheld the rent-a-charter model, the differences across jurisdictions and resulting regulatory uncertainty create new operational challenges for marketplace lenders. *See, e.g.*, *Sawyer v. Bill Me Later*, Inc., 23 F. Supp.3d 1359 (D. Utah 2014). The proper use of the special purpose charter and the ongoing involvement of a firm with a special purpose charter in owning and servicing the loans generated should resolve the true lender issues highlighted in *CashCall* and *Madden*.

[17] Because this case study has been developed for use in a classroom setting that will have already discussed marketplace lending and preemption, consideration of lending-focused Fintechs is being kept to a minimum to allow focus instead on the payment applications of the OCC's Fintech Charter.

[18] *See* OCC Preemption Final Rule, 76 Fed. Reg. 43,549, 43,555 (July 21, 2011). The OCC has taken the view that payment services are permissible activities for national banks as incidental to the business of banking. See generally, Office of the Comptroller of the Currency, Activities Permissible for a National Bank, Cumulative (April 2012).

[19] State-level licensing requirements that prevent, or significantly interfere or conflict with the exercise by a national bank of its federally-granted powers, including the power to engage in payment services, are preempted in accordance with the legal standard established in Barnett Bank v. Nelson, 517 U.S. 25 (1996). See OCC Preemption Final Rule, 76 Fed. Reg. 43,549, 43,556 (July 21, 2011).

[20] *See, e.g.*, N.Y. Code, Banking 13-B; Tex. Fin. Code § 151; Ca. Fin. Code § 2000; Fla. Stat. § 560.

[21] *See, e.g.*, Md. Code Ann., Fin. Inst. § 12-401 ("Money transmission" includes the business of selling or issuing payment instruments or stored value devices, or receiving money or monetary value, for transmission to a location within or outside the United States by any means, including electronically or through the Internet, bill payer services, accelerated mortgage payment services, and any informal money transfer system engaged in as a business for, or network of persons who engage as a business in, facilitating the transfer of money outside conventional financial institutions to a location within or outside the United States.)

In contrast, firms with special-purpose charters, like full-service national banks, could avoid state-level money transmitter licensing requirements, allowing them to avoid the costly state-by-state licensing regime and potentially significantly reducing their compliance costs and complexity. Such firms would still be required to comply with federal anti-money laundering laws….[Firms] that engage in activities subject to a "state consumer financial law"[22] would generally remain subject to such laws, unless the explicit grounds for preemption under the Dodd-Frank Act were met.[23] Examples of state consumer protection laws that would generally apply include state laws on anti-discrimination and fair lending. Moreover, the OCC explicitly states in the Charter Proposal that state laws aimed at unfair or deceptive treatment of customers also apply to federally chartered banks.[24]

As national banks, firms with special-purpose charters will be required to be members of the Federal Reserve System pursuant to the Federal Reserve Act and will be subject to direct oversight as member banks by the Federal Reserve Board.[25] Member banks, and all insured depository institutions, have access to the Federal Reserve discount window and other Federal Reserve services, including the ability to create a Master Account at the Federal Reserve.

The Federal Reserve allows member banks, other depository institutions, U.S. branches of foreign banks and certain U.S. government entities to create Master Accounts with their local Federal Reserve Bank.[26] A Master Account allows a financial institution to settle transactions with other financial institutions directly on the books of the Federal Reserve. If a JPMorgan Chase customer, for example, sends money to a Bank of America customer, the two banks can exchange funds via their Master Accounts at the Federal Reserve. A Master Account provides the ability to "accept and clear customer checks drawn on other banks;…to issue checks or otherwise make payments other than in cash; and…to transfer funds to other banks."[27] Without a Master Account, a bank would be nothing more than a "network of cash vaults that would provide customers with the ability to transact business only with other customers of the bank, with no ability to transact business outside of the…bank network."[28]

Institutions that are not eligible for a Master Account, or that choose not to create one, can only access the Federal Reserve's payments system indirectly, through an intermediary relationship with a bank that does have a Master Account, called a correspondent bank. PayPal, for example, contracts with a bank for payment services. Where both the payor and recipient are PayPal customers and the funds reside in PayPal accounts, funds can be transferred easily within the private sector by transferring the

[22] "State consumer financial law" is generally defined as any state law that regulates any "financial transaction [or related] account…with respect to a consumer." See 12 U.S.C. § 25b(a)(2).

[23] 12 U.S.C. § 25(b)(1). The Dodd-Frank Act provided that state consumer financial laws are preempted only if the application of the law would have a discriminatory effect on national banks (compared to state banks), the OCC determines on a case-by-case basis that the law "prevents or significantly interferes" with the exercise by the national bank of its powers, or the state law is preempted by another federal law. *Id.*

[24] Davis Polk & Wardwell LLP, supra note 11, at 3.

[25] For the purposes of this case study, we are assuming that membership in the Federal Reserve System would be granted to firms with an OCC Fintech Charter.

[26] FED. RESERVE BANKS, OP. CIRCULAR 1: ACCOUNT RELATIONSHIPS § 2.2 (Feb. 1, 2013), https://www.frbservices.org/assets/resources/rules-regulations/020113-operating-circular-1.pdf.

[27] Level 4 Ventures, Inc. et al, State-backed Financial Institution (Public Bank) for the State of California Servicing the Cannabis Industry Feasibility Study 2018 17 (Dec. 6, 2018).

[28] *Id.*

funds from one PayPal account to another.[29] However, when money is transferred between PayPal and non-PayPal accounts, such as when a customer makes a payment that requires pulling the funds out of their checking account, clearing and settlement requires a mix of the private sector and Federal Reserve involvement. Correspondent banks, of course, charge a fee for providing clearing and settlement services. Payment-focused Fintechs that can obtain their own Master Accounts—instead of having to go through a correspondent bank—can avoid this fee.

A national bank charter would also allow an entity to avoid paying interchange fees, which are the fees charged to merchants when customers pay using a debit or credit card. Interchange fees are further described in the Financial Regulation textbook:

> Credit and debit card networks are highly concentrated. In 2017, Visa's total purchase volume accounted for 53% of the credit card market, followed by MasterCard at 22% and American Express at 21%, with Discover accounting for the remaining 4% share. When you swipe your credit or debit card at a merchant terminal, your bank (the issuer) debits your account and sends the transaction to the card network, which then forwards the transaction information to the merchant's bank (the acquirer). The acquirer then credits the merchant's account. The acquirer does not credit the merchant the full amount of the retail transaction because the issuer charges the acquirer an interchange fee, and the acquirer deducts those fees, along with the acquirer's own fees, from the amount credited to the merchant. That amount is known as the merchant discount. Interchange fees are costs to merchants and revenue to card issuers. Issuers and acquirers also pay a switch fee to the network.[30]

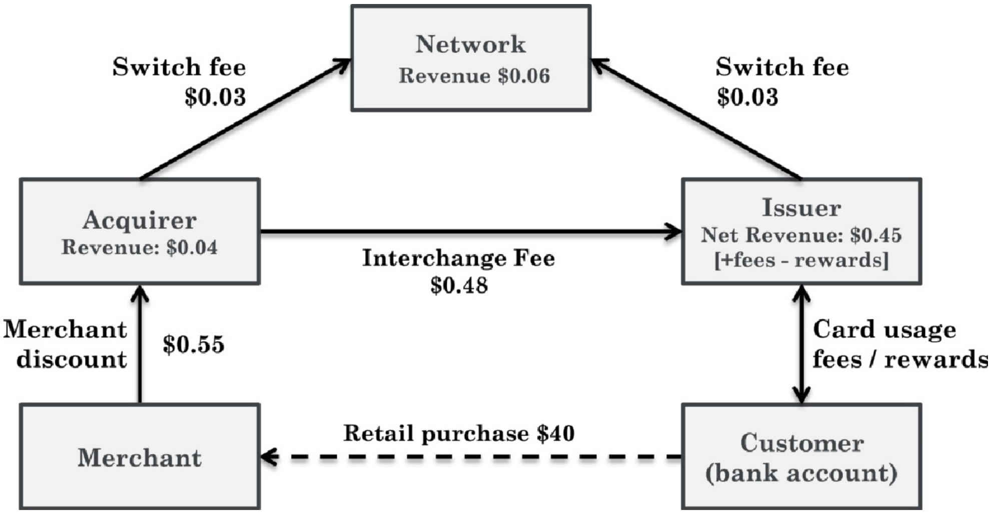


Figure 1. Overview of Interchange Fees[31]

[29] Richard J. Sullivan, *The Federal Reserve's Reduced Role in Retail Payments: Implications for Efficiency and Risk*, FED. RESERVE BANK OF KANSAS CITY 86–87 (2012), https://www.kansascityfed.org/publicat/econrev/pdf/12q3Sullivan.pdf.

[30] BARR, JACKSON & TAHYAR, *supra* note 5, at 842–43.

[31] Benjamin S. Kay et al., *Bank Profitability and Debit Card Interchange Regulation: Bank Responses to the Durbin Amendment* 7 (Divisions of Research & Statistics and Monetary Affairs, Fed. Reserve Bd. Fin. and Econ. Discussion Series No. 2014-77, 2014).

For a large retailer like Walmart or Amazon, avoiding even 55 cents per transaction can significantly boost profits when multiplied over billions of transactions. If a retailer opens a bank, it can assume the role of the acquirer—at the very least—and avoid having to pay a fee to its bank. More importantly, if it can issue its own payment products and convince customers to use them, it can avoid almost the entirety of the interchange fee, in addition to receiving issuer fees when customers use its payment products at other retailers.

In addition to preemption and payment processing benefits, companies may find that a Fintech Charter gives them options to enhance business lines or generate new streams of revenue. Institutions that have access to large amounts of consumer data could leverage consumer information to generate entirely new models of the banking relationship. Given the wealth of customer data that Amazon has, for example, it could develop unique lending algorithms that give it a competitive advantage over traditional banks who must rely on customer-provided data or credit bureau reports.

PayPal Holdings Inc. has extended more than $6 billion in small-business loans since 2013, using data collected by processing payments for internet retailers. Over the past seven years, independent merchants that sell goods on Amazon have borrowed more than $3 billion from the e-commerce giant, which approves loans based on sellers' historical volumes, Amazon reviews and other factors."[32]

A Google Bank account could integrate seamlessly into a user's Google Calendar and Gmail to create reminders when bills are due and make payments automatically. It could use predictive technologies and artificial intelligence to monitor personal budgets and send alerts when a user has spent too much on dinner with friends.

What are Some Concerns about the Fintech Charter?

When the OCC initially proposed a Fintech Charter in 2016, the comments received were mixed. Some commenters strongly supported the proposal and encouraged the OCC to provide further flexibility under the charter framework to ensure that certain types of new payment services would be within the scope of the Charter and that the regulatory requirements applicable to firms with a Fintech Charter, such as capital and liquidity standards, would be commensurate with the nature and size of an institution's business. Comment letters in this category were largely submitted by Fintech firms and trade associations representing Fintechs or other non-bank institutions.[33]

Commenters representing a mix of existing banking organizations, such as Fintech firms and consumer advocacy organizations, supported the special purpose charter so long as companies with a Fintech Charter were subject to the same rules and requirements that applied to all national banks.[34]

Many commenters opposed the OCC's proposal based on their view that the Charter would create an uneven playing field between insured banks and uninsured special purpose national banks, harm consumers, and/or that the OCC lacked the legal authority to authorize the special purpose charter. This

[32] Peter Rudegeair, *A $150,000 Small Business Loan—From an App*, WALL ST. J (Dec. 28, 2018), https://www.wsj.com/articles/a-150-000-small-business-loanfrom-an-app-11546002022.

[33] *See, e.g.*, Lending Club, *Comment Letter on OCC White Paper on Exploring Special Purpose National Bank Charters for Fintech Companies* (Jan. 17, 2017), https://www.occ.gov/topics/responsible-innovation/comments/comment-lending-club.pdf.

[34] *See, e.g.*, The Clearing House et al., *Comment Letter on OCC White Paper on Exploring Special Purpose National Bank Charters for Fintech Companies* (Jan. 17, 2017), https://www.occ.gov/topics/responsible-innovation/comments/comment-clearing-house-et-al.pdf.

opposition mainly came from state regulators and attorneys general, consumer advocacy organizations, banking organizations and trade associations representing those groups.[35]

Commenters opposing the proposal expressed concern that the special purpose charter would enable non-depository institutions to enjoy the benefits of a national bank charter without being subject to the same requirements as deposit-taking institutions. Although the OCC stated in its charter framework that obligations similar to those imposed under the Community Reinvestment Act, and federal and state consumer protection laws would still apply to firms with a Fintech Charter, several commenters argued that the special purpose charter would allow Fintech companies to evade financial inclusion obligations and consumer protection requirements.[36] Moreover, a few commenters believed that the ability of a special purpose charter holder to operate outside the scope of the BHCA, thus enabling the holder to mix banking and commerce, is contrary to the policies embedded in the BHCA and the National Bank Act.

Commenters also criticized the special purpose charter as a potential avenue for firms with a Fintech Charter to avoid having to comply with federal and state consumer protection laws. For example, the Conference of State Bank Supervisors (CSBS) argued that firms with a Fintech Charter would not be subject to the same scope of federal consumer financial laws as insured depository institutions given the more limited supervision the CFPB has over non-depository institutions. Consumer advocacy organizations and state attorneys general also emphasized that the special purpose charter would allow institutions to preempt state and local consumer protection laws. In the CSBS's lawsuit against the OCC over the Fintech Charter, the CSBS states:

[S]tate laws, which face a clear threat of preemption under the OCC's unauthorized nonbank charter plan, provide vital protections to the economies, communities and citizens of every state. As recent history has shown, however, broad preemption of state law with respect to nationally chartered banks is not good public policy. State government officials have unique expertise in the banking practices and market conditions in their communities, which makes them uniquely situated to recognize and act upon consumer financial protection issues. Due to their proximity to the consumers and the communities they are charged with protecting, state regulators are also uniquely locally accountable relative to centralized federal agencies."[37]

How are Other Countries Approaching Fintech?

The nature of the U.S. dual-banking system has led to a fragmented and patchwork response to emerging trends like Fintech. Other countries have responded to new business models in the financial sector in vastly different ways. "International and US regulators approach emerging business practices, products, and services in three distinct but complementary ways: creating outreach programs to bring together regulators and market participants to clarify how innovation fits into the existing regulatory

[35] *See, e.g.*, Nat'l Cons. Law Ctr., *Comment Letter on OCC White Paper on Exploring Special Purpose National Bank Charters for Fintech Companies* (Jan. 17, 2017), https://www.occ.gov/topics/responsible-innovation/comments/comment-nclc-et-al.pdf.

[36] *Id.*

[37] Complaint at 7, Conf. of State Bank Supervisors v. Off. of Comp. of Currency, 313 F. Supp. 3d 285 (D.D.C. 2018).

framework; changing the regulatory framework to encompass new products, practices, and providers; or suspending regulatory barriers to encourage innovation."[38]

The United Kingdom is one example of a country that has applied the outreach model to Fintech. The UK Financial Conduct Authority (FCA) "issued a call for input on the development of a financial innovation hub, which included communication with stakeholders as a specific agency objective."[39] "In October 2014, the FCA launched Project Innovate and the Innovation Hub to foster competition and growth in financial services by helping firms with new products understand and navigate the regulatory framework and apply for a business license….The project has also created "regulatory surgery" sessions to allow firms time to address specific regulatory issues, questions, or concerns."[40]

The UK also embraced a "sandbox" model, which allows "companies to experiment with products in a modified regulatory framework, either in a controlled testing environment or through regulatory relief whereby agencies suspend certain regulations for novel business practices. This allows regulators to observe a product's effect on consumers and engage with new market participants regarding products that do not fit neatly into the existing regulatory structure."[41] This regulatory approach appears to be paying off in some ways, for example, in the first eight months of 2019, London had attracted $2.1 billion in fundraising deals in 2019, $200 million ahead of New York in total deal value.[42]

China, by contrast, took a completely different approach to financial technology and has, likewise, seen a booming Fintech sector. As of early 2018, out of 27 Fintech startups with valuations exceeding $1 billion, nine are Chinese.[43] "In 2016, Chinese consumers spent approximately $22.8 trillion (RMB 157.55 trillion) through mobile payment platforms, far exceeding the volume of transactions in the United States ($112 billion). Over 90 percent of that sum stemmed from mobile payment apps that belong to China's two biggest tech conglomerates: Alibaba's Alipay (54 percent) and Tencent's TenPay (37 percent)."[44] Much of this growth has been attributed to a combination of: "(1) high national Internet and mobile penetration, (2) a large e-commerce system with domestic Internet companies focused on payments, (3) relatively unsophisticated incumbent consumer banking, and (4) accommodative regulations."[45]

The Chinese regulators took a relatively arms-length approach to Fintech, allowing the tremendous scale we see now.[46] "Under a relatively lax regulatory environment over the past decade, a number of nonfinancial Chinese firms have waded into multiple financial sectors and achieved breakneck

[38] Pew Trusts, *How Can Regulators Promote Financial Innovation While Also Protecting Consumers?* (Aug. 2, 2018), https://www.pewtrusts.org/research-and-analysis/reports/2018/08/02/how-can-regulators-promote-financial-innovation-while-also-protecting-consumers.

[39] *Id.*

[40] *Id.*

[41] *Id.*

[42] Ryan Browne, *London Just Overtook New York for Fintech Investment, Research Shows,* CNBC (Sep. 22, 2019), https://www.cnbc.com/2019/09/22/london-just-overtook-new-york-for-Fintech-investment-research-shows.html.

[43] Wei Wang & David Dollar, *What's Happening With China's Fintech Industry?*, BROOKINGS (Feb. 8, 2018), https://www.brookings.edu/blog/order-from-chaos/2018/02/08/whats-happening-with-chinas-Fintech-industry/.

[44] *Id.*

[45] Citi GPS: Global Perspectives and Solutions, *Digital Disruption: How Fintech is Forcing Banking to a Tipping Point* 9 (Mar. 2016), https://ir.citi.com/D%2F5GCKN6uoSvhbvCmUDS05SYsRaDvAykPjb5subGr7f1JMe8w2oX1bqpFm6RdjSRSpGzSaXhyXY%3D.

[46] EY, *UK Fintech: On the Cutting Edge* 16, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/502995/UK_Fintech_-_On_the_cutting_edge_-_Full_Report.pdf.

expansion because they were not subject to rules applied to traditional institutions like banks."[47] While this has started to change, China's regulations remain "relatively less onerous" than those in markets such as Singapore and the UK.[48]

Your Assignment from the Senators

Your briefing is intended to help the Senators decide whether or not to support the proposed bill. Staff from the Federal Reserve will be presenting the views of the Federal Reserve, and whether the Federal Reserve would support the proposed bill. Staff from the New York Department of Financial Services (DFS) present the views of the DFS.

The Senators have allocated 15 minutes each for the Federal Reserve and the DFS. You, as Senate staffers, have been allocated a combined 45 minutes. You can present together or separately, as you wish. You should coordinate between yourselves and with the representatives from the Federal Reserve and the DFS on which topics you wish to present, and in what order. As you know, the Senators' time is extremely limited, and they expect you to be succinct but thorough.

The Senators expect you, as Senate staffers, to brief them on the following issues and, in particular, to be prepared to brief on the political dimensions of the below issues for each party:

Competition. The Senators would like to know the potential impact of the OCC Fintech Charter on competition in the financial sector. Community banks are vocal constituents in their states, as are large banks. Google, Amazon and other large tech companies are also, of course, influential. Keep in mind that competition from new entrants may not be equally felt across the banking sector and community banks and large banks may face different challenges and opportunities in responding to competition from new entrants. How will various constituents think about the Fintech Charter? How should the Senators craft their positions on the legislation given the competing interests of stakeholders, both within the banking sector and between the banking and technology sectors?

Innovation for consumers. Fintechs promise a greatly enhanced banking experience for consumers. How would granting a federal charter to Fintech firms impact consumers? What is the potential impact on the speed of innovation? What is the potential for the Fintech Charter to increase access to financial services for the unbanked and underbanked?

Global competition. The United Kingdom and China are two examples of different models of regulatory engagement around Fintech, and the United States risks falling behind in the global race for Fintech investment. What light can the differing experiences of the UK and China shed on the approach the US regulators should take towards Fintech domestically?

Consumer protection and the CRA. As discussed, some of the critics of the OCC's Fintech Charter are concerned that the charter will be used to evade state consumer-protection laws that may be more stringent than Federal laws. Some have suggested that the DFS and the CSBS are more concerned with protecting their licensing fees and revenues than in consumer protection. Is there any validity to this

[47] Stella Yifan Xie & Chao Deng, *China to Tighten Rules on Five Financial Giants*, WALL ST. J. (Nov. 3, 2018), https://www.wsj.com/articles/china-to-tighten-rules-on-five-financial-giants-1541246489.

[48] DBS & EY, *The Rise of Fintech in China* 27 (Nov. 2016), https://www.ey.com/Publication/vwLUAssets/ey-the-rise-of-Fintech-in-china/$FILE/ey-the-rise-of-Fintech-in-china.pdf.

point of view? How should the Senators approach this issue and how should they balance these concerns against the potential for consumer benefits? Further, because an entity with a Fintech Charter would not take deposits, it would not be subject to the Community Reinvestment Act (CRA) which requires deposit-taking institutions to make investments in low- and moderate-income communities. The CRA, however, has not been significantly reformed since 1977 and is based on a geographic catchment model that links loans to the geographic area in which deposits are gathered. There is an ongoing and highly controversial effort to reform the CRA.[49] How should the Senators deal with these concerns?

Size and concentration concerns. Some Senators are concerned about the concentration of economic power in a few companies. If Amazon, Facebook or Google obtains a bank charter, are there concerns with a single company having such a large footprint in both commerce and banking? Are there systemic risk concerns? On the other hand, could broadening the financial sector to include non-traditional banks reduce systemic risk?

Political and electoral concerns. Aside from the policy points above which, of course, have political implications, each Senator has specific political concerns related to fundraising and the nature of their state's constituency. What might these be? How should they impact private discussions the Senators have with the committee chairman and other Senators? How should they impact any public statements the Senators make at the hearing? How, if at all, should the Senators' private and public postures differ?

The Senators expect staff from the Federal Reserve to describe why the Federal Reserve has not been able to determine, after four years, whether and under what conditions it would permit a financial institution with a Fintech Charter to obtain a Master Account. What are the advantages and disadvantages of allowing access to a Master Account from the perspective of the Federal Reserve? Why is the Federal Reserve unable to clarify its view on this issue?

The Senators expect staff from the DFS to lay out in full the concerns of the DFS and the Conference of State Banking Supervisors against the Fintech Charter. Since the bill being considered would resolve the uncertainty surrounding the OCC's authority to issue the Fintech Charter, their briefing is expected to focus on why they are against the concept of the Fintech Charter and not on the OCC's authority to issue one.

[49] *See* Rachel Witkowski, *Cheat Sheet: 5 Pressure Points in CRA Reform Debate*, AM. BANKER (Aug. 30, 2018), https://www.americanbanker.com/list/cheat-sheet-5-pressure-points-in-cra-reform-debate.

Appendices

1. Office of the Comptroller of the Currency, *OCC Begins Accepting National Bank Charter Applications from Financial Technology Companies*, Press Release (July 31, 2018). https://www.occ.gov/news-issuances/news-releases/2018/nr-occ-2018-74.html
2. Lacewell v. Office of the Comptroller of the Currency, No. 18 Civ. 8377, 2019 U.S. Dist. LEXIS 182934, at *4 (S.D.N.Y. Oct. 21, 2019). https://www.law360.com/dockets/download/5db0b9ef3afb12094ab4183f?doc_url=https%3A%2F%2Fecf.nysd.uscourts.gov%2Fdoc1%2F127125725167&label=Case+Filing
3. Statement, Linda A. Lacewell, Statement on Court Ruling on OCC's Fintech Charter (Oct. 22, 2019). https://www.dfs.ny.gov/reports_and_publications/statements_comments/2019/st1910221
4. Office of the Comptroller of the Currency, *Policy Statement on Financial Technology Companies' Eligibility to Apply for National Bank Charters* (July 31, 2018). https://www.occ.gov/news-issuances/news-releases/2018/pub-other-occ-policy-statement-Fintech.pdf
5. Emily Glazer, Laura Stevens & AnnaMaria Andriotis, *Jeff Bezos and Jamie Dimon: Best of Frenemies*, WALL ST. J (Jan 5, 2019). https://www.wsj.com/articles/jeff-bezos-and-jamie-dimon-best-of-frenemies-11546664451?
6. Todd H. Baker, *How Regulators Besides the OCC Can Help Fintechs*, AM. BANKER (Dec. 17, 2018). https://www.americanbanker.com/opinion/how-regulators-besides-the-occ-can-help-Fintechs
7. Thomas Curry, *Congress Can Work Around Court's Nixing of OCC Fintech Charter*, AM. BANKER (Nov. 18, 2019). https://www.americanbanker.com/opinion/congress-can-work-around-courts-nixing-of-occ-Fintech-charter

PART II

CAPITAL MARKETS

HARVARD LAW SCHOOL | The Case Studies

CSP046
APRIL 2020

Robo-Advising

RYAN CHAN-WEI

Memorandum

DATE: February 1, 2019

TO: Jay Cleighton, Chair, Securities and Exchange Commission
Robert W. Coke, President and CEO, Financial Industry Regulatory Authority

FROM: Office of Craig Fillups, Counsel, Department of the Treasury

RE: Concept Paper on a Maximally Digital Robo-adviser—iRobo, Inc.

Now that the shutdown is behind us, Craig Fillups has asked me to reach out to the two of you about a potentially promising new initiative in the FinTech space.

As we have discussed on numerous occasions, the Trump Administration is committed to improving the financial well-being of all Americans by supporting responsible innovation in financial services. Over the past few months, we have been approached by dozens of FinTech entrepreneurs with new and exciting value propositions.

As a pilot program, Craig Fillups has decided to vet a handful of these proposals with the leadership of key regulatory agencies. To that end, I am sending along materials regarding a proposal to set up a "maximally digital" robo-advisory firm (iRobo, Inc.). Mr. Fillups received the proposal last week, and we're forwarding this package in the hopes of beginning a high-level conversation regarding the desirability and viability of this approach. To the extent that your schedule permits, we were hoping to set up a preliminary meeting on the topic next week on Thursday afternoon. We envision the conversation as being entirely informational with the understanding that this proposal would remain subject to otherwise applicable legal processes.

As you will see, the iRobo team contemplates an advisory platform with a markedly reduced level of human involvement—it will only have one human employee. The advisory process itself will be fully automated, with a view to keeping costs as low as possible and increasing access to capital market

Written by Ryan Chan-Wei under the supervision of Howell E. Jackson, James S. Reid, Jr. Professor of Law at Harvard Law School. Case development at Harvard Law School is partially funded by a grant from Dechert LLP. Cases are developed solely as the basis for class discussion. They are not intended to serve as endorsements, sources of primary data, legal advice, or illustrations of effective or ineffective management.

Copyright © 2020 President and Fellows of Harvard University. No part of this publication may be reproduced, stored in a retrieval system, used in a spreadsheet, or transmitted in any form or by any means—electronic, mechanical, photocopying, recording, or otherwise—without permission. To order copies or permissions to reproduce materials please visit our website at casestudies.law.harvard.edu or contact us by phone at 617-496-1316, by mail at Harvard Law School Case Studies Program, 1545 Massachusetts Avenue – Areeda 507, Cambridge, MA 02138, or by email at HLSCaseStudies@law.harvard.edu.

investments. More details can be found in the letter and supporting documents, which are appended to this memorandum.

At our meeting next week, we hope to take up two questions:

1. Whether a proposal of this sort is desirable as a matter of public policy; and
2. The extent to which it could be implemented under current laws and regulations.

At the same time, we will be having a Treasury Department team consider whether the iRobo proposal is consistent with the Department's own recommendations in its July 2018 FinTech Report.

Finally, Regulation Best Interest (BI) need not be considered at this stage, as this rulemaking is still pending as of early 2019.

Thank you.

Letter of Transmittal: Time-dated 21 January 2019; 14:32:45

i-Robo, Inc.

DATE: February 2019

TO: Office of Craig Fillups, Department of the Treasury

FROM: Ernie D'Amato

RE: Proposal of a Maximally Digital Robo-Adviser— iRobo, Inc.

I obtained your address from one of my professors and he encouraged me to get in touch. I am a recent MBA graduate of the Harvard Business School, and I am writing to enlist the support of the Department of the Treasury for iRobo, Inc., a robo-advisory firm that I am planning to set up.

iRobo would be the first maximally-digital robo-adviser and I will be the only human employee. All financial transactions will be executed using computer algorithms. Outside contractors will be hired only when necessary to handle compliance with anti-money laundering requirements and other compliance matters. Additionally, we are still in the process of deciding on iRobo's revenue model, but we are cognizant of the respective challenges posed by both a transaction fees model and an AUM-based (assets under management) fee model.

This idea was conceived as part of a business school class, "FinTech Innovation," and I am writing to you now because I hope to secure the backing of the Department of the Treasury as we attempt to obtain regulatory approval.

My colleagues and I are still exploring how best to structure the business, but a possible model is for iRobo to be a dual registrant, meaning that it would function as both an SEC-registered broker-dealer and a registered investment adviser under applicable state and federal laws. This means that iRobo would have to comply with both the suitability and fiduciary standards incumbent on dual registrants.

Alternatively, as is the case with the vast majority of robo-advisers, iRobo may function only as a registered investment adviser (albeit with broker-dealer transactional support in the background). This would mean that iRobo is only required to comply with the fiduciary standard incumbent on registered investment advisers. This might be an appropriate model because states have no jurisdiction over a registered investment adviser with more than $100 million in assets under management, and we expect iRobo to far exceed that sum. By contrast, state regulators continue to have oversight of broker-dealers regardless of their amount of assets under management, and it may be an unnecessary regulatory burden for iRobo to subject itself to both state and federal oversight.

Regardless of which model we eventually choose, in working up our business proposal, my colleagues and I became aware that issues have arisen with respect to how robo-advisers can comply with the aforementioned regulatory standards. We foresee that these concerns may be amplified with respect to iRobo because it will have far fewer human employees than any existing robo-advisory firm.

We have, however, addressed these issues and, to that end, I am attaching a paper written by one of my classmates in the FinTech Innovation course and a recent Juris Doctor graduate of the Harvard Law School. Her paper explains how iRobo could meet both the suitability and fiduciary standards incumbent on dual registrants, and her arguments remain cogent regardless of whether we eventually decide to pursue a dual registrant model. This is because she addresses the suitability and fiduciary standards in discrete sections. (We've addressed other issues related to recordkeeping, custodial arrangements, and related compliance materials elsewhere.).

As her paper documents, the investment advice given by humans is not inherently superior to advice dispensed by algorithms and, indeed, the supervision by algorithms is likely more straight-forward than the supervision of humans. I trust you will find her arguments as persuasive as I did.

I look forward to hearing back from you and gaining your support for this endeavor.

The iRobo Business Model

This is a brief overview of how the iRobo platform would operate:

1. Potential clients begin by visiting the iRobo website (www.irobo.com).
2. They click on the "Get Started" tab, which prompts them to create an account by providing their identification, contact, and bank account details.
3. Clients are asked to fill in a questionnaire with respect to age, occupation, investing experience, annual income, investable assets, investing goals, and risk profile. Clients will also be required to complete an additional survey designed to generate an accurate estimate of each client's appetite for risk. Our algorithm matching process was designed by computer scientists, adapting practices refined in online dating applications with a demonstrated record of eliciting unbiased customer profiles and successful matches.
4. Clients are free at all times to amend the responses to both questionnaires and surveys and will be reminded on a monthly basis of their ability to make these amendments.
5. Clients are directed to an external consultant's website to address compliance with anti-money laundering requirements. (Outside vendors will also provide compliance and other recordkeeping and custodial services required of registered broker-dealers and investment advisers.).
6. Clients deposit an initial sum of money into their iRobo accounts and are given the option to set up an "Auto Deposit," which enables them to make regular, periodic deposits from their checking account to their iRobo accounts.
7. iRobo's algorithms process the information provided above and identify an appropriate asset allocation and a targeted annual rate of return, then execute what it determines to be an optimal investment strategy for each client.
    a. Clients are given the option of viewing further details, such as:
        i. An in-depth analysis of the assets held (e.g., characteristics and disclosure documents related to all holdings);
        ii. A detailed breakdown of how their assets are allocated (e.g., percentages and investment horizons); and
        iii. Key components of the iRobo optimization algorithm (e.g., risk-return goals, tax efficiency, and expense minimization).
    b. Clients are also given the option to engage in further customization (e.g., setting stop-loss orders or adjusting asset allocation) at any point.
    c. Our investment algorithms will track market movements in real-time and update investment strategies and optimization protocols as appropriate.
8. Customers will receive all required disclosures and statements in electronic format through a computerized process overseen by our compliance algorithm. For those interested in verbal communications, iRobo has purchased a state-of-the-art automated phone system to respond to customer queries.

9. iRobo has hired a panel of leading computer scientists to review the operation of its algorithms on a periodic basis (initially monthly, but eventually quarterly or yearly). All algorithms and databases will be available for review by supervisory personnel at any time, including (if desired) on a real-time feed. (iRobo does, however, request that this information be treated as confidential supervisory information and not be disclosed to third parties.)

The Regulation of Robo-Advising: What Is the Minimum Amount of Human Involvement Required to Provide Investment Advice?*

Introduction

Robo-advisers have changed the complexion of the financial services industry in a multitude of ways, not least by reducing the need for a human adviser to be present for investment advice to be dispensed. This paper will focus on that issue, by examining the minimum amount of human involvement required to provide investment advice.

Although there are myriad robo-advisory services, for the sake of clarity this paper will focus on robo-advising firms that are regulated as "dual registrants." These firms perform the dual functions of investment adviser and broker-dealer and are consequently regulated as such—they are required to register with both the SEC and FINRA.

The upshot is that dual registrants—as the name suggests—face twofold obligations. On the one hand, they are subject to the fiduciary obligations imposed on investment advisers by the Investment Advisers Act of 1940. On the other hand, they also must comply with the suitability standard set out for broker-dealers in the Securities Exchange Act of 1934 and FINRA Rule 2111.

Admittedly, in the case of dual registrants, it is difficult to draw a bright-line distinction between the fiduciary and suitability standards; they often shade into each other, and there have been calls for a harmonized fiduciary standard. However, it is beyond the ambit of this paper to delve into the nuances of that debate. The fiduciary and suitability standards are sufficiently distinct to warrant separate treatment for the purposes of understanding the regulatory issues discussed below.

This paper will argue that the minimum amount of human involvement required for a robo-adviser to provide investment advice is <u>one</u> person and, to that end, it will proceed in four stages:

1. The first section will provide a brief explanation of the fiduciary and suitability standards and elaborate on the minimum amount of human involvement required for *any* dual registrant to provide investment advice (i.e., one person).
2. The second section will focus on the central claim of this paper—that only one human being is needed—and set out the key arguments that must be justified for this claim to stand. In essence, this paper will need to show that the use of robo-advising technology does not affect the ability of a dual registrant to fulfill either the fiduciary or suitability standard, which would mean that a dual-registrant robo-advising firm can thus dispense investment advice just as *any* dual registrant would. Therefore, in accordance with the prevailing regulatory requirements, this would mean that only one person is needed.

   As a tangential matter, this section will also draw on empirical research to contend that robo-advisers are not necessarily inferior to human advisers. Much ink has been spilled over concerns that algorithms can never replicate a "human touch," but it will be argued that the underlying thrust of this paper—that robo-advising firms should be welcomed—is ultimately borne out by empirical evidence.

* Prepared by Jane Gonzales in connection with the HBS Financial Innovation Competition

3. The third section will focus on the suitability standard that must be met by broker-dealers and evaluate the arguments for and against whether robo-advising firms can meet that standard. It will be argued that robo-advisers are fundamentally able to fulfill the suitability standard.
4. In a similar vein, the fourth and final section will highlight the fiduciary obligations incumbent on investment advisers and assess the arguments for and against whether robo-advisers can successfully discharge those obligations. As noted in the preceding section, it will be argued that robo-advisers can also satisfy the fiduciary standard, although it may be harder to do so than with the suitability standard.

The Existing Regulatory Framework

This paper focuses on robo-advising firms that are regulated as dual registrants, and such firms face twofold regulatory requirements. As investment advisers, they are held to a fiduciary standard; as broker-dealers, they must comply with a suitability standard. This section will explain what these standards entail and highlight the existing regulatory framework for the minimum number of humans required for investment advice to be dispensed.

The exact content of the fiduciary obligations that an investment adviser must discharge is not cut and dried, but it is sometimes described as constituting: 1) a duty of loyalty to serve the best interests of clients and to disclose any conflicts of interest; and 2) a duty of care requiring the investment adviser to provide suitable advice and to seek the best execution of his clients' securities transactions.[1]

The suitability standard for broker-dealers can be found in FINRA Rule 2111, and it is markedly similar to the second limb of an investment adviser's fiduciary duty. Specifically, it requires that a broker-dealer "must have a reasonable basis to believe that a recommended transaction or investment strategy involving a security or securities is suitable for the customer."[2]

Although the fiduciary and suitability standards sound similar, they are in fact sufficiently distinct to warrant different treatment. To understand the relationship between the fiduciary and suitability standards, it is best to simply see the latter as "a less intensive form of fiduciary duty" than the one imposed on investment advisers.[3] An excellent explanation can be found in an article by Professor Howell Jackson and Talia Gillis, who argue that the suitability requirement for broker-dealers "tracks the essence of fiduciary duty: legal obligations that arise out of the nature of the relationship between a firm and its customers."[4]

Lastly, under the existing regulatory framework, at minimum only one human is needed for a dual registrant to dispense investment advice. For both investment advisers and broker-dealers, this information can be found in their SEC registration documents—Form ADV and Form BD respectively. Their registration documents allow for the possibility of an investment adviser functioning as a "sole

[1] Stephen Wink, Stefan Paulovic and Michael Shaw, *Dually Registered Brokers and Advisers*, 46 THE REVIEW OF SECURITIES & COMMODITIES REGULATION 191, 195, Sept. 4, 2013.

[2] FINRA Rule 2111, Suitability, http://finra.complinet.com/en/display/display_main.html?rbid=2403&element_id=9859 [https://perma.cc/RKN9-E6UG], accessed January 31, 2019.

[3] Howell Jackson and Talia Gillis, *Fiduciary Duties in Financial Regulation: Harvard Public Law Working Paper No. 18-24, 16*, *SOCIAL SCIENCE RESEARCH NETWORK* (Apr. 17, 2018), https://papers.ssrn.com/sol3/abstract=3149577, [https://perma.cc/MJY7-KEMP].

[4] *Id.*

proprietor," with the individual in question wearing multiple hats (e.g., Chief Executive Officer and Chief Compliance Officer).[5]

Only One Human Is Needed

The central claim of this paper is that the minimum amount of human involvement required for a robo-adviser to provide investment advice is one person, and this section will set out the key arguments that must be justified for this claim to stand.

So far, it has been established that at minimum only one human is required for a typical dual registrant to dispense investment advice (i.e. a sole proprietor), and the overarching argument of this paper is that the use of robo-advising technology does not affect this minimum requirement.

Subsequent sections will show that the use of robo-advising technology does not impair the ability of a dual registrant to fulfill either the fiduciary or suitability standard, which would mean that a dual registrant robo-advising firm could thus dispense investment advice just as any dual registrant would. In essence, the prevailing regulatory framework would still apply to robo-advisers, and therefore only one human would be needed.

In addition, it is important at this juncture to address the normative question of whether robo-advising algorithms are inherently inferior to human advisers. The succeeding discussion will operate on the working assumption that robo-advisers are at least equal, if not superior, to human advisers; therefore, before proceeding, it is worthwhile to assuage concerns that algorithms can never replicate a "human touch" in decision-making.

Much ink has been spilled over the notion that robo-advising algorithms are less effective than human advisers, especially because of their "inability to address subtleties" that humans can provide through "personalized advice."[6] The implication is that human advisers have superior judgment and following their advice allows clients to attain a better rate of return on their investments compared to following the advice of robo-advisers.

However, there is in fact a plethora of empirical research suggesting the contrary. Economist Brian Melzer and his colleagues have conducted research in Canada which suggests that advice proffered by human advisers is "one-size-fits-all" rather than "personalized,"[7] and that human advisers often hold "misguided beliefs."[8] Similarly, Terrance Odean has published a wealth of articles suggesting that humans

[5] Division of Investment Management, Securities and Exchange Commission (SEC), *Form ADV, Uniform Application for Investment Adviser Registration and Report by Exempt Reporting Advisers* (07-17), SEC Form ADV, SEC Form 1707 (07-17), Part 1A, https://www.sec.gov/about/forms/formadv-part1a.pdf; Division of Trading and Markets, Securities and Exchange Commission (SEC), *Form BD, Uniform Application for Broker-Dealer Registration* (01-2008), SEC Form 1490 (1-08), https://www.sec.gov/files/formbd.pdf; [https://perma.cc/SVU5-AWDK].

[6] Tara Bernard, *The Pros and Cons of Using a Robot as an Investment Adviser*, THE NEW YORK TIMES, Apr. 29, 2016, http://www.nytimes.com/2016/04/30/your-money/the-pros-and-cons-of-using-a-robot-as-an-investment-adviser.html [https://perma.cc/V4F9-DYFB].

[7] Stephen Foerster, Juhani Linnainmaa, Brian Melzer & Alessandro Previtero, *Retail Financial Advice: Does One Size Fit All?*, 72 THE JOUR. OF FIN. 1441, 2017.

[8] Juhani Linnainmaa, Brian Melzer & Alessandro Previtero, *The Misguided Beliefs of Financial Advisers: Kelly School of Business Research Paper No. 18-9,* SOCIAL SCIENCE RESEARCH NETWORK, Jan. 20, 2018, https://papers.ssrn.com/sol3/id=3101426 [https://perma.cc/4TSB-LSQ8].

tend to behave irrationally when making investments;[9] he points out that humans making investments "systematically share biases"[10] and are particularly susceptible to the disposition effect, which is the tendency "to hold losing investments too long and sell winning investments too soon."[11]

The above-mentioned papers only represent the tip of the iceberg—behavioral economists have conducted a substantial amount of research on these issues[12]—but the upshot is that robo-advising algorithms are not necessarily inferior to human advisers and may in fact be superior because they bring a level of dispassionate objectivity that humans are not capable. The corollary, therefore, is that robo-advising firms offer much that can be welcomed.

Meeting the Suitability Standard

The suitability requirement states that a broker-dealer "must have a reasonable basis to believe that a recommended transaction or investment strategy involving a security or securities is suitable for the customer."[13]

The argument that robo-advisers cannot meet the suitability requirement without additional human involvement turns on the concern that robo-advisers "are not a substitute for human judgment."[14] For example, FINRA sees human judgement as an essential component of conducting portfolio analysis in a way that is "appropriate for an individual client,"[15] because robo-advising algorithms do not possess "the requisite knowledge about the securities or customer necessary to make a suitable recommendation."[16]

In particular, FINRA is concerned about the inability of robo-advisers to 1) gather and adequately evaluate all of the required information about clients to make a suitability determination; 2) rectify

conflicting answers to client profile questionnaires; and 3) pair clients' investment profiles with suitable securities or investment strategies.[17]

FINRA's concerns are understandable, but these problems are by no means insurmountable and will be subsequently addressed to show how robo-advisers can in fact meet the suitability standard. Ultimately, the lack of human involvement that many perceive to be robo-advising's greatest weakness should instead be seen as its greatest strength. Regulators must, therefore, be careful not to throw the baby out with the bathwater.

[9] *See, e.g.*, Brad Barber & Terrance Odean, *The Behavior of Individual Investors*, HANDBOOK OF THE ECONOMICS OF FINANCE: VOLUME TWO (George Constantinides, Milton Harris & Rene Stulz, Eds., 2013).

[10] Brad Barber & Terrance Odean, *The Courage of Misguided Convictions*, 55 FINANCIAL ANALYSTS JOURNAL 41 (1999).

[11] Terrance Odean, *Are Investors Reluctant to Realize Their Losses?* 53 THE JOURNAL OF FINANCE 1775 (1998).

[12] *See, e.g.*, Matthew Rabin, *Psychology and Economics*, 36 Journal of Economic Literature 11, 1998; Robert Shiller, *Human Behavior and the Efficiency of the Financial System* 1999: NBER Working Paper No. 6375, NAT. BUR. ECON. RESEARCH; Harrison Hong, José Scheinkman & Wei Xiong, *Advisers and Asset Prices: A Model of the Origins of Bubbles*, 89 JOURNAL OF FINANCIAL ECONOMICS 268, 2008.

[13] FINRA, *supra* note 2.

[14] Melanie Fein, *Regulatory Focus on Robo-Advisors*, SOCIAL SCIENCE RESEARCH NETWORK, Sept. 12, 2017, https://ssrn.com/abstract=3028259 [https://perma.cc/U75Y-DNXC].

[15] Melanie Fein, *FINRA's Report on Robo-Advisors: Fiduciary Implications*, SOCIAL SCIENCE RESEARCH NETWORK, Apr. 1 2016, https://ssrn.com/abstract=2768295 [https://perma.cc/6ZXX-VG95].

[16] Regulatory Operations, *Report on Digital Investment Advice*, FINANCIAL INDUSTRY REGULATORY AUTHORITY, March 15 2016, http://www.finra.org/sites/default/files/digital-investment-advice-report.pdf [https://perma.cc/MR4W-4Y2D].

[17] Fein, *supra* note 14 at 8.

An important caveat to the discussion that follows is that it will proceed on the assumption that the robo-advisers in question are "well designed." While this is undoubtedly "stacking the deck in favor of robo-advisers," as Professors Tom Baker and Benedict Dellaert have done, it is necessary to delimit the scope of this paper lest it morphs into a paper on algorithm design.[18]

Gathering Information

Firstly, FINRA is concerned about the ability of robo-advisers to "gather and adequately evaluate all of the required information about clients to make a suitability determination."[19] This concern is understandable and will be swiftly evident to anyone who has signed up for an account at any of the major robo-advising platforms.

For instance, a Betterment account can be opened in less than five minutes, and the pre-sign-up questionnaire consists almost entirely of multiple-choice questions.[20] In comparison, Wealthfront has a more comprehensive pre-sign-up process that also involves a risk assessment analysis,[21] but it also still falls short of the level of nuance required to conduct an appraisal of suitability tailored to the individual customer.[22]

For example, consider Wealthfront's risk tolerance questionnaire,[23] which asks a customer how they would respond to a steep market correction. In response, a customer can only choose from the following four options: "buy more," "keep them all," "sell some," or "sell them all"; there are no intermediate options that allow a customer to specify an exact percentage of their stock portfolio or the price(s) at which they would buy or sell.[24] However, this is far removed from reality—trying to invest effectively with only four options for action is like trying to hit a baseball pitch by swinging the bat at four pre-determined angles.

It is therefore unsurprising that FINRA has expressed unease about this aspect of robo-advising. However, the issue does not lie with robo-advisers but rather with the structure of the client onboarding questionnaire. For that reason, rather than concluding that robo-advisers are inherently unable to meet the suitability standard, the better response may be to set out guidelines for questionnaires that would assist robo-advisers in obtaining the information required to meet the suitability standard.

This is not an inordinately difficult undertaking, as the questionnaires do not need to be especially sophisticated; they only need to replicate a typical conversation that a human investment adviser would have with their client, and this should not be hard to accomplish considering the advancement of artificial intelligence technology.[25]

[18] Tom Baker & Benedict Dellaert, *Regulating Robo Advice across the Financial Services Industry*, 103 Iowa Law Rev. 713, 724, 2018.

[19] Fein, *supra* note 14, 8.

[20] Betterment, *Get Started: Here's what to expect*, Betterment, 2018, https://wwws.betterment.com/app/get_started.

[21] Wealthfront, *Get Started: Let's build a smart investment plan*, Wealthfront, 2018, https://www.wealthfront.com/start/intro [https://perma.cc/XW49-6QV6].

[22] Caelainn Carney, Robo-Advisers and the Suitability Requirement: How They Fit in the Regulatory Framework 2018 Columbia Bus. Law Rev. 586, 601, 2018.

[23] Wealthfront, *supra* note 21.

[24] Carney, *supra* note 22, 601.

[25] Jennifer Hill, W. Randolph Ford, & Ingrid Farreras, Real conversations with artificial intelligence: A comparison between human–human online conversations and human–chatbot conversations, 49 Computers in Human Behavior 245 (2015); Heloisa Candello, Claudio Pinhanez, David

Essentially, such a questionnaire could take the form of a chatbot that mimics the reactive and adaptive nature of human conversation—if a customer says that he would "sell some" of his stocks in a market downturn, the chatbot would then ask him to specify a percentage of his portfolio and a price range for his shares. By the end of the online conversation, the robo-adviser platform should have enough information to make investment decisions that are sufficiently tailored to the specific context of the client, moving one step closer towards meeting the suitability standard.

At the end of the day, the difference between human and robo-advisers is one of degree rather than kind; admittedly, humans offer a "warm-body effect" that robo-advisers do not possess,[26] but the substantive process is similar. A human adviser that has dealt with hundreds of clients will inadvertently have a mental checklist that he subconsciously refers to during the client onboarding process,[27] and this is no less formulaic than how a robo-advising algorithm would operate.

Rectifying Conflicting Answers

Secondly, FINRA is concerned about the ability of robo-advisers to "rectify conflicting answers to client profile questionnaires."[28] Once again this concern stems from an issue with questionnaire design rather than with robo-advisers; it would be inadvisable to dismiss robo-advisers as being inherently unable to meet the suitability standard without first considering alternative solutions to this problem.

For example, a possible solution might involve adding built-in triggers to the questionnaire that 1) prompt a customer when their responses appear to be internally inconsistent, and 2) flag the inconsistent information for further review by a human adviser before an account can be opened.[29] The result is that conflicting responses would be subject to multiple levels of checks, and a customer would not be able to start an account with a robo-advising platform until the conflicts have been resolved.

FINRA's concerns over resolving conflicting responses to questionnaires can be alleviated, and they should not pose any obstacle to robo-advisers meeting the suitability standard.

Pairing Clients with Investments

Lastly, FINRA is concerned about the ability of robo-advisers to "pair clients' investment profiles with suitable securities or investment strategies."[30] This is the easiest of FINRA's concerns to resolve. As discussed earlier, empirical research has demonstrated that human advisers are susceptible to a surfeit

Millen & Bruna Daniele Andrade, Shaping the Experience of a Cognitive Investment Adviser in DESIGN, USER EXPERIENCE, AND USABILITY: UNDERSTANDING USERS AND CONTEXTS (PART 3) (Aaron Marcus & Wentao Wang, Ed's. 2017.

[26] Jill Fisch, Marion Laboure and John Turner, *The Economics of Complex Decision Making: The Emergence of the Robo Adviser*, UNIVERSITY OF PENNSYLVANIA LAW SCHOOL – INSTITUTE FOR LAW AND ECONOMICS, 2017, [https://perma.cc/8CCP-ETF6].

[27] *See, e.g.*, Daniel Kahneman & Mark Riepe, *Aspects of Investor Psychology*, 24 JOURNAL OF PORTFOLIO MANAGEMENT 52, 64 1998.

[28] Fein, *supra* note 14, 8.

[29] Carney, *supra* note 22, 603; Securities and Exchange Commission, Division of Investment Management, *Guidance Update: Robo-Advisers*, SECURITIES AND EXCHANGE COMMISSION, No. 2017-02, 7, Feb. 23, 2017) 7, https://www.sec.gov/investment/im-guidance-2017-02.pdf [https://perma.cc/UT5K-2MFW].

[30] Fein, *supra* note 14, 8.

of biases, suggesting that dispassionate robo-advisers should be able to match customers to investments at least as well as—if not even better than—human advisers.[31]

This leads to the corollary conclusion that if human advisers are capable of meeting the suitability standard, then so are robo-advisers. Understandably, this then raises questions of algorithm design (i.e., only well-designed robo-advisers should be able to meet the suitability standard, in the same way that only competent human advisers can do so), but the answers to those questions lie beyond the scope of this paper.

It is clear that robo-advisers are able to match clients with appropriate investment strategies that equal, if not surpass, the ability of a human broker-dealer.

Discharging Fiduciary Obligations

Having addressed the suitability standard, this section will examine the question of whether robo-advising firms can meet the fiduciary obligations incumbent on investment advisers. This section will argue that robo-advisers can meet the fiduciary standard as well, even though their case might not be as strong as with the suitability standard.

Having established earlier that the suitability standard is "a less intensive form of fiduciary duty,"[32] and because the suitability standard has already been examined in the previous section, this section will focus on the area in which the fiduciary standard goes above and beyond what is required under the suitability standard.

This aspect of the fiduciary standard bears repeating, because it is at the crux of the debate: the key distinguishing feature is that the investment-adviser fiduciary relationship requires advisers to act in the "best interest" of their clients. While the content of "best interest" is not "well defined,"[33] for the purposes of this discussion about robo-advisers, it is clear that it is a higher bar than the suitability standard because it requires the adviser to conduct "initial and ongoing due diligence."[34] In essence, this means that the investment-adviser fiduciary relationship is a continuing relationship, as opposed to the predominantly transactional nature of broker-dealer relationships.

It is, therefore, inherently more challenging for robo-advisers to meet the fiduciary standard than the suitability standard, because they "have no human contact with the client" and it is consequently harder for them to identify their client's best interest within the context of an "ongoing relationship."[35] This is the position taken by a broad spectrum of commentators, ranging from Melanie Fein and Professor Arthur Laby, to the Massachusetts Securities Division.

[31] Foerster, supra note 7; Linnainmaa, *supra* note 8; Barber, *supra* note 9; Barber, supra note 10; Odean, *supra* note 11; Rabin, *supra* note 12; Shiller, *supra* note 12; Hong, *supra* note 12.

[32] Jackson, *supra* note 3, 16.

[33] Carney, *supra* note 22, 598.

[34] Fein, *supra* note 15, 4.

[35] Melanie Fein, *Are Robo-Advisors Fiduciaries?*, SOCIAL SCIENCE RESEARCH NETWORK 18, 2017, https://ssrn.com/abstract=3028268 [https://perma.cc/LS4C-QXS7]

Challenges Faced in Meeting the Fiduciary Standard

For instance, the Massachusetts Securities Division (MSD) has argued that robo-advisers "may be inherently unable" to carry out the fiduciary obligations of an investment adviser.[36] The division arrived at this conclusion primarily on the grounds that robo-advisers 1) do not conduct either initial or ongoing due diligence on clients and 2) often disclaim the obligation to act in a client's best interests.[37] Specifically on the latter point, the MSD argued that clients are routinely left to provide crucial updates about any changes to their financial or personal situation; robo-advisers typically decline any ongoing duty to make such inquiries, despite the fact that such changes may well have an impact on the appropriateness of investment decisions.[38]

Similarly, Professor Arthur Laby has suggested that robo-advisers will struggle to meet the fiduciary standard because they are unable to capture the nuances that would ordinarily arise in a human-to-human interaction.[39] Professor Laby argues that clients cannot inform robo-advisers of "wrinkles," such when the client anticipates the possibility of significant changes in their financial situation (e.g., an inheritance), and this inability to account for the complete factual matrix means that a robo-adviser cannot be said to be acting in a client's "best interest."[40]

Melanie Fein, a former head of Arnold & Porter's Bank Mutual Funds Practice, goes one step further and argues that robo-advisers cannot meet the fiduciary standard not only because they are unable to conduct "ongoing due diligence," but also because they are not equipped to act in a client's "best interest" during times of severe market corrections.[41] This notion finds support from former SEC Commissioner Kara Stein, who has also raised concerns that "robo-advisers will not be on the phone providing counsel if there is a market crash."[42]

These concerns are not unfounded—even though algorithms are disinterested and dispassionate, their human clients are still subject to the emotional turmoil wrought by market vicissitudes.[43] Because robo-advisers are unable to appreciate the nuances of human emotion (e.g., fear or greed) in providing investment advice, human advisers will still be needed during market downturns to provide the emotional reassurance that algorithms cannot offer. This has been described as the "warm-body effect,[44] and is perhaps best summarized by a Wall Street Journal article which argued that "an email or text message in

[36] Massachusetts Sec'y of State, Securities Division, *News and Updates: Policy Statement: Robo-Advisors and State Investment Adviser Registration*, MASSACHUSETTS SEC'Y OF STATE, SECURITIES DIVISION 8, Apr. 1, 2016, https://www.sec.state.ma.us/sct/sctpdf/Policy-Statement--Robo-Advisers-and-State-Investment-Adviser-Registration.pdf [https://perma.cc/P92H-4CV5].

[37] *Id.*

[38] Fein, *supra* note 14), 20.

[39] Bernard, *supra* note 6.

[40] *Id.*

[41] Melanie Fein, *Robo-Advisors: A Closer Look, Scholarly Paper ID 2658701*, SOCIAL SCIENCE RESEARCH NETWORK 5, 2015, https://ssrn.com/abstract=2658701 [https://perma.cc/2BXF-TQAQ].

[42] Kara Stein, *Surfing the Wave: Technology, Innovation, and Competition: Remarks at Harvard Law School's Fidelity Guest Lecture Series*, Nov. 9, 2015), http://www.sec.gov/news/speech/stein-2015-remarks-harvard-law-school.html [https://perma.cc/MHF8-6T8Y].

[43] Bret Strzelczyk, Rise of the Machines: The Legal Implications for Investor Protection with the Rise of Robo-Advisors, 16 DePaul Business and Commercial Law Journal 54, 62, 2018.

[44] Fisch, *supra* note 26, 15.

the fall of 2008 would not have sufficed to keep millions of panicked savers from selling, with devastating consequences for their nest eggs."[45]

Overcoming the Challenges

There are two primary issues that have been identified, namely the inability of robo-advisers to 1) conduct "ongoing due diligence," and 2) act in the "best interests" of clients during times of market stress. Both contain a kernel of truth but have been blown out of proportion.

Firstly, while it is true that robo-advisers are unable to conduct "ongoing due diligence" in the sense that they depend on customer input, the issue yet again lies with algorithm design rather than with robo-advisers. After all, Professor Laby's concern that robo-advisers are not able to account for "wrinkles" applies to human advisers just as much as it does to robo-advisers—a human investment adviser would also be unable to account for such information unless it had been disclosed.

The inability to conduct "ongoing due diligence" is thus not an insuperable barrier to meeting the fiduciary standard; critics may have painted robo-advisers as entirely passive platforms, but this is not necessarily the case. Just as an investment adviser might call his clients monthly to check for updates to their financial situation, so too could a robo-adviser be pre-programmed to prompt clients monthly to provide updates, if any, regarding their financial and personal situation.

Secondly, concerns about the inability of robo-advisers to act in the "best interests" of clients during market downturns are similarly overstated. Admittedly, a robo-adviser may not be able to provide the reassurance that comes with the "warm-body effect,"[46] but it cannot be said that human investment advisers always have a steady hand on the tiller when market corrections occur. After all, it has been observed by John Bogle that "investors are more volatile than investments."[47]

Considering that human advisers are not likely to be paragons of calm during market crashes, it is not implausible that robo-advisers could do at least as good a job as human advisers in acting for the "best interests" of their clients during times of market stress. For example, robo-advisers could be preprogrammed to execute stop-loss orders during severe downturns, with the trigger price determined by answers to the risk-appetite questionnaire during the client onboarding process.

Additionally, it is also possible for robo-advisers to protect the "best interests" of their clients by implementing a trading "kill switch" that is activated when the market volatility exceeds a predetermined benchmark. For example, although not specifically referred to as a "kill switch," this occurred on the morning after the Brexit vote in 2016, when Betterment suspended all trading on its platform for over two hours. The rationale behind the trading halt was to protect the "best interests" of Betterment's clients—Betterment explained that it would have been "undesirable" for their clients to trade into such

[45] Robert Litan and Hal Singer, *Obama's Big Idea for Small Savers: "Robo" Financial Advice*, WALL STREET JOURNAL, July 21, 2015), https://www.wsj.com/articles/obamas-big-idea-for-small-savers-robo-financial-advice-1437521976 [https://perma.cc/C6A4-AC82].

[46] Fisch, supra note 26, 15.

[47] John Bogle, *Black Monday and Black Swans*, 64 Financial Analysts Journal 30, 34, 2008.

"wild price swings,"[48] and the halt was meant to "protect clients from making panicked decisions that would result in poor trade execution and higher transaction costs."[49]

Therefore, we can see that neither objection is insurmountable, and that perhaps it might be possible for robo-advisers to meet the fiduciary standard after all.

Disclosure-and-Consent Requirements

Up to this point, the arguments in favor of robo-advisers meeting the fiduciary standard have primarily been defensive and argued that the criticisms levelled against robo-advisers can be rebutted. However, this subsection will attempt to put forward a novel argument, by arguing that their fiduciary obligations could also be discharged through disclosure-and-consent requirements.

The foundation for this idea is borrowed from Professor Howell Jackson and Talia Gillis of Harvard Law School, who point out that "sometimes disclosure-and-consent requirements are so onerous that they approximate rules of conduct."[50]

The reasoning behind this approach is that 1) disclosure-and-consent requirements and 2) conduct rules are essentially two sides of the same "fiduciary duty" coin. In light of the fact that it is structurally more challenging for robo-advisers to meet conduct rules, for example because they lack volition, the emphasis should instead fall on the use of disclosure-and-consent requirements as a means by which robo-advisers can meet the fiduciary standard. After all, as long as the disclosure-and-consent requirements are "sufficiently stringent," they can be approximated to a rule of conduct.[51]

As Professor Jackson and Talia Gillis suggest, a "sufficiently stringent" regulatory framework could take the form of ex post disclosure-and-consent requirements, such as "where a fiduciary must obtain consent for every transaction falling within a certain category."[52] An ex post disclosure-and-consent requirement might seem like an unduly onerous burden for both robo-advisers and their clients, especially because robo-advising is meant to streamline and automate the investment advisory process. However, it is a necessary imposition if a balance is to be appropriately struck between allowing robo-advisers to discharge their fiduciary obligations and ensuring that clients are protected.

This paper does not have the scope to flesh out the specificities of an ex post disclosure-and-consent requirement for robo-advisers, but a model might be drawn from Article 24(4) of the European Union's recently implemented Markets in Financial Instruments Directive II.[53]

[48] Michael Wursthorn and Anne Tergesen, *Robo Adviser Betterment Suspended Trading During 'Brexit' Market Turmoil* WALL STREET JOURNAL, June 24, 2016, http://www.wsj.com/articles/robo-adviser-betterment-suspended-trading-during-brexit-market-turmoil-1466811073 [https://perma.cc/D3KM-J2A8].

[49] Megan Ji, Are Robots Good Fiduciaries? Regulating Robo-Advisors Under the Investment Advisers Act of 1940, 117 Columbia Law Review 1543, 1568, 2017.

[50] Jackson, *supra* note 3, 17.

[51] Jackson, *supra* note 3, 21.

[52] *Id.*; the specific example used is Section 206(3) of the Investment Advisers Act of 1940, which requires investment advisers to acquire consent for every relevant transaction when trading with a client as principal. Professor Jackson and Talia Gillis argue that "such a consent requirement creates an insuperable barrier to certain kinds of transactions, effectively approximating a rule of conduct."

[53] Article 24(4) of Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014.

Article 24(4) imposes an ex post disclosure requirement on investment advisers that is precisely the sort desired in this subsection, with the only difference being the lack of an additional requirement for informed consent.

Among other things, Article 24(4) requires that the following information be provided to clients "in good time":

- whether or not the advice is provided on an independent basis; and
- whether the advice is based on a broad or on a more restricted analysis of different types of financial instruments and, in particular, whether the range is limited to financial instruments issued or provided by entities having close links with the investment firm or any other legal or economic relationships…so close as to pose a risk of impairing the independent basis of the advice provided.[54]

Additionally, Article 24(4) also requires that "the information about all costs and charges…which are not caused by the occurrence of underlying market risk, shall be aggregated to allow the client to understand the overall cost as well as the cumulative effect on return of the investment, and where the client so requests, an itemized breakdown shall be provided. Where applicable, such information shall be provided to the client on a regular basis…during the life of the investment."[55]

Ex post disclosure-and-consent requirements are thus a possible means by which robo-advisers could discharge their fiduciary obligations, although this is not as straightforward as meeting the suitability standard. No matter how stringent they may be, the notion that meeting disclosure-and-consent requirements alone could be sufficient for a robo-adviser to perform its fiduciary duty does not comport with the orthodoxy of investment adviser fiduciary law.

However, although it may be easy to conclude that this proposal holds no prospect of success, it is important to heed recent guidance from the SEC, which hints at a likelihood that such a disclosure-based strategy could work.[56] Specifically, the SEC has acknowledged the notion that robo-advisers can meet the investment adviser fiduciary standard, provided they comply with key qualitative metrics: such as e*x ante* "adequate and effective disclosure."[57]

The SEC's suggestion of an *ex ante* disclosure-only requirement is less rigorous than what has been proposed in this subsection. What they suggest is more similar to a hedge clause recommending that robo-advising firms alert potential clients to, among other things, "the particular risks inherent in the use of an algorithm;[58] they also emphasize that the disclosures should be written in "plain English" and brought to the attention of potential clients (e.g., "through design features such as pop-up boxes").[59] In essence, the SEC seems to suggest that sufficient *ex ante* disclosure would entail ensuring that clients signing up to a robo-advising platform do so with a heightened awareness of its unique features and attendant risks.

[54] *Id* at 5.

[55] *Id*.

[56] Securities and Exchange Commission, Division of Investment Management, *supra* note 29.

[57] Nicole Iannarone, Computer as Confidant: Digital Investment Advice and the Fiduciary Standard, 93 CHICAGO-KENT LAW REVIEW 141, 158, 2018.

[58] Securities and Exchange Commission, Division of Investment Management, *supra* note 29, 4.

[59] *Id* at 5.

The proposal in this subsection goes even further than the SEC's *ex ante* disclosure-only requirement by arguing for an *ex post* disclosure-and-consent requirement. Therefore, even though it may be unconventional, it is likely to be sufficient to allow robo-advisers to discharge their fiduciary obligations.

Conclusion

Robo-advisers are capable of meeting the suitability and fiduciary standards, and thus the prevailing regulatory framework should apply to them—meaning that at minimum only one human being is needed for investment advice to be dispensed.

However, an important caveat is that the preceding discussion takes place at a very high level of abstraction. Although it is a helpful intellectual exercise to consider the minimum amount of human involvement required for a robo-adviser to provide investment advice, in practice robo-advising firms are unlikely to be pushing that envelope. After all, dual registrants of the sort discussed in this paper will often have assets under management in excess of $100 million, and it would be inadvisable for a single individual to be responsible for such vast sums.

Robo-advising algorithms are our friend, not foe; therefore, regulators should be careful to avoid knee-jerk responses that risk throwing the baby out with the bathwater. It is sometimes said that it is "better to be approximately right than precisely wrong,"[60] and the advent of robo-advising provides us with the opportunity to do just that; the path ahead is uncertain but filled with transformative potential and, in stepping forward, we should be careful not to sacrifice financial innovation on the altar of over-regulation.[61]

[60] This aphorism is often attributed to Warren Buffett.

[61] Chris Brummer and Yesha Yadav, *FinTech and the I*nnovation Trilemma Scholarly Paper ID 3054770, SOCIAL SCIENCE RESEARCH NETWORK 12, 2018, https://www.ssrn.com/abstract=3054770 [https://perma.cc/88QQ-DJAJ].

Appendices

1. Melanie L. Fein, Regulatory Focus on Robo-Advisors (September 12, 2017). https://ssrn.com/abstract=3028259 or http://dx.doi.org/10.2139/ssrn.3028259
2. Melanie L. Fein, FINRA's Report on Robo-Advisors: Fiduciary Implications (April 1, 2016). https://ssrn.com/abstract=2768295 or http://dx.doi.org/10.2139/ssrn.2768295
3. Melanie L. Fein, Are Robo-Advisors Fiduciaries? (September 12, 2017). https://ssrn.com/abstract=3028268 or http://dx.doi.org/10.2139/ssrn.3028268
4. Betterment, How It Works. https://www.betterment.com/how-it-works or https://perma.cc/H6MW-AC2M.
5. Financial Industry Regulatory Authority, Report on Digital Investment Advice. https://www.finra.org/sites/default/files/digital-investment-advice-report.pdf or https://perma.cc/D7UH-7MXB.
6. Securities and Exchange Commission, IM Guidance Update: Robo-Advisers. https://www.sec.gov/investment/im-guidance-2017-02.pdf or https://perma.cc/2TCM-S3GU
7. Massachusetts Securities Division, Policy Statement: Robo-Advisors and State Investment Adviser Registration.

   https://www.sec.state.ma.us/sct/sctpdf/policy-statement--robo-advisers-and-state-investmentadviser-registration.pdf or https://perma.cc/792K-LS37
8. Tom Baker and Benedict G. C. Dellaert, Regulating Robo Advice Across the Financial Services Industry (2018).

   https://ssrn.com/abstract=2932189 or http://dx.doi.org/10.2139/ssrn.2932189.
9. Jill Fisch, Marion Laboure and John Turner, The Economics of Complex Decision Making: The Emergence of the Robo Adviser.

   https://pensionresearchcouncil.wharton.upenn.edu/wp-content/uploads/2018/05/Fisch.pdf or https://perma.cc/9WBG-LS7N.
10. Caelainn Carney, Robo-Advisers and the Suitability Requirement: How They Fit in the Regulatory Framework.

    https://perma.cc/E3TE-DBRV
11. Megan Ji, Are Robots Good Fiduciaries? Regulating Robo-Advisors Under the Investment Advisers Act of 1940.

    https://perma.cc/L9A4-MLZX
12. Nicole Iannarone, Computer as Confidant: Digital Investment Advice and the Fiduciary Standard.

    https://scholarship.kentlaw.iit.edu/cgi/viewcontent.cgi?article=4196&context=cklawreview or https://perma.cc/N5VY-6HAK.
13. Tom Anderson, More robo-advisors are adding a human touch to their services (January 31, 2017).

    https://www.cnbc.com/2017/01/31/more-robo-advisors-are-adding-that-human-touch.html or https://perma.cc/NX25-L7ZE

Other Academic Papers:

14. Juhani Linnainmaa, Brian Melzer and Alessandro Previtero, The Misguided Beliefs of Financial Advisors (May 16, 2018).
    https://ssrn.com/abstract=3101426 or http://dx.doi.org/10.2139/ssrn.3101426
15. Brad Barber and Terrance Odean, The Behavior of Individual Investors (September 7, 2011).
    https://ssrn.com/abstract=1872211 or http://dx.doi.org/10.2139/ssrn.1872211
16. Howell Jackson and Talia Gillis, Fiduciary Duties in Financial Regulation (April 17, 2018).
    https://ssrn.com/abstract=3149577 or http://dx.doi.org/10.2139/ssrn.3149577
17. John Lightbourne, Algorithms & Fiduciaries: Existing and Proposed Regulatory Approaches to Artificially Intelligent Financial Planners (2017).
    https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/duklr67&section=19
18. Andrea L. Seidt, Noula Zaharis and Charles Jarrett, Paying Attention to That Man Behind the Curtain: State Securities Regulators' Early Conversations with Robo-Advisers (2019)
    https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/utol50&section=38
19. Jake Rifkin, Robo-Advisers Jumping on the Bandwagon: Yet Another Cry for a Uniform Standard (2019)
    https://scholarship.law.unc.edu/cgi/viewcontent.cgi?article=6716&context=nclr
20. Nicole Iannarone, Rethinking Automated Investment Adviser Disclosure (2019)
    https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/utol50&section=33
21. Xusen Cheng et al., Exploring the Trust Influencing Mechanism of Robo-Advisor Service (2019)
    https://www.mdpi.com/2071-1050/11/18/4917
22. Jennifer Klass and Eric Perelman, The Evolution of Advice: Digital Investment Advisers as Fiduciaries (2016)
    https://www.morganlewis.com/-/media/files/publication/report/im-the-evolution-of-advice-digital-investment-advisers-as-fiduciaries-october-2016.ashx?la=en&hash=7A28D9586FD8ACADC9731733BFE4281F4E6FEB49

Note: The Treasury Department FinTech Report of July 2018 addresses issues related to robo-advising on pages – 159 to 164.

HARVARD
LAW SCHOOL | The Case Studies

CSP055
JUNE 2020

Market Manipulation: Definitional Approaches

CHRISTINA DRAKEFORD

Memorandum

DATE: June 21, 2020

TO: Junior Staffer, U.S. Securities and Exchange Commission

FROM: Chair, Securities and Exchange Commission

RE: Potential changes to the definition of manipulation

The popularity of algorithmic trading has increased substantially over the last decade. About 70 percent of total trading volumes of financial securities in developed markets stems from algorithmic trading.[1] As you know, an algorithm is simply a procedure to be followed in calculations or other operations, including those done by a computer.[2] Algorithmic trading is a process whereby a pre-programmed algorithm is responsible for deciding on price, timing, and volume when trading in financial instruments and securities.[3] In its simplest terms, algorithmic trading uses complex formulas to allow the computer to make decisions on whether to buy or sell financial securities on an exchange and how to go about doing so.[4]

Algorithmic trading is mostly used by institutional investors and big brokerage firms in order to decrease the costs associated with trading.[5] High-frequency trading (HFT) is a subset of algorithmic trading.[6] It allows buys and sells to occur at a very fast rate.[7] Humans do not have the ability to compute

[1] Ravi Kant, *Why algorithmic trading is dangerous*, Asia Times (May 7, 2019), https://www.asiatimes.com/2019/05/opinion/why-algorithmic-trading-is-dangerous/.

[2] TechTerms, *Algorithm*, https://techterms.com/definition/algorithm (last visited Feb. 10, 2020).

[3] James Chen, *What is Algorithmic Trading?*, Investopedia (Oct. 15, 2019), https://www.investopedia.com/terms/a/algorithmictrading.asp (last visited Feb. 10, 2020).

[4] *Id.*

[5] *Id.*

[6] Velvetech, *The Role of High-Frequency and Algorithmic Trading*, Velvetech, https://www.velvetech.com/blog/high-frequency-algorithmic-trading/ (last visited Feb. 10, 2020).

[7] *Id.*

Written by Christina Drakeford, under the supervision of Howell E. Jackson, James S. Reid, Jr., Professor of Law at Harvard Law School. Case development at Harvard Law School is partially funded by a grant from Dechert LLP. Cases are developed solely as the basis for class discussion. They are not intended to serve as endorsements, sources of primary data, legal advice, or illustrations of effective or ineffective management.

Copyright © 2020 President and Fellows of Harvard University. No part of this publication may be reproduced, stored in a retrieval system, used in a spreadsheet, or transmitted in any form or by any means—electronic, mechanical, photocopying, recording, or otherwise—without permission. To order copies or permissions to reproduce materials please visit our website at casestudies.law.harvard.edu or contact us by phone at 617-496-1316, by mail at Harvard Law School Case Studies Program, 1545 Massachusetts Avenue – Areeda 507, Cambridge, MA 02138, or by email at HLSCaseStudies@law.harvard.edu.

and analyze huge volumes of trading data in a short time frame, but a computer can.[8] HFT uses a powerful computer to implement a large number of orders in fractions of a second based on complex algorithms that are programmed to execute orders based on market conditions important to the programmer.[9]

With the increased popularity surrounding algorithmic trading and high-frequency trading, worries have grown more pronounced about whether our existing regulatory scheme can catch manipulative acts involved in such trading.

Mounting Problems Regarding the Use of Algorithmic Trading

2010 Flash Crash. On May 6, 2010, the Dow Jones Industrial Index fell by about 1,000 points and erased over $862 billion (amounting to 9% of value) from the US stock market.[10] This is deemed a "flash crash" (*i.e.*, large downward price changes in a very short period of time).[11] Public reporting highlighted the role of Waddell & Reed, an American mutual fund, that had placed a sell order for $4.1 billion.[12] That sell order was executed through the use of algorithmic trading.[13]

Computer Malfunctions. In 2013, Knight Capital Americas LLC agreed to pay a $12 million settlement for a computer malfunction that disrupted the markets.[14] Despite knowing that a function in its router was defective, Knight Capital kept the function in the router (intending for it not to be used).[15] The router was incorrectly used and as a result, it could not recognize when orders had been filled.[16] The router sent more than 4 million orders into the market and the Fund acquired several billion dollars in unwanted positions.[17] The SEC charged Knight Capital with violating the market access rule, for "[putting] both the firm and the markets at risk."

Low Trade-to-Order Submission Ratios. There is a growing concern about HFT generating a large amount of orders and then cancelling them. "Data show the typical trade-to-order submission ratios are between 2% and 4% on the major exchanges. That is, between 25 and 50 orders are generated for every execution."[18] Some believe this is evidence of market manipulation through the use of HFT.[19] Others

[8] *Id.*

[9] James Chen, *High-Frequency Trading (HFT)*, INVESTOPEDIA, https://www.investopedia.com/terms/h/high-frequency-trading.asp (last updated Oct. 10, 2019).

[10] *See* Kant, *supra* note 1.

[11] *Id.*

[12] *Id.*

[13] *Id.* Note that there is no government document officially blaming Waddell & Reid, and the Fund maintains that it was not at fault for the crash. *See* Graham Bowley, *Lone $4.1 Billion Sale Led to 'Flash Crash' in May*, NY TIMES (Oct. 1, 2010), https://www.nytimes.com/2010/10/02/business/02flash.html. The Fund placed a very large order on a day with world turmoil, causing normal institutional sources of liquidity to back away from the market. *See Findings Regarding the Market Events of May 6, 2010: Report of The Staffs of The CFTC and SEC to The Joint Advisory Committee on Emerging Regulatory Issues*, SEC (Sep. 30, 2010), https://www.sec.gov/news/studies/2010/marketevents-report.pdf.

[14] US Securities and Exchange Commission, *SEC Charges Knight Capital with Violations of Market Access Rule* (Oct. 16, 2013), https://www.sec.gov/news/press-release/2013-222.

[15] *Id.*

[16] *Id.*

[17] *Id.*

[18] Ryan J. Davies & Erik R. Sirri, The Economics of Trading Markets, in SECURITIES MARKET ISSUES FOR THE 21ST CENTURY, 145, at 172 (Merritt B. Fox et al. eds., 2018), https://www.law.columbia.edu/sites/default/files/microsites/capital-markets/securities_market_issues_for_the_21st_century.pdf, at 173.

[19] *Id.*

arguing that the cancellations are not exactly a bad phenomenon—noting that the large number of cancellations can lead to market making and price accuracy.[20]

Electronic Front-Running. Electronic front-running involves an HFT trader becoming aware of a transaction taking place on one trading venue (e.g., they see a trader trying to execute a certain trade on one stock exchange), and through that deducing that that trade must be on the way to several trading venues.[21] Because HFT involves a speed advantage, they can beat that trader to the other trading venues and execute the trades.[22] This typically disadvantages the trader that initially placed the order.[23] Although generally not illegal, some people have called this "front-running," which is a phrase that more traditionally describes the illegal practice of a broker-dealer using information about a customer's order to trade for the broker-dealer's own benefit before executing the customer's order.

Rebate Arbitrage. Liquidity rebates are small rebates from exchanges that are given to investors upon execution of their limit orders because they have contributed to stock liquidity.[24] HFT traders can receive these rebates by engaging in market making activity, and stock exchanges pay them a "rebate" for filling that role.[25] Rebate arbitrage involves high frequency traders attempting to get liquidity rebates without actually engaging in liquidity-enhancing activity.[26]

Slow Market Arbitrage. Some high frequency traders are able to exploit the structure of markets.[27] Stock markets do not adjust instantaneously to price changes.[28] Because HFT moves so quickly, if they are able to predict where the market will move in terms of price in the next millisecond, they can obtain a profit.[29]

Existing Regulatory Scheme–the Need for a Change?

The prevention of market manipulation is a goal of both the Securities Exchange Act of 1934 (SEA) and the Commodity Exchange Act (CEA).[30] The Acts generally prohibit three types of behavior: (1) fraud and misstatements, (2) fictitious trades, and (3) manipulation.

[20] Tom C.W. Lin, *The New Market Manipulation*, 66 EMORY L.J. 1253, 1288–30 (2017).

[21] Heleen Boonen, High Frequency Trading, Electronic Frontrunning and Structural Insider Trading Under the EU Market Abuse Regulation: Need for Reform?, NYU JLB (2017), https://www.nyujlb.org/single-post/2017/11/27/High-Frequency-Trading-Electronic-Frontrunning-and-Structural-Insider-Trading-Under-the-EU-Market-Abuse-Regulation-Need-for-Reform.

[22] *Id.*

[23] Elise Fleischaker, Why Front Running Traders Hurt Fair & Open Markets, NEURENSIC (2016), https://neurensic.com/front-running-traders-hurt-fair-open-markets/.

[24] UNDERSTANDING HIGH-FREQUENCY TRADING TERMINOLOGY, INVESTOPEDIA, https://www.investopedia.com/articles/active-trading/042414/youd-better-know-your-highfrequency-trading-terminology.asp (last updated May 30, 2019).

[25] *Id.*

[26] *Id.*

[27] *Id.*

[28] *Id.*

[29] *Id.*

[30] *See* 7 U.S.C. § 6c; 15 U.S.C. § 78j. The focus of your inquiry should be on manipulation in the national securities exchanges and not, for example, manipulation in tender offers and the OTC markets, which are also statutorily prohibited.

Fraud and Misstatements

Section 10(b) of the SEA grants the Securities and Exchange Commission (SEC) broad authority to prohibit "manipulative and deceptive devices and contrivances" in relation to the purchase or sale of a security.[31] The SEC's corresponding Rule 10b-5 prohibits fraud, deception, and material misstatements.[32] For claims under section 10(b) and Rule 10b-5, the plaintiff must show that "(1) the defendant made a material misstatement or omission or used a fraudulent device, (2) she did so with scienter (that is, intent), (3) her conduct was related to the purchase or sale of a security, (4) the plaintiff relied on the misstatement, and (5) the plaintiff was harmed."[33]

Congress granted the Commodities Futures Trading Commission (CFTC) the authority to prohibit fraud-based manipulation in 2010 under section 6(c)(1) of the CEA and Rule 180.1.[34] The statute and rule are almost identical to section 10(b) and Rule 10b-5.[35] They prohibit the same conduct, signaling that the CFTC has incorporated Rule 10b-5 jurisprudence with its Rule 180.1.[36]

Fictitious Trades

Fictitious trades increase the volume of trading occurring on exchanges with no change in the ownership of the underlying assets. Examples include wash sales, matched orders, and layering/spoofing. Section 9(a)(1) of the SEA and section 4c(a)(1) of the CEA prohibit trades that don't result in a change in ownership. The CFTC statute specifically prohibits spoofing; the SEC brings those cases under Sections 9 and 10 of the SEA.[37]

Manipulation

Price manipulation is prohibited in Section 9(a)(2) of the SEA.[38] It forbids transactions in exchange-listed securities whose purpose it is to affect the price of a security in order to induce others to buy the security.[39] Section 6(c)(3) of the CEA also prohibits manipulation of the price of a commodity or swap.[40]

[31] 15 U.S.C. § 78j. Congress created the SEC in 1934 in order to regulate the securities markets. James Chen, *Securities and Exchange Commission (SEC)*, INVESTOPEDIA, https://www.investopedia.com/terms/s/sec.asp (last updated May 14, 2019). "The SEC promotes full public disclosure, protects investors against fraudulent and manipulative practices in the market, and monitors corporate takeover actions in the United States." *Id.*

[32] *See* 17 C.F.R. § 240.10b-5 (2018).

[33] *See* Gina-Gail S. Fletcher, Legitimate Yet Manipulative: The Conundrum of Open-Market Manipulation, 68 DUKE L. J. 479, 498 (2018).

[34] *Id.* Congress created the CFTC in 1974 in order to regulate commodity futures and options markets. James Chen, *Commodity Futures Trading Commission (CFTC)*, INVESTOPEDIA, https://www.investopedia.com/terms/c/cftc.asp (last updated Apr. 9, 2019). Its goals include the promotion of competitive and efficient futures markets and the protection of investors against manipulation, abusive trade practices, and fraud. *Id.*

[35] Fletcher, *supra* note 37.

[36] *Id.* at 498–99.

[37] Spoofing is the process by which a trader places a large order for an asset, without the intention of executing, thereby artificially increasing demand for the asset. *See What Is Spoofing?*, FXCM, https://www.fxcm.com/markets/insights/what-is-spoofing/#:~:text=Spoofing%20is%20an%20illegal%20form,high%20demand%20for%20the%20asset (last visited June 14, 2020).

[38] Section 9(a)(2) [15 U.S.C. 78i(a)(2)] states:

"It shall be unlawful for any person, directly or indirectly, by the use of the mails or any means or instrumentality of interstate commerce, or of any facility of any national securities exchange, or any member of a national securities exchange…[t]o effect, alone or with 1 or more other persons, a series of transactions in any security registered on a national securities exchange, any security not so registered, or in connection with any security-based swap or security-based swap agreement with respect to such security creating actual or apparent active trading in such security, or raising or depressing the price of such security, for the purpose of inducing the purchase or sale of such security by others.".

[39] Fletcher, *supra* note 37, at 500.

[40] 7 U.S.C. § 9

To successfully allege price manipulation against a defendant under the SEA, the plaintiff must prove that "(1) the defendant possessed an ability to influence market prices; (2) an artificial price existed; (3) the defendant caused the artificial price; and (4) the defendant specifically intended to cause the artificial price."[41] Specific intent requires that the defendant has "acted (or failed to act) with the purpose or conscious object of causing or effecting a price or price trend in the market that did not reflect the legitimate forces of supply and demand."[42]

Manipulation can harm the market in two ways—"[f]irst, it undermines the market's efficiency by distorting its pricing mechanisms. Second, it impairs the market's integrity because the conduct can lead other market participants to believe the market is unfair."[43] The Supreme Court and the SEC have defined manipulation with a focus on the manipulative intent of the actor. This poses issues for legal actions which involve making trading decisions based on AI technology, such as algorithmic trading/HFT, where it can be difficult to prove an individual's intent.

We would like you to explore whether the Commission should adopt a rule under Section 10(b) of the Exchange Act or change its enforcement/litigation strategies to prohibit manipulation in cases where algorithmic trading or other computerized transactions were utilized and harmful actions were employed.

As you know, the Division of Trading and Markets has been working on issues relating to algorithmic trading and HFT. They have explored various solutions, including minimum resting times and order-to-execution ratios. Discussions of various solutions are included in the Appendix. However, your inquiry is more narrow and should focus on whether the definition of manipulation should change in order to meet challenges posed by these new technologies.

The remainder of this memorandum summarizes the approaches taken thus far by regulators (including the SEC) and approaches suggested by scholars which incorporate intent in some manner. Those approaches would likely be insufficient to catch the harms that can occur through algorithmic trading because of the difficulty of proving traditional intent to engage in manipulation on the part of a computer/algorithm. Also included are appendices with more information that would be helpful to an analysis on this subject. Lastly, I have listed a set of questions you should address below.

Intent-Based Approaches

The Supreme Court and the SEC have adopted an approach to manipulation which focuses principally on whether the intent of the actor was manipulative. In *Ernst & Ernst v. Hochfelder*, the Court stated that manipulation "connotes intentional or willful conduct designed to deceive or defraud investors by controlling or artificially affecting the price of securities."[44] The SEC argued in its *amicus curiae* brief that nothing in Section 10(b) of the Exchange Act "limits its operation to knowing or intentional practices."[45] The SEC also reasoned that "since the 'effect' upon investors of given conduct is the same

[41] Fletcher, *supra* note 37, at 501.

[42] 15 U.S.C. § 78i(a)(2).

[43] Fletcher, *supra* note 37, at 489.

[44] Ernst & Ernst v. Hochfelder, 425 U.S. 185, 186 (1976).

[45] *Id.* at 197–98.

regardless of whether the conduct is negligent or intentional, Congress must have intended to bar all such practices and not just those done knowingly or intentionally."[46] The Court rejected this argument, stating that the Commission must not have realized that their desired approach would logically lead to imposing liability on actors for conduct that was "faultless," something that there is no way the Commission would want.[47] The Court ruled that investors in a fraudulent securities scheme perpetrated by a company were not entitled to damages under 10b-5 from the company's accounting firm because they had only alleged that the accounting firm *negligently* failed to conduct proper audits of the company.[48]

By 1984, the SEC was on board with an intent-based approach. In that year, the CFTC, Federal Reserve, and the SEC stated that intent was an essential element for all market manipulation claims.[49] One year later, in *Santa Fe Industries v. Green*, the Supreme Court stated that "'Manipulation' is virtually a term of art when used in connection with securities markets, and refers generally to practices, such as wash sales, matched orders or rigged prices, that are intended to mislead investors by artificially affecting market activity."[50] The Court held that "[m]ere instances of corporate mismanagement in which essence of the complaint is that shareholders were treated unfairly by a fiduciary" is neither deceptive nor manipulative and thus did not violate SEC Rule 10b-5 or the Securities Exchange Act provision.[51]

The D.C. Circuit also takes an approach to manipulation that relies principally on the manipulative intent of the actor. In *Markowski v. S.E.C.*, the United States Court of Appeals for the D.C. Circuit stated that "manipulation can be illegal solely because of the actor's purpose."[52] The Court reasoned that Section 9(a)(2) of the Exchange Act is "quite separate from the subsections of § 9 prohibiting manipulation through fraudulent devices such as wash sales, 15 U.S.C. § 78i(a)(1)(A), matched sales, *id.* at § 78i(a)(1)(B)-(C), and false statements, *id.* at § 78i(a)(4)" and thus Congress must have wanted to enable manipulation to turn solely on the actor's intent.[53] Analyzing transactions that do not involve fictitious trades, the court said, is difficult because "[w]ithout such transactions, the core of the offense can be obscure."[54] Specifically, "[i]t may be hard to separate a 'manipulative' investor from one who is simply over–enthusiastic, a true believer in the object of investment."[55] Thus, "illegality would thus depend entirely on whether the investor's intent was "an investment purpose" or "solely to affect the price of [the] security."[56]

[46] *Id.* at 198.

[47] *Id.* ("The logic of this effect-oriented approach would impose liability for wholly faultless conduct where such conduct results in harm to investors, a result the Commission would be unlikely to support.").

[48] *Id.* at 215.

[49] Lin, *supra* note 20, at 1301 (citing H.R Comm. of Agriculture, 98th Congress, A Study Of The Effects On The Economy Of Trading In Futures And Options (Comm. Print 1985) (A report by the Bd. of Gov. of Fed. Res., Comm. Futures Trading Comm., and Sec. & Exch. Comm., to the H.R. Comm. on Agriculture and the H.R. Comm. on Energy & Fin., and to the S. Comm. on Ag., Nutrition and Forestry and the S. Comm. on Bkg., pursuant to Section 23(a) of the Commodity Exchange Act, as amended (Dec. 1984)).

[50] Santa Fe Indus., Inc. v. Green, 430 U.S. 462, 97 (1977).

[51] *Id.* at 474–75.

[52] Markowski v. S.E.C., 274 F.3d 525, 529 (D.C. Cir. 2001).

[53] *Id.*

[54] *Id.* at 528.

[55] *Id.*

[56] *Id.*

Not everyone agrees with the *Markowski* decision. Gina-Gail S. Fletcher looked to *United States v. Markowski* as an example of why an analysis of intent is insufficient.[57] Fletcher commented that "[a]lthough the court's holding feels correct given the havoc the defendants wreaked on the market, it is disconcerting that the sole stated basis for liability was the defendants' manipulative intent."[58]

Nonetheless, the Second Circuit agrees with the D.C. Circuit. In *Fezzani v. Bear, Stearns & Co.*, the court clarified that manipulation under § 10(b) "[does] not require that reliance by a victim on direct oral or written communications by a defendant must be shown in every manipulation case."[59] The court also stated that it "agree[s] with the propositions of law asserted by the SEC that, in a manipulation claim, a showing of reliance may be based on 'market activity' intended to mislead investors by sending 'a false pricing signal to the market,' upon which victims of the manipulation rely."[60] The court ultimately held there was no manipulation involved in *Fezzani*, because "[t]here is no…reliance based on any identifiable market, and—given the lack of an allegation that any plaintiff knew of the stock parking or prices used therein—no allegation of reliance upon the parking transactions."[61]

Some courts recognize that it is difficult to make conclusions about intent on its own, because it is a subjective element. Therefore, they may look to the conduct of the defendant in order to find support for a claim of manipulative intent. For example, in granting partial summary judgment, the Court in *S.E.C. v. Masri* explicitly stated that "[t]he defendant's manipulative intent can be inferred from the conduct itself."[62] A recent decision on this issue is *S.E.C v. Lek Securities Corp.*, where the court held that, if the SEC properly showed that the defendants engaged in conduct that artificially raised prices, the court could hold that they violated the Securities and Exchange Act and thus fulfilled the intent requirement.[63]

Fischel/Ross/Easterbrook Approaches

In a famous article, Daniel Fischel and David Ross argued that "the concept of manipulation should be abandoned all together."[64] Specifically, "[f]ictitious trades should be analyzed as a species of fraud. Actual trades should not be prohibited as manipulative regardless of the intent of the trader."[65] The authors analyzed the case of *United States v. Mulheren* to demonstrate that "manipulative trades cannot be distinguished from non-manipulative trades without reference to the intent of the trader…[and]…the observable characteristics of trades cannot distinguish trades made with bad intent from trades made with good intent."[66]

[57] Fletcher, *supra* note 33, at 509.

[58] *Id.* at 510.

[59] Fezzani v. Bear, Stearns & Co. Inc., 777 F.3d 566, 571 (2d Cir. 2015).

[60] *Id.* at 571–72.

[61] *Id.* at 574.

[62] S.E.C. v. Masri, 523 F.Supp. 2d 361, 367 (S.D.N.Y. 2007).

[63] U.S. SECURITIES AND EXCHANGE COMMISSION, *Court Denies Broker's Attempt to Dismiss Market Manipulation Claims* (Aug. 29, 2017), https://www.sec.gov/litigation/litreleases/2017/lr23923.htm.

[64] Daniel R. Fischel and David J. Ross, *Should the Law Prohibit 'Manipulation' in Financial Markets?*, 105 HARV. L. R. 503, 507 (1991), https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1554&context=journal_articles.

[65] *Id.*

[66] *Id.* at 533.

In that case, defendant Mulheren—who served as the chief trader and general partner of Jamie Securities Co.—was indicted and convicted for manipulating Gulf & Western Industries, Ind. (G&W) stock.[67] The conviction was reversed on appeal in the Second Circuit.[68] Arbitrageur Ivan Boesky owned an "enormous block" of stock in G&W, and the government alleged that Mulheren, through Jamie, sought to raise the price of G&W stock, as a favor to Boesky, above $45 per share so that Boesky could sell his shares "back to the company at that price."[69]

Boesky testified that he called Mulheren and told him that while he "liked" G&W stock he "would not pay more than 45 [dollars] for it" and "it would be great if it traded at 45."[70] Mulheren replied, "I understand."[71] Jamie then bought 50,000 shares of G&W stock at market price, and the order was fulfilled at prices that were below $45 per share.[72] Shortly after that, Jamie placed another order for 25,000 shares of G&W and all shares were purchased at $45 per share. Then, Boesky sold his stock back to G&W at $45 per share, and at the end of the day Jamie sold its position, incurring a loss.[73] The Second Circuit stated that "[t]he meaning of this cryptic conversation is, at best, ambiguous, and we reject the government's contention that this conversation 'clearly conveyed Boesky's request that the price of the stock be pushed up to $45...[and Mulheren's] agreement to help.'"[74] The Circuit also concluded that while Mulheren's actions could be consistent with him having manipulative intent, they were also consistent with the theory that Mulheren had investment intent.[75] Accordingly, Fischel and Ross argue that analyzing actions for manipulative intent is ambiguous because sorting out good intent from bad intent is too difficult.

The authors also argue that "there is no compelling reason to be concerned about [actors trading with manipulative intent] because it is likely to be self-deterring."[76] This is because of the "low probability that trade-based manipulations can succeed" due to it being difficult for an actor to exert price changes on a security.[77] The authors point out that the latter point is especially prominent in futures markets, where "acquisition of market power requires a large amount of capital" and "for some commodities, such as Treasury securities, this is likely impossible."[78] It would therefore be difficult to acquire enough market power to manipulate the futures market.

Frank Easterbrook took a different approach, and argued that manipulation should be defined as conduct in which profit flows solely from the trader's ability to conceal his position from other traders and the trades do not move prices more quickly in the direction that reflects long-run conditions of supply and demand.[79] Fischel and Ross disagree, stating that the definition is "unsatisfactory…[W]hat happens if the trades move prices in one direction because the trader genuinely believes that prices will move in this

[67] United States v. Mulheren, 938 F.2d 364 (2d Cir. 1991).

[68] *Id.* at 372.

[69] *Id.* at 365-66.

[70] *Id.* at 367; Fischel, *supra* note 69, at 533.

[71] *Mulheren*, 938 F.2d at 367.

[72] *Id.*

[73] *Id.* at 368.

[74] *Id.* at 369.

[75] *Id.* at 372.

[76] Fischel, *supra* note 69, at 553.

[77] *Id.* at 506, 514.

[78] *Id.* at 547.

[79] Frank H. Easterbrook, Monopoly, Manipulation, and the Regulation of Futures Markets, 59 J. BUS. S103–06 (1986).

direction, but the trader turns out wrong and prices ultimately move in the opposite direction? Trading based on a genuine belief that prices will ultimately move in the direction of the trades is the essence of non-manipulative trading."[80]

Professor Wendy Collins Perdue also disagreed with Easterbrook. She stated that his approach suffers "from many…practical problems…, including the problems of determining 'conditions of supply and demand' and defining the 'long-run.'"[81] Additionally, "in attempting to ascertain the motivation for a trader's desire for secrecy, many courts likely will find themselves lost in a standardless examination of intent."[82] She proposed a definition of manipulation as conduct that is "uneconomical or irrational," regardless of the effect on price.[83]

Intent and Unlawful Conduct/Harm Approaches

Various definitions of manipulation revolve around the actor's intent and the conduct's harm on the marketplace or its unlawfulness. Fletcher argues that the approach of the SEC and CFTC—that transactions are manipulative if the trader intends to manipulate the market—is "fundamentally flawed" because "[t]raders may be treated differently for the same conduct under this approach, and it leaves market actors none the wiser as to when their conduct may be considered manipulative."[84] She argues that "only those open-market transactions that impede the markets' efficiency and undermine their integrity should be deemed manipulative."[85]

Open-market manipulation involves no objectively bad acts and is executed through otherwise lawful transactions on the open market.[86] Additionally, while "[a] defendant's intent is salient to demonstrating the purposefulness of her actions…, intent is inadequate as an explanation of why otherwise legitimate transactions are manipulative."[87]

Fletcher proposes a definition that still includes the element of intent. She states that "[a] trader's manipulative intent is important in proving that her conduct was not accidental or negligent and, as such, that the trader is blameworthy."[88] But intent is not the only element (as there needs to be some harm to the market under her definition) because "[a]n exclusive focus on manipulative intent conflates scienter with misconduct."[89]

The Third Circuit has adopted the approach of looking to an actor's intent and unlawful conduct as the test for manipulation. In *GFL Advantage Fund, Ltd. v. Colkitt*, the court stated that "[r]egardless of whether market manipulation is achieved through deceptive trading activities or deceptive statements as to the issuing corporation's value, it is clear that the essential element of the claim is that inaccurate

[80] Fischel, *supra* note 69, at 509.

[81] Wendy Collins Perdue, *Manipulation of Futures Markets: Redefining the Offense*, 56 FORDHAM L.R 345, 388 (1987).

[82] *Id.*

[83] *Id.* at 348.

[84] Fletcher, *supra* note 37, at 479.

[85] *Id.*

[86] *Id.* at 501–02.

[87] *Id.* at 510.

[88] *Id.* at 517.

[89] *Id.* at 518.

information is being injected into the marketplace." Thus, trading for the purpose (*i.e.*, with the intent) of moving a security's price is not enough to be considered an injection of inaccurate information in the marketplace, and hence it is not, by itself, manipulation. In the case, the court ruled that because "Colkitt has not presented any evidence that GFL did anything but lawfully engage in short sales of National Medical and EquiMed stock," Colkitt's claim of market manipulation fails.[90] Thus, there is currently a split among the federal circuits regarding whether lawful trading activity, without some further unlawful act, can be considered manipulation.

Questions

Your briefing with the Chair of the SEC will help her to decide whether to address the rise of new technologies like algorithmic trading and HFT and their potential for market manipulation. If you conclude that the SEC must take steps to address potential manipulation through using new technologies, be sure to explain whether the SEC should change its enforcement/litigation strategies or engage in rulemaking/enact guidance. When doing so, address President Trump's recent Executive Orders regarding guidance documents and Supreme Court precedent regarding fair notice, which are included in the Appendix. The Chair would like to be on board with the Trump Administration and not run afoul of the Executive Orders or Supreme Court precedent.

Please review the materials included in the attached Appendix and brief the incoming Chair. In particular, she is eager to hear your thoughts on the following topics:

- What is market manipulation?
- What are the principal new technological trading strategies?
- To what extent do the principal new technological trading strategies pose problems for the existing doctrine of market manipulation?
- What approaches have scholars and others proposed that define manipulation in terms that do not place emphasis on manipulative intent?
- How should the SEC respond to the problems posed by these new technological trading strategies? Specifically, should the SEC:
    - Keep the traditional rule; or
    - Adjust the traditional rule.
- If you think that the SEC should adjust the traditional rule, should this be done by rulemaking/guidance or by adjusting enforcement and/or litigation strategies? Why?
- If you believe that the SEC should step in with a rule promulgation/guidance, what should the rule/guidance say?
- To what extent would structural reforms be a viable option, vis-à-vis adjusting the definition of manipulation?

[90] GFL Advantage Fund, Ltd. v. Colkitt, 272 F.3d 189, 207 (3d Cir. 2001).

Appendices

Background

1. James Chen, *Algorithmic Trading*, Investopedia. https://www.investopedia.com/terms/a/algorithmictrading.asp (updated Oct. 15, 2019)
2. James Chen, *High-Frequency Trading (HFT)*, Investopedia. https://www.investopedia.com/terms/h/high-frequency-trading.asp (updated Oct. 10, 2019)

Economic Perspectives on Algorithmic/HFT

3. Joel Hasbrouck & Gideon Saar, *Low-latency trading*, 16 Jour. of Fin. Mkts. 646, 646–47 (May 232, 2013). http://people.stern.nyu.edu/jhasbrou/Research/lowLatencyTrading/lowLatencyTradingHasbrouckSaarJFM.pdf
4. Jonathan Brogaard, Terrence Hendershott and Ryan Riordan, *High-Frequency Trading and Price Discovery*, 27 Rev. of Fin. Studies 2267 (Aug. 2014). https://doi.org/10.1093/rfs/hhu032

Potential Problems Stemming from Algorithmic Trading

5. Ashley Chorpenning, *Flash Crash: Definition, Examples, and Implications*, Yahoo Finance (Nov. 6, 2019). https://finance.yahoo.com/news/flash-crash-definition-examples-implications-002607954.html
6. Ravi Kant, *Why algorithmic trading is dangerous*, Asia Times (May 8, 2019). https://www.asiatimes.com/2019/05/opinion/why-algorithmic-trading-is-dangerous/

The Question of Intent in Manipulation Doctrine

7. Daniel R. Fischel & David J. Ross, *Should the Law Prohibit 'Manipulation' in Financial Markets?*, 105 Harv. L. R. 503 (1991). https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1554&context=journal_articles
8. Frank H. Easterbrook, *Monopoly, Manipulation, and the Regulation of Futures Markets*, 59 J. Bus. S103–06 (1986).
9. Gregory Scopino, *Do Automated Trading Systems Dream of Manipulating the Price of Futures Contracts? Policing Markets for Improper Trading Practices by Algorithmic Robots*, 67 Fla. L. Rev. 221 (2016). https://scholarship.law.ufl.edu/cgi/viewcontent.cgi?article=1223&context=flr
10. Yesha Yadav, *The Failure of Liability in Modern Markets*, 102 Va. L. Rev. 1031 (2016). https://www.virginialawreview.org/sites/virginialawreview.org/files/Yadav_Online.pdf

11. Ryan J. Davies & Erik R. Sirri, *The Economics of Trading Markets*, in SECURITIES MARKET ISSUES FOR THE 21ST CENTURY, 145, at 172-173 (Merritt B. Fox et al. eds., 2018)
    https://www.law.columbia.edu/sites/default/files/microsites/capital-markets/securities_market_issues_for_the_21st_century.pdf

Other Possible Approaches for Manipulation Doctrine

12. Tom C.W. Lin, The New Market Manipulation, 66 EMORY L. J. 1253 (2017).
13. Merritt B. Fox & Kevin S. Haeberle, Evaluating Stock-Trading Practices and Their Regulation, 42 J. Corp. L. 887, 887 (2017).
14. Fox, Lawrence R. Glosten & Gabriel V. Rauterberg, *Stock Market Manipulation and Its Regulation*, 35 YALE J. ON REG. 67 (2018).
    https://digitalcommons.law.yale.edu/yjreg/vol35/iss1/2/
15. Matthijs Nelemans, *Redefining Trade-Based Market Manipulation*, 42 VAL. U. L. REV. 1169 (2008).
    https://scholar.valpo.edu/vulr/vol42/iss4/4/
16. Donald C. Langevoort, *Taming the Animal Spirits of the Stock Markets: A Behavioral Approach to Securities Regulation*, 97 NW. U. L. Rev. 135 (2002).
    https://heinonline.org/HOL/LandingPage?handle=hein.journals/illlr97&div=9&id=&page=
17. Gina-Gail S. Fletcher, *Legitimate Yet Manipulative: The Conundrum of Open-Market Manipulation*, 68 DUKE L. J. 479 (2018).
    https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=3959&context=dlj

Rulemaking vs. Changing Enforcement Strategies

18. Dale Brown, *It's time to end 'rulemaking by enforcement'*, INVESTMENT NEWS (July 29, 2019)
    https://www.investmentnews.com/its-time-to-end-rulemaking-by-enforcement-80618
19. President Trump's Executive Orders:
    a. Background:
        i. Keith Bradley & Darin J. Smith, Administrative Law Corner: The End of Federal Agency Guidance as We Know It? Not So Fast., Nat. L. Rev. (Nov. 27, 2019). https://www.natlawreview.com/article/administrative-law-corner-end-federal-agency-guidance-we-know-it-not-so-fast
    b. The orders:
        i. Exec. Order 13891 84 F.R. 55235 (2019).
           https://www.federalregister.gov/documents/2019/10/15/2019-22623/promoting-the-rule-of-law-through-improved-agency-guidance-documents
        ii. Exec. Order 13892 84 F.R. 55239 (2019).
           https://www.federalregister.gov/documents/2019/10/15/2019-

22624/promoting-the-rule-of-law-through-transparency-and-fairness-in-civil-administrative-enforcement-and

c. Supreme Court Precedent Regarding Fair Notice:

i. Christopher v. SmithKline Beecham Corp., 567 U.S. 142 (2012).

ii. Fox I - F.C.C. v. Fox Television Stations, Inc., 556 U.S. 502, 515 (2009).

iii. Fox II - F.C.C. v. Fox Television Stations, Inc., 567 U.S. 239, 132 (2012).

20. S.E.C., *Rulemaking, How It Works*, U.S. SEC. & EXCH. COMM. https://www.sec.gov/fast-answers/answersrulemakinghtm.html (last visited Mar. 24, 2020).

Optional Material: Other Ways to Regulate New Technologies

21. Michael Morelli, Implementing High Frequency Trading Regulation: A Critical Analysis of Current Reforms, 6 MICH. BUS. & ENTREPRENEURIAL L. REV. 201 (2017). https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1059&context=mbelr

HARVARD LAW SCHOOL | The Case Studies

CSP050
MAY 2020

Algorithmic Trading Strategies

ANZHELIKA ISHKHANYAN AND ASHER TRANGLE

Memorandum

DATE: January 9, 2020
TO: Special Counsel, CFTC Division of Market Oversight
FROM: Director, CFTC Division of Market Oversight
RE: Algorithmic Trading and Regulation Automated Trading

Welcome to DMO. I'm confident that you'll find the position a challenging one, and I've already got a meaty topic to get you started on.

I recently received an email from the Chairman expressing his concerns regarding the negative effects of algorithmic trading on financial markets. The Chairman is convinced that the CFTC should have direct access to trading systems' source code to prevent potential market abuses with systemic implications. To that end, the Chairman proposes we reconsider Regulation Automated Trading ("Regulation AT") which would require all traders using algorithms to register with the CFTC and would give CFTC direct and unfettered access to their source code. Please find attached the Chairman's email which outlines his priorities and main concerns pertaining to algorithmic trading. In addition, I have sketched out my own reactions to reconsidering Regulation AT in an informal memo, attached as Appendix I. In addition, you may find it useful to refer to a legal intern's memoranda, attached as Appendix II, which offers a brief overview of Regulation AT, its history, and a short discussion of other regulators' efforts to address algorithmic trading.

After considering these materials, please come and brief me on the following questions:

- What, precisely, are the public policy challenges posed by the emergence of algorithmic trading, and does this practice pose any serious problems to U.S. capital markets?
- To what extent are there legal or policy problems with implementing a regime of the sort contemplated in the revised version of Regulation AT?

Written by Anzhelika Ishkhanyan and Asher Trangle under the supervision of Howell E. Jackson, James S. Reid, Jr., Professor of Law at Harvard Law School. Case development at Harvard Law School is partially funded by a grant from Dechert LLP. Cases are developed solely as the basis for class discussion. They are not intended to serve as endorsements, sources of primary data, legal advice, or illustrations of effective or ineffective management.

Copyright © 2020 President and Fellows of Harvard University. No part of this publication may be reproduced, stored in a retrieval system, used in a spreadsheet, or transmitted in any form or by any means—electronic, mechanical, photocopying, recording, or otherwise—without permission. To order copies or permissions to reproduce materials please visit our website at casestudies.law.harvard.edu or contact us by phone at 617-496-1316, by mail at Harvard Law School Case Studies Program, 1545 Massachusetts Avenue – Areeda 507, Cambridge, MA 02138, or by email at HLSCaseStudies@law.harvard.edu.

- If the Commission chooses to take up the issue of direct access to source code as the Chairman seems to want, are there other approaches to the issue that might be preferable to the approach that the revised Regulation AT contemplated?

In answering the above questions, please focus your presentation on potential reform proposals. Specifically, the presentation should indicate how a proposal (or aspects of a proposal) address or solve (at least some of) the issues raised in the materials below.

In preparing for the briefing, please make sure that you examine the supplemental materials that my other DMO staff members have gathered on the topic, attached as Appendices III – XII, which should provide both useful background as well as more tendentious perspectives from a variety of interested parties. Appendix II contains some information pertaining to the ways in which other actors have sought to address the problems raised by HFT and algorithmic trading. Appendix VI also addresses these alternative proposals in sections IV(B) and IV(C). When answering the questions framed above, please bear in mind that there may be overlapping or different concerns raised by the Chairman, the legal intern, and me. Please address the concerns raised by the incoming Chairman in the detailed email below. I think that you will find that all three of these documents may raise important implications for your analysis.

CFTC Chairman Smith Email

DATE: April 12, 2019

TO: Director, CFTC Division of Market Oversight

FROM: CFTC Chairman

RE: Algorithmic Trading – Reviving Regulation Automated Trading

Dear DMO Director:

I am writing to request your advice on the possibility of reviving plans to regulate algorithmic trading. In 2015, the CFTC proposed Regulation Automated Trading ("Regulation AT") largely as a regulatory response to the events of May 6, 2010, better known as the *Flash Crash*.[1] As you know, during this event, the use of an automated trading algorithm caused major U.S. equity indices to plummet 5 to 6% and rebound almost instantly.[2] Due to a lack of visibility in the market, it took the CFTC and SEC four months to identify potential causes of this market failure that took a mere 20 minutes to unfold.[3] Both the reasons for this incident and the identity of those responsible remain highly contested.[4] This investigation formed part of the basis for Regulation AT. A key component of the proposed rule would require automated trading firms to allow the CFTC to inspect the source code of these trading algorithms. However, due to its controversial nature and industry pushback, the CFTC subsequently abandoned Regulation AT. Then Commissioner Brian Quintenz famously pronounced Regulation AT "D-E-A-D."[5]

To me, the most critical component of Regulation AT pertains to gaining access to the relevant source code. However, regardless, I believe that the subsequent failure of the CFTC to regulate automated trading in any capacity was a mistake. I still have grave concerns over the nature and use of automated trading, which I have briefly sketched out below:

Main Concerns Regarding Algorithmic Trading

Market Stability

A chief concern is the effect of algorithmic trading on market stability. The 2010 Flash Crash showcased how rapid algorithmic trading can quickly lead to a widespread destabilization of the market. It turns out that the Flash Crash was not an isolated incident. Since then there have been thousands of

[1] *CFTC Unanimously Approves Proposed Rule on Automated Trading*, U.S. Commodity Futures Trading Commission (Nov. 24, 2015), https://www.cftc.gov/PressRoom/PressReleases/pr7283-15 [https://perma.cc/R5R5-LCRV].

[2] Jill Treanor, *The 2010 "flash crash": how it unfolded,* THE GUARDIAN (April 22, 2015), https://www.theguardian.com/business/2015/apr/22/2010-flash-crash-new-york-stock-exchange-unfolded; Report of the Staffs of the CFTC and SEC to the Joint Advisory Committee on Emerging Regulatory Issues, *Findings Regarding the Market Events of May 6, 2010*, 104 (2010).

[3] Dave Michaels et al., *Flash Crash Arrest Shows Lack Of Market Regulation*, AUSTRALIAN FINANCIAL REVIEW (Apr. 23, 2015), https://www.afr.com/markets/equity-markets/flash-crash-arrest-shows-lack-of-market-regulation-20150423-1mrayk [https://perma.cc/42R4-T3SB].

[4] Matt Levine, *Guy Trading at Home Caused the Flash Crash*, BLOOMBERG (Apr. 21, 2015), https://www.bloomberg.com/opinion/articles/2015-04-21/guy-trading-at-home-caused-the-flash-crash.

[5] *CFTC commissioner: plans to seize algo trading source code are "D-E-A-D",* FINEXTRA RESEARCH (Oct. 5, 2017), https://www.finextra.com/newsarticle/31157/cftc-commissioner-plans-to-seize-algo-trading-source-code-are-d-e-a-d [https://perma.cc/UV8D-6H89].

flash crashes, some of which have considerably disrupted the market.[6] These flash crashes have mostly been attributed to or said to have been exacerbated by algorithmic trading.[7] Furthermore, many highly reputable market analysts and financial regulators (including the Bank of England)[8] have warned that further market crashes are likely.[9] More troubling, these reports warn that if a flash crash were to occur during a recession (heretofore all flash crashes have taken place during favorable economic conditions), the negative impact would be greatly multiplied and could lead to a serious liquidity crisis.

I believe that there are two issues at the root of the threat to market stability. The first issue is the near-instantaneous nature of algorithmic trades. Algorithms are programmed to perform thousands of trades in mere seconds, and the smallest error in the programming language of an algorithm can cause major market disruptions. These disruptions can cause catastrophic damage to the financial system and investors may suffer huge losses before intervention is possible. Temple Law School Professor Tom Lin has described the resulting systemic risk as "too fast to save."[10]

The second issue stems from the linked or connected nature of modern markets. Some argue that electronic trading has greatly exacerbated the interconnectedness of markets. Given the new forms of market interconnectedness,[11] these disruptions are liable to have ripple effects and cause market distress.[12] For example, one false tweet regarding explosions in the White House caused algorithms linked to social media to begin executing certain trades. This one incident caused the S&P 500 Index to lose more than $135 billion of value in mere seconds following the post.[13] Both the speed of algorithmic trading and the linked nature of financial markets demonstrate how algorithmic trading can have negative effects on overall market stability.

[6] Jean-Philippe Serbera, *Flash crashes: if reforms aren't ramped up, the next one could spell global disaster*, THE CONVERSATION (JAN. 7, 2019) https://theconversation.com/flash-crahttpsshes-if-reforms-arent-ramped-up-the-next-one-could-spell-global-disaster-109362 [https://perma.cc/6TF8-ETTK] (giving an overview of flash crashes which have occurred since 2010).

[7] Michelle Fox, *SEC "has" to investigate Christmas Eve sell-off, says ex-SEC attorney*, CNBC (Jan. 24, 2019), https://www.cnbc.com/2019/01/24/sec-has-to-investigate-christmas-eve-sell-off-says-ex-sec-attorney.html [https://perma.cc/Z2KM-LETV] (blaming HFT for 2018 Christmas Eve crash); Wayne Cole & Swati Pandey, *Japanese Yen Soars As "Flash Crash" Sweeps Currency Market*, REUTERS (Jan. 2, 2019), https://www.reuters.com/article/us-markets-forex/japanese-yen-soars-as-flash-crash-sweeps-currency-market-idUSKCN1OW1UH [https://perma.cc/M53V-WPS2](Algorithms said to have exacerbated the flash crash of the yen); GIOVANNI CESPA & XAVIER VIVES, HIGH FREQUENCY TRADING AND FRAGILITY, ECB WORKING PAPER (2017), https://www.ecb.europa.eu/pub/pdf/scpwps/ecbwp2020.en.pdf?f0853c8630ef920d9429e31ff85b2682; Netty Ismail & Lukanyo Mnyanda, *Pound's Flash Crash Has Traders Blaming Algos for Selling Frenzy,* BLOOMBERG BRIEFS (Oct. 07, 2016), https://www.bloomberg.com/professional/blog/pounds-flash-crash/ (algorithms blamed for British Pound Crash).

[8] Patrick Graham, *UPDATE 1-Bank Of England's Salmon Says Brace For Further Flash Crashes*, REUTERS (Jan. 24, 2017) https://www.reuters.com/article/britain-boe-flashcrash/update-1-bank-of-englands-salmon-says-brace-for-further-flash-crashes-idUSL5N1FE6IF [https://perma.cc/KQ2T-97GA].

[9] Thomas Heath, *The Warning From JPMorgan About Flash Crashes Ahead*, THE WASHINGTON POST (Sept. 5, 2018), https://www.washingtonpost.com/business/economy/the-warning-from-jpmorgan-about-flash-crashes-ahead/2018/09/05/25b1f90a-b148-11e8-a20b-5f4f84429666_story.html?utm_term=.21f78c4f8358 [https://perma.cc/ER85-3GQY].

[10] Tom C.W. Lin, *The New Investor*, 60 UCLA L. REV. 678, 711-14 (2013), https://www.uclalawreview.org/the-new-investor-2/ [https://perma.cc/M4H6-7NUC].

[11] *Id.* at 714.

[12] Dave Michaels, *Machine Trading Needs More Oversight, Departing SEC Official Says*, WALL STREET JOURNAL (December 21, 2018), https://www.wsj.com/articles/machine-trading-needs-more-oversight-departing-sec-official-says-11545404400.

[13] Mark Prigg, The tweet that cost $139 BILLION: Researchers analyse impact of hacked message claiming President Obama had been injured by White House explosion, DAILY MAIL ONLINE (MAY 20, 2015), https://www.dailymail.co.uk/sciencetech/article-3090221/The-tweet-cost-139-BILLION-Researchers-analyse-impact-hacked-message-claiming-President-Obama-injured-White-House-explosion.html [https://perma.cc/2FW6-X2SD].

The potential for information monoculture only enhances these systemic risks. For example, if trading algorithms used by multiple market participants all rely on the same sources of information or contain the same coding or design error (such as the above-mentioned tweet), this could trigger a cascade of erroneous trades. Because artificial intelligence may become embedded in these algorithms, there is also a risk that independently developed algorithms may "learn" to perform the same trading strategy. A number of algorithms engaged in similar or connected trading would significantly heighten systemic risk.[14]

Market Manipulation and Investor Confidence

Another concern prompting me to reconsider Regulation AT is how algorithmic trading has led to new techniques to manipulate the market and the resulting erosion of investor trust in financial markets. These new forms of manipulative conduct have prompted investors and academics to speculate whether the "market is rigged."[15] A prime example of market manipulation is how high-frequency traders place servers within dark-pool data centers to get information regarding stock orders before other market participants. Once the traders receive information regarding the upcoming purchase, they leverage their superior trading speed to buy the assets in question. Thus, the original purchaser has no other option but to acquire the assets from the high-frequency trader at a premium.[16] This technique is most commonly referred to as "front-running." A further problem is that exchanges actively participate in these practices by charging higher prices for placing servers closer to the exchange system.[17] Other malicious practices include taking advantage of the fragmented nature of the market to perform spoofing,[18] and pinging,[19]which are currently happening on an unprecedented scale.

Market Opacity and Insufficient Information

My third concern is that neither the CFTC nor other U.S. financial regulators have enough visibility into the market.[20] The fallout from the Flash Crash clearly demonstrated how difficult it is for regulators to determine the reasons for a crash or ascribe responsibility to individuated manipulative practices.[21] Part of the difficulty is proving the requisite intent in cases where there might not even be a paper trail to follow (such as a silent change of source code).[22] Indeed, a source of academic debate is whether the

[14] Lin, *supra* note 10, at 25.

[15] Kamal Ahmed, *'The market is rigged' - Michael Lewis*, BBC NEWS (April 10, 2015), https://www.bbc.com/news/business-32246655 [https://perma.cc/EY64-CVFL].

[16] Jacob Adrian, Informational Inequality: How High Frequency Traders Use Premier Access to Information to Prey on Institutional Investors, 14 TECHNOLOGY REVIEW 24 (2016).

[17] *Id.*

[18] Matthew Leising, *Spoofing*, BLOOMBERG (Jan. 19, 2017), https://www.bloomberg.com/quicktake/spoofing (Citigroup recently fined $25M for spoofing. Spoofing is the practice of asking or bidding then canceling before the order is executed. This creates the illusion that the market is moving. Traders thus benefit from the actual increase in value resulting from market optimism).

[19] Gregory Scopino, *The (Questionable) Legality of High-Speed "Pinging" and "Front Running" in the Futures Market,* 47 CONN. L. REV. 607, 611-2 (2015) (involves placing small orders in the market at different price levels to detect large trading orders and accordingly trade ahead).

[20] Luis A. Aguilar, Commissioner, SEC, Keynote Address at the Georgia Law Review Annual Symposium: Preparing for the Regulatory Challenges of the 21st Century (Mar. 20, 2015) (transcript available at https://www.sec.gov/news/speech/preparing-for-regulatory-challenges-of-21st-century.html [https://perma.cc/EH3Q-6WBC].

[21] Levine, *supra* note 4.

[22] Gregory Scopino, Special Counsel, CFTC, Remarks at the 23rd Annual Financial Markets Conference: Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies (May 2018) (transcript available at https://www.frbatlanta.org/news/conferences-and-

current regulatory regime is adequate to combat these malicious practices.[23] As markets become increasingly more complex and fragmented, the lack of access to critical data becomes more acute.[24]

The Solution: Reviving Regulation AT

The CFTC is mandated to guard against financial crises and to foster open, transparent, competitive and financially sound markets.[25] The CFTC cannot fulfill its mandate without regulating algorithmic trading and banning manipulative practices. I am committed to providing overdue guidance and regulation on this issue. In addition, I believe that worries over this Regulation's impact on algorithmic trading are overblown. For example, columnist Matt Levine opined that "[t]he thing is, high-frequency trading just isn't that important" and ought not lead to such intense emotional debate.[26]

Furthermore, I fervently believe that this issue cannot be effectively regulated without reserving source code access to the CFTC, and that the source code provisions are the most crucial component of the overall Regulation AT framework. The CFTC needs access to source code in order to accurately and quickly identify algorithmic trading practices that may lead to systemic risk.[27] Access to source code would essentially provide the CFTC with the ability to preempt and possibly even *prevent* flash crashes, as well as more easily reconstruct market events and determine their causes post hoc. I therefore propose that the CFTC reconsider Regulation AT.

events/conferences/2018/0506-financial-markets-conference/transcripts/research-papers/scherer-regulating-artificial-intelligence-systems-risks-challenges-competencies-strategies.aspx [https://perma.cc/EH3Q-6WBC] (describing the difficulty of proving intent given the new possibility of misconduct without a paper trail, save source code).

[23] See Gregory Scopino, Do Automated Trading Systems Dream of Manipulating the Price of Futures Contracts? Policing Markets for Improper Trading Practices by Algorithmic Robots, 67 FLA. L. REV. 221 (2016). See also generally, Tom C.W. Lin, The New Market Manipulation, 66 Emory L.J. 1253 at 1288-90 (2017).

[24] Aguilar, *supra* note 20.

[25] *Mission & Responsibilities*, U.S. COMMODITY FUTURES TRADING COMMISSION, https://www.cftc.gov/About/MissionResponsibilities/index.htm [https://perma.cc/56V8-3LXW] (last visited May 15, 2019).

[26] *See* Matt Levine, *Source Code and Chicken Indexes*, Bloomberg (November 7, 2016), https://www.bloomberg.com/opinion/articles/2016-11-07/source-code-and-chicken-indexes (last visited January 23, 2019).

[27] See Michael Morelli, Regulating Secondary Markets in the High Frequency Age: A Principled and Coordinated Approach, 6 Mich. Bus. & Entrepreneurial L. Rev. 79 (2016).

Appendix I: DMO Director Memorandum

Memorandum

DATE: July 22, 2019

TO: CFTC DMO Staff

FROM: Director, CFTC Division of Market Oversight

RE: Regulation AT Considerations

This memo highlights my concerns with the requirement in Regulation AT that would grant the CFTC direct access to source code. The most important issues that ought to be considered are market manipulation, governmental use of algorithms, governmental oversight issues, constitutionality concerns, beneficial aspects of HFT and cybersecurity.

Market Manipulation

The Chairman mentioned before that investors and academics have highlighted that algorithmic trading has created the potential for new forms of market manipulation. However, I think that this issue is so crucial that I write separately to emphasize that the market impact of manipulative practices must not be underestimated. First, manipulative practices contribute to a shift in asset prices that is unrelated to a change in expectations regarding the future cash flows of the assets. This results in "artificial prices" and inhibits market efficiency.[1] It can also harm market "fairness" as investors find out the true value of the asset when its price is eventually corrected.[2] Second, wary of falling prey to manipulators who are better informed of future price changes, liquidity providers widen their bid-ask spread, heightening transaction costs.[3] This, in turn, deters market participants from trading, which results in decreased market liquidity. Thus, market manipulation negatively affects "both of the market's core social functions—facilitating liquidity and enhancing price accuracy."[4]

Despite near universal agreement that "market manipulation" ought to be outlawed (its codification came in the form of the 1934 Securities Exchange Act)[5], there is no consensus over which practices are "manipulative" based on two main reasons. First, the legal definition of market manipulation is overbroad. Second, it is very difficult in practice to distinguish illegitimate practices from legitimate trading.[6] Because trading in securities, even when it results in an impact on price, is otherwise legitimate, the element that differentiates market manipulation from market trading is a showing of *manipulative*

[1] *See* Merritt B. Fox, Lawrence R. Glosten, & Gabriel V. Rauterberg, *Stock Market Manipulation and Its Regulation*, 35 YALE JOURNAL ON REGULATION 61, 73 (2018).

[2] *Id.*

[3] *Id.* at 102.

[4] *Id.* at 73.

[5] *See* Jerry W. Markham, Law Enforcement and the History of Financial Market Manipulation 53-6 (2015).

[6] *See* Ignacio Orellana Garcia, Market Manipulation in The Age of Machines: An Analysis of Two Trading Strategies (May, 2019) (unpublished LL.M Paper, Harvard Law School) (on file with Harvard University Library system).

intent.[7] However, when trades are facially legitimate, proof of manipulative intent requires nothing less than a "smoking gun,"[8] such as discussion of the strategy in written correspondence. As CFTC Special Counsel Gregory A. Scopino notes, in the age of algorithms where a manipulative strategy is simply programmed into a trading platform, a sufficient paper trail may not exist.[9] Therefore, in many cases, source code itself can become the "smoking gun" regulators need to prove scienter.

Algorithmic trading has introduced a new dimension to this debate. As commenters have noted, high-frequency traders are increasingly using their superior trading speeds to submit orders and cancel them in fractions of a second. These practices can harbor an intent to move the stock price in their desired direction (spoofing) or find out the price point at which market participants are willing to trade (pinging). High frequency traders also harness their speed to trade ahead of known future price changes (front-running). These new practices are accurately described and helpfully put in parallel with traditional forms of manipulation in an article by Professor Tom Lin, which has been provided for your reference as Appendix VII.[10] Some argue that high frequency traders use these practices to prey on unsuspecting market participants and make considerable profits at the expense of investors and the marketplace.

Government Usage of Algorithms

Governmental entities are also increasingly using algorithms to make decisions affecting the lives of millions of Americans. Algorithms have played a role in decisions on Medicare eligibility, school placement, and even criminal sentencing. Although these decisions may have a tremendous impact on individuals, governmental algorithms generally remain completely outside of the scope of public scrutiny. These automated decision systems are sometimes deployed without public knowledge, and the government does not explain how these decisions were made. As a result, people have less power to question or appeal them.[11] Just as regulators have been trying to access private (*e.g.*, company) algorithmic source code, academics, NGOs, and civil rights advocates have been pressuring government agencies to publicize information regarding governmental algorithms.[12] Some even argue that keeping these algorithms secret goes against the idea of a democratic government and threatens the rule of law.[13]

[7] *Id.* at 69; *see also* Orellana, *supra* note 6 (citing *Ernst & Ernst v. Hochfelder*, 425 U.S. 185, 198, (1976), where the Court described market manipulation as "*intentional or willful* conduct designed to deceive or defraud investors by controlling or artificially affecting the price of securities." (emphasis added).

[8] Yesha Yadav, *The Failure of Liability in Modern Markets*, 102 VIR. L. REV. 1031, 1053 (2016).

[9] Gregory Scopino, Special Counsel, CFTC, Remarks at the 23rd Annual Financial Markets Conference: Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies (May 2018) (transcript available at https://www.frbatlanta.org/news/conferences-and-events/conferences/2018/0506-financial-markets-conference/transcripts/research-papers/scherer-regulating-artificial-intelligence-systems-risks-challenges-competencies-strategies.aspx [https://perma.cc/EH3Q-6WBC] (describing the difficulty of proving intent given the new possibility of misconduct without a paper trail, save source code).

[10] Tom C.W. Lin, *The New Market Manipulation*, 66 EMORY L.J. 1253, 1280-92 (2017).

[11] Dillon Reisman, Jason Schultz, Kate Crawford & Meredith Whittaker, *Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability*, AI NOW, April, 2018, https://ainowinstitute.org/aiareport2018.pdf [https://perma.cc/2WGG-DARB].

[12] *See*, Sonia K. Katyal, *Private Accountability in the Age of Artificial Intelligence*, 66 UCLA L. Rev. 54, 2019; Tom Simonite, *AI Experts Want To End 'Black Box' Algorithms In Government*, WIRED, Oct. 18, 2017, https://www.wired.com/story/ai-experts-want-to-end-black-box-algorithms-in-government/ [https://perma.cc/389X-T239]; Julia Angwin, *Make Algorithms Accountable*, THE NEW YORK TIMES, Aug. 1, 2016), https://www.nytimes.com/2016/08/01/opinion/make-algorithms-accountable.html [https://perma.cc/7YLX-D4V6]; Saranya Vijayakumar, *Algorithmic Decision-Making*, HARVARD POLITICAL REV. ,June 28, 2017, http://harvardpolitics.com/covers/algorithmic-decision-making-to-what-extent-should-computers-make-decisions-for-society/.

[13] David S. Levine, Secrecy and Unaccountability: Trade Secrets in Our Public Infrastructure, 59 Fla. L. Rev. 135, 138 (2017).

Despite calls for reform, governmental agencies have repeatedly refused to make public the source code they utilize and argue that algorithms are not "agency records" or "records" subject to disclosure. In addition, they argue that these algorithms fall under the trade secret exemption of the Freedom of Information Act ("FOIA") allowing records to be withheld if releasing them would harm a company's competitive advantage.[14]

One recent high-profile incident captures this potential hypocrisy.[15] In 2017, New York City Council Member James Vacca drafted a bill mandating that city agencies make publicly available any source code used in an automated-decision system.[16] New York City Mayor Bill de Blasio opposed the idea.[17] He voiced concerns that this proposal would threaten government cybersecurity and the intellectual property rights of certain companies, and would violate procurement agreements with vendors—dissuading them from further contracting with the city.[18] Thereafter, the bill was significantly altered and forfeited the disclosure requirements.[19]

Similarly, in the context of stress tests, some theorists argue that increasing demands by regulators for more information from regulated entities weakens the ability of the regulator to, in turn, deny requests for disclosing their own internal documents or algorithms. For example, Professor Hal Scott believes that the Federal Reserve ought to follow a normal notice-and-comment regulatory process which could involve the Fed disclosing more of its internal examination documents.[20] It could similarly be argued that it would be difficult for the CFTC to continue to refuse to disclose its own algorithms used to detect manipulative practices while demanding access to the source code of high frequency traders. Industry groups could point to a concrete example of information withheld by the CFTC and, perhaps, legitimize their resistance to source code access.

Regulatory Secrecy

A culture of supervisory confidentiality has historically existed in the banking sector.[21] Since the 1800s, bank examinations have been conducted under a cloak of secrecy and kept in place by the criminalization of "spreading false rumors about a bank."[22] The traditional view is that confidential bank examination is necessary to prevent a "run on the banks" if the examination yields negative results. A

[14] Freedom of Information Act 5 U.S.C § 552(b) (4) (2000). *See* Katherine Fink, *Opening the government's black boxes: freedom of information and algorithmic accountability*, 21 Information, Communication & Society (discussion of Exemption 4 in the context of algorithms).

[15] Julia Powles, THE NEW YORKER (Dec. 20, 2017), https://www.newyorker.com/tech/annals-of-technology/new-york-citys-bold-flawed-attempt-to-make-algorithms-accountable.

[16] *Id.*

[17] Lauren Kirchner, *Federal Judge Unseals New York Crime Lab's Software for Analyzing DNA Evidence*, ProPublica (Oct. 20, 2017, 08:00 AM), https://www.propublica.org/article/federal-judge-unseals-new-york-crime-labs-software-for-analyzing-dna-evidence.

[18] *Id.*

[19] Powles, *supra* note 15.

[20] *See* Hal Scott, Stress Tests: Restore Compliance with the APA, THE CLEARING HOUSE, (2017), https://www.theclearinghouse.org/banking-perspectives/2017/2017-q3-banking-perspectives/articles/stress-tests-apa-compliance.

[21] Margaret E. Tahyar, *Are Bank Regulators Special?*, TCH BANKING PERSPECTIVES, https://www.theclearinghouse.org/banking-perspectives/2018/2018-q1-banking-perspectives/articles/are-bank-regulators-special [https://perma.cc/42XS-5T8U] (last visited May 5, 2019).

[22] See Guidance, Supervisory Expectations, and the Rule of Law: How do the Banking Agencies Regulate and Supervise Institutions: Hearing before the S. Comm. On Banking, Housing, and Urban Affairs, 116th Cong. (2019). (Statement of Margaret E. Tahyar, Partner, Davis Polk & Wardwell LLP), https://www.banking.senate.gov/imo/media/doc/Tahyar%20Testimony%204-30-19.pdf.

further justification has been the need for a direct line of communication between the regulator and the financial institution uninhibited by any fear of disclosure to the general public.[23]

Ironically, federal financial regulators used the passage of FOIA to expand the scope of the confidentiality requirement.[24] FOIA exempts information "contained in or related to examination…by an agency responsible for the regulation or supervision of financial institutions."[25] This has given regulators leeway to promulgate rules asserting that examinations are the property of the regulator and imposing further constraints on their disclosure. As a result, financial institutions are not allowed to disclose "confidential supervisory information,"[26] such as CAMELS ratings which evaluate a bank's overall health. Moreover, while sharing confidential supervisory information ("CSI") *within* the banking organization is generally permitted, the OCC has limited sharing to situations where it is "necessary or appropriate for business purposes."[27]

This legal framework, founded in the 1960s, does not account for the volume of information currently generated by financial institutions on a daily basis. The broad definition of CSI could theoretically encompass every email, file and megabyte of data shared with the regulator.[28] Because regulators consider CSI to be their property, its theft or misuse implies criminal liability. Thus, financial institutions and their personnel now daily operate with the constant threat of criminal liability for the "property" of financial regulators.[29]

The confidentiality of supervisory information has given regulators unchecked discretionary power and a culture of "secret guidance and secret lore".[30] The theory and logic behind banking supervision is shrouded in secrecy and inaccessible even to financial entities subject to supervision. In some instances, rules of behavior and conduct were not even disclosed to the supervised entities. Indeed, they were not even written down anywhere. Rather, they are passed down orally from experienced federal employees to new hires like "gnostic secrets…transmitted…from shaman to novice."[31] Supervised entities operate in an environment where they are not even allowed to know the rules for how they ought to behave, which, in turn, increases the risk that regulators will arbitrarily punish supervised entities for unrelated reasons.

While CSI materials are primarily utilized by other regulatory entities, the CFTC has analogous procedures whereby they also receive confidential information of a proprietary nature. The CFTC routinely requests and receives similar sensitive information from its own regulated entities which may give rise to worries that similar problems may plague the relationship between financial institutions and the CFTC regulators. Specifically, there may be similar restrictions on the ability of the regulated entities (expanded

[23] *Id.*

[24] *Id.*

[25] 5 U.S.C. § 552(b)(8) (2016).

[26] 12 CFR § 4.32(b) (1995); *see* also Clifford S. Stanford, *Towards A Coherent and Consistent Framework for Treatment of Confidential Supervisory Information*, 22 N.C. BANKING INST. 41, 46 (2018) (Confidential Supervisory information is defined as any information related to an examination, inspection or other visitation of a financial institution prepared by on behalf of or for the use of financial regulatory agencies).

[27] 12 C.F.R. § 4.37(b)(2).

[28] *See* Hearings, *supra* note 22.

[29] *Id.* at 6.

[30] *Id.* at 9.

[31] *Id.* (citing Board of Governors of the Federal Reserve System, Transcript Open Board Meeting on April 23, 2019, at 2–3).

under Regulation AT) to disclose or disseminate information that had been shared with CFTC regulators as part of regulatory requirements.

Punitive Regulators

Similarly, this culture of secrecy has also allowed regulators to engage in the practice of "regulation by negotiation" whereby regulators attempt to use the power disparity to achieve unrelated ends or use underhanded methods, such as unlimited delays and silence, to achieve a preferred result. For example, three financial institutions "voluntarily" consented to limit their market share in exchange for having an application expedited to the Federal Reserve.[32] With regulators unwilling to disclose certain supervisory practices, some argue that it seems unfair that banking organizations have been required to disclose infinitely more information following the strong tilt towards transparency and accountability prompted by the New Deal.[33] Some argue that the proposed request for direct access to source code is another, more extreme, example of the trend to impose heavy transparency requirements on banking organizations. However, given the different roles played by financial institutions and financial regulators as well as their different goals, it may be rational to have different transparency schemes for each type of actor.

Benefits of High Frequency Trading

Whether algorithmic trading causes market volatility is a question that has given rise to vociferous academic dispute. Many researchers argue that HFT, as currently regulated, provides important benefits to markets. If true, it could be that Regulation AT would impede the positive effects that come from algorithmic trading.

Many researchers argue that HFT reduces transaction costs[34] and improves pricing accuracy in secondary markets.[35] Furthermore, there is evidence that HFT bolsters market liquidity by raising the volume of purchases and sales, and it may reduce volatility levels. Harvard Law School professor Hal Scott testified before the Senate that it was his opinion that "high frequency trading activity in and of itself has not negatively affected our secondary markets."[36] He went on to state that by increasing liquidity and driving issuance prices downward, HFT had improved capital formation and bolstered growth in the real economy.[37] Most critics of HFT cite the May 6, 2010 *Flash Crash* as conclusive evidence of its negative effects. During the Flash Crash, a trader used an automated algorithm which caused U.S. equity indices to take a massive dip (and rebound) during the course of a single day. However, in its joint report with the

[32] *Id.* at 12-3.

[33] *See* Hearings, *supra* note 22.

[34] Hearing on High Frequency Trading's Impact on The Economy Before the Subcomm. On Securities, Insurance, and Investment of the S. Comm. On Banking, Housing, and Urban Affairs, 113th Cong. (2014) (Testimony of Hal Scott, Nomura Professor, Harvard Law School), https://www.govinfo.gov/content/pkg/CHRG-113shrg91299/html/CHRG-113shrg91299.htm (stating that transaction costs had fallen 50% since 2006).

[35] *See* Terrence Hendershott et. al., *Does Algorithmic Trading Improve Liquidity?*, 66 THE J. OF FIN. 1, 1-33 (2010) http://faculty.haas.berkeley.edu/hender/Algo.pdf; *see also* Cristina McEachern Gibbs, *Breaking It Down: An Overview of High- Frequency Trading*, WALL STREET & TECHNOLOGY (Sept 29, 2009).

[36] Hearings, *supra* note 34.

[37] *Id.*

CFTC on the Flash Crash, the U.S. Treasury conceded that HFT has brought market benefits such as reduced costs and increased market efficiency.[38] Some argue that imposing additional restrictions in the form of Regulation AT would diminish the benefits that HFT has created.

Constitutionality Concerns Over Source Code Access

Many entities and opponents of the initial version of Regulation AT's source code provision believed that it would allow regulators to sidestep constitutional protections against unreasonable searches and seizures by the government.[39] In *New York v. Burger*,[40] the Supreme Court held that the expectation of privacy in commercial property is particularly attenuated in "closely regulated" industries. The Supreme Court recognized that, due to a heightened government interest in regulating particular markets, a warrantless inspection may be reasonable under the meaning of the Fourth Amendment in certain circumstances. The Supreme Court established a three-part test whereby regulators must show that:

1. there is "substantial" government interest underlying the regulatory scheme that purports to authorize the inspection at issue;
2. the warrantless inspection is "necessary to further [the] regulatory scheme"; and
3. "the inspection program, in terms of certainty and regularity of its application provides a constitutionally adequate substitute for warrant."

Much of the literature related to this issue comes from industry insiders who may be predisposed to argue that Regulation AT's provisions would fail the *Burger* test. For example, in a comment, the Futures Industry Association hypothetically applied the *Burger* test to conclude that a warrantless inspection of source code would not be "reasonable" and was, therefore, likely unconstitutional.[41]

Given the inconclusive nature of the effects of algorithmic trading (and high frequency trading, specifically), some argue it may be conceivable that the CFTC lacks "substantial" government interest in requesting direct access to source code. However, it would be very difficult to contend that financial regulators do not have a "substantial" government interest in preventing market manipulation, which in many cases has been known to have algorithmic trading at root.[42] Moreover, substantial government interest has been found in industries (cases cited below) which have far more limited impact on the nation. Similarly, it is of government interest to have visibility into the financial market so as to determine and monitor the extent of systemic risk. It is for the above reason that, when providing commentary to the

[38] Tom Bailey, *US Treasury takes aim at high frequency traders*, WORLD FINANCE (Jul. 14, 2015), https://www.worldfinance.com/strategy/government-policy/us-treasury-takes-aim-at-high-frequency-traders [https://perma.cc/E63P-WQ6J].

[39] John S. Servidio & Bo Harvey, McGuireWoods LLP, *Avocados, the U.S. Constitution and the CFTC's regulation Automated Trading*, LEXOLOGY (Nov. 9, 2016), https://www.lexology.com/library/detail.aspx?g=5d746725-6f7b-4d88-9854-7e958a6bc955 [https://perma.cc/3F6N-GX4M].

[40] *See* New York v. Burger, 482 U.S. 691 (1987).

[41] Futures Industry Association (FIA), Comment Letter on Notice of Proposed Rulemaking on Regulation Automated Trading (Mar. 16, 2016), https://fia.org/sites/default/files/content_attachments/2016-03-16_Regulation_AT_Comment_Letter.pdf [https://perma.cc/LBU5-YDZE].

[42] Matt Levine, *The Computers Are Sorry About the Flash* Crashes, BLOOMBERG (Jan. 3, 2019, 11:55 AM), https://www.bloomberg.com/opinion/articles/2019-01-03/the-computers-are-sorry-about-the-flash-crashes.

proposed regulation, market participants have generally not disputed the CFTC's interest in requesting source code.

Other opponents have challenged the notion that the lower level of due process afforded in the event of an administrative inspection of source code is "necessary" to further the regulatory scheme of Regulation AT. They cite the use of various programming languages and complex algorithmic strategies to conclude that the CFTC would need to employ expert staff to review source code.[43] Incidentally, members of the CFTC have themselves admitted to a lack of resources.[44] This has pushed market participants to argue that because source code would be "of little practical benefit" to the CFTC, this requirement cannot be "necessary" and, thus, does not satisfy the second prong of the test established in *Burger*.[45] Indeed, even CFTC Commissioner Giancarlo has expressed doubt that access to source code is necessary.[46]

Another argument grounded in the second *Burger* prong is that the Commodity Exchange Act already allows the CFTC to access source code in its course of conducting investigations, that the CFTC has failed to show why these powers are insufficient, and that the compulsory source code preservation and access provision is not "necessary" in the context of the agency's already-broad investigatory powers.

Finally, market participants also contend that the source code section of Regulation AT does not satisfy the third prong of the test. The use of the terms "all code used in the production environment," "related systems," and "software" in §1.81 of the Regulation does not indicate with sufficient clarity or precision the types of information subject to inspection. Furthermore, the Regulation does not specify the regularity with which the source code can be inspected. Thus, market participants contend that the inspection cannot provide a "constitutionally adequate substitute for a warrant," as its scope and regularity under Regulation AT are uncertain.[47] Most importantly, commenters have voiced concerns that the new provision strips market participants of the important procedural safeguards afforded by the subpoena process, such as limits on the scope of inspection or the ability to apply for a protective order, to ensure the proper maintenance of any disclosed information.[48]

However, despite these arguments from Regulation AT opponents, it would likely be exceedingly difficult to successfully challenge Regulation AT on the grounds that the regulation would authorize unreasonable searches or seizures. While the U.S Supreme Court has rarely spoken on what qualifies as a closely regulated industry, both state and lower federal courts have greatly expanded the definition.[49] For example, there are a whole series of cases indicating that credit unions, banking, and insurance are closely regulated industries.[50] Some have concluded that, considering the breadth of types of industries that

[43] FIA, *supra* note 41.

[44] Hearing to review the Fiscal Year 2017 budget request and funding justification for the SEC and CFTC Before the Subcomm. on Financial Services and General Gvt. Of the S. Comm. on Appropriations, 114th Cong. (2016) (Testimony of Timothy Massad, Chairman, CFTC), https://www.appropriations.senate.gov/imo/media/doc/041216%20CFTC%20Chairman%20Massad%20Testimony.pdf ("[T]he agency does not have the resources to adequately oversee these markets.").

[45] FIA, *supra* note 41, at 46.

[46] J. Christopher Giancarlo, Commissioner, CFTC, Statement Regarding Notice of Proposed Rulemaking on Regulation Automated Trading (Nov. 24, 2015) (transcript available at https://www.cftc.gov/PressRoom/SpeechesTestimony/giancarlostatement112415 [https://perma.cc/6ZAT-N43J].

[47] *See* FIA, *supra* note 41, at 47-8.

[48] Citadel LLC, Comment Letter on Notice of Proposed Rulemaking on Regulation Automated Trading (Mar. 16, 2016), available at https://comments.cftc.gov/PublicComments/ViewComment.aspx?id=60745&SearchText [https://perma.cc/2SJN-J2QC].

[49] *See* Rethinking Closely Regulated Industries, 129 Harv. L. Rev. 797, 805 (2016)

[50] *Id.*

qualify, the exception may actually be "the default rule in searches of businesses".[51] Further precedential support for the proposition that the Court would not invalidate Regulation AT on these grounds comes from lower courts. As noted in an Eastern District of New York case that upheld warrantless inspections on cigarette sellers, "the Supreme Court has identified a handful of industries that are subject to pervasive and often longstanding regulation".[52] Courts appear to consider it important whether there has been a longstanding history of government oversight. Also, courts put emphasis on whether it can be said that a given entity has tacitly consented or "voluntarily chosen to subject himself to a full arsenal of governmental regulation."[53] Based on these cases, it could be that fears over legal challenges to the constitutionality of Regulation AT are overblown.

Non-Legal Concerns with Source Code Access

Unique Nature of Source Code

Regulation AT proponents such as CFTC Chairman Timothy Massad argue that source code is indistinguishable from other types of confidential information routinely provided to the CFTC.[54] However, others, such as CFTC Commissioner Giancarlo, consider source code different from ordinary records because it shows "what positions the firm intends to buy or sell *in the future*."[55] Giancarlo stated that Regulation AT effectively "lowered the bar for the federal government" to access intellectual property and future business strategies.[56] Commenters largely shared the view of Commissioner Giancarlo,[57] and they emphasized that source code is "not a routine business record and should not be treated as such."[58] The argument is based on the view that source code both reflects historical information but also contains information regarding future business strategies. The intellectual property contained in source code, thereby, contains commercially valuable strategic information which some market participants have even described as the "lifeblood of…commercial success."[59]

In support of the argument that source code differs from ordinary records, opponents point out that proprietary source code is afforded protections under multiple areas of the law (*e.g.*, trade secret law, database rights, copyright law), whereas ordinary records contain mere facts and are generally not entitled to such protections. Commenters emphasized that if a trade secret is accidentally or intentionally exposed, it loses its protected character.[60] In essence, accidental disclosure of algorithmic-trading source code could render as public information the trading strategies of the most successful investment firms.[61]

[51] *Id.*

[52] United States v. Mansour, 252 F. Supp. 3d 182, 190 (W.D.N.Y. 2017)

[53] *Id.*

[54] Timothy Massad, Chairman, CFTC, Statement Regarding Approval of Supplemental Proposal to Automated Trading Regulation (Nov. 4, 2016), https://www.cftc.gov/PressRoom/SpeechesTestimony/massadstatement110416 [https://perma.cc/3J2X-V6M7].

[55] Giancarlo, *supra* note 46.

[56] *Id.*

[57] *See* Citadel LLC, *supra* note 48; *see also* FIA, *supra* note 41.

[58] CME Group Inc., Comment Letter on Notice of Proposed Rulemaking on Regulation Automated Trading, 38 (Mar. 16, 2016), https://comments.cftc.gov/PublicComme/ViewComment.aspx?id=60765&SearchText= [https://perma.cc/43JX-Y2F3].

[59] FIA, *supra* note 41 at 8.

[60] *Id.* at 50.

[61] Citadel, *supra* note 52.

Information Security Concerns

Adding to the weight of the abovementioned arguments is that worries over the confidentiality of source code are not groundless. Hackers have increasingly targeted financial institutions and regulators.[62] CFTC Chairman Massad echoed this point when he stated that "cyber security is the single most important new risk to market integrity and financial stability."[63] On this point, Commissioner Giancarlo agrees that confidentiality of source code is a strong concern and highlights the federal government's "poor track record of keeping sensitive information secure from cyber-attacks."[64]

Indeed, financial regulators have been known to suffer from both internal and external data thefts. In 2015, the Federal Deposit Insurance Corporation (FDIC) suffered one of the largest internal data thefts. A report from the FDIC's Office of Inspector General that investigated a series of eight separate information security incidents from 2015 to 2016 found serious issues with the FDIC responses to these data breaches.[65] In one of those instances, an employee left the agency with a USB containing the "living wills" of several systemically important financial institutions.[66] In another case, a Federal Reserve employee passed confidential information to a former supervisor working at an investment bank.[67] Data security issues have not been limited to just the FDIC. In 2016, the SEC suffered one of the most severe external data breaches to date. This incident involved the theft of corporate announcements from SEC's EDGAR filing system which contained nonpublic earnings results.[68] The hackers responsible for the theft allegedly gained around $4 million in illegal profits by trading on the information.[69] The CFTC and the DOJ have also suffered cyber security breaches resulting in the loss of confidential employee information which included social security numbers.[70] These episodes show that no executive agency is safe from the threat of both internal and external data breaches.

Regulation AT also extended source code testing and retention requirements to algorithms licensed from third-party providers. Commenters strongly oppose this provision, stating that it is not clear how traders who license systems from third parties, and thus do not have access to source code, can comply with the provision. Furthermore, market participants cannot be required to obtain source code

[62] Bhakti Mirchandani, *Laughing All The Way To The Bank: Cybercriminals Targeting U.S. Financial Institutions*, Forbes (Aug. 28, 2018, 01:57AM), https://www.forbes.com/sites/bhaktimirchandani/2018/08/28/laughing-all-the-way-to-the-bank-cybercriminals-targeting-us-financial-institutions/#798496396e90.

[63] *Hearing Before the H. Comm. on Agriculture*, 114th Cong. (2015) (Testimony of Timothy Massad, Chairman, CFTC), https://www.cftc.gov/PressRoom/SpeechesTestimony/opamassad-11 [https://perma.cc/QVT8-MBED].

[64] Giancarlo, *supra*, note 46.

[65] See Federal Deposit Insurance Corporation, Office of the Inspector General, *Special Inquiry Report*, (April 2018). https://www.fdicoig.gov/sites/default/files/report-release/OIG-18-001.pdf.

[66] *Former Senior Employee at FDIC Convicted of Embezzling Confidential Documents*, DEPARTMENT OF JUSTICE U.S. ATTY'S OFFICE, EASTERN DISTRICT OF N.Y. (Dec. 11, 2018), https://www.justice.gov/usao-edny/pr/former-senior-employee-fdic-convicted-embezzling-confidential-documents [https://perma.cc/2KNH-9YXB].

[67] Former Employee of Federal Reserve Bank of New York Pleads Guilty in Manhattan Federal Court to Theft of Confidential Information From the Federal Reserve, DEPARTMENT OF JUSTICE U.S. ATTY'S OFFICE, SOUTHERN DISTRICT OF N.Y., https://oig.federalreserve.gov/releases/news-gross-guilty-theft-confidential-information-nov2015.htm [https://perma.cc/6KSF-RBHQ].

[68] Matt Robinson & Chris Dolmetsch, *SEC Sues Same Group Behind Press Release Hack Over Its Edgar Breach*, BLOOMBERG (Jan. 15, 2019, 9:33AM), https://www.bloomberg.com/news/articles/2019-01-15/sec-files-lawsuit-over-scheme-to-hack-edgar-database.

[69] *SEC Brings Charges in EDGAR Hacking Case*, SEC (Jan. 15, 2019), https://www.sec.gov/news/press-release/2019-1 [https://perma.cc/5QE3-H6Y9].

[70] Spencer Ackerman & Sam Thielman, *US officials downplay impact of Department of Justice hacking*, THE GUARDIAN (Feb. 8, 2016 2:48 PM), https://www.theguardian.com/technology/2016/feb/08/department-of-justice-homeland-security-hacking [https://perma.cc/K795-HKMU]; Silla Brush, *CFTC Data Breach Risks Employees' Social Security Numbers*, BLOOMBERG (June 25, 2012, 12:01 AM), https://www.bloomberg.com/news/articles/2012-06-25/cftc-data-breach-risks-employees-social-security-numbers.

from vendors. Even if the latter were to provide their code, the costs associated with maintaining the proprietary information of a third-party would be prohibitive.[71]

In addition to data breaches, market participants made note of the existing controversy regarding the applicability of the FOIA to source code. Although government agencies contend that source code is not a "record," and is thus exempt from FOIA requirements, this question remains a subject of debate. In response to the argument that source code would be protected by FOIA's trade secret exemption even if FOIA did apply, commenters note that the protections provided are not absolute and do not shield companies from requests made by Congress and other regulatory agencies.[72]

A recent Supreme Court case strongly suggests that materials disclosed to the CFTC under Regulation AT would be covered by the trade secret exemption. In *Food Marketing Institute*, the Court widened the breadth of information considered "confidential" for purposes of FOIA's Exemption 4 for trade secrets and commercial or financial information.[73] In this case, the Court categorically rejected the idea that a company must show "substantial competitive harm" in order for the disclosed information to be protected.[74] Instead, provided that (1) the information is customarily treated as private or privately held the by the person providing it and (2) there are assurances by the government that it will not be disclosed, then the disclosed information will fall under this exemption.[75] This likely means that private entities who are providing sensitive financial documents or data to the federal government can likely rest assured the information will not be released under FOIA.[76] This would suggest that this particular worry over data leakage as a result of Regulation AT may be overblown.

Conclusion

The above concerns are founded on my experience working in the intersection of law and finance for the past several decades and ought to bear heavily on any future decisions regarding how to regulate HFT and algorithmic trading.

[71] International Swaps and Derivatives Association (ISDA), Comment Letter on Notice of Proposed Rulemaking on Regulation Automated Trading (Mar. 16, 2016), https://www.isda.org/a/vniDE/regulation-at-comment-03-16-16-002.pdf [https://perma.cc/CC9N-F2J9].

[72] FIA, *supra* note 41.

[73] *See* Food Mktg. Inst. V. Argus Leader Media, 139 S. Ct. 2356 (2019).

[74] *Id.* at 2363.

[75] *Id.*

[76] Davis Polk, *SCOTUS Expands Scope of FOIA Trade Secrets and Commercial Information Exemption*, https://www.davispolk.com/files/2019-06-26_scotus_expands_scope_of_foia_trade_secrets_commercial_information_exemption.pdf (last visited March 28, 2019).

Appendix II: Legal Intern Research Memorandum on Regulation AT

Memorandum

DATE: July 15, 2018

TO: Director, CFTC Division of Market Oversight

FROM: Summer 2018 Legal Intern

RE: Regulation Automated Trading Overview

On November 15, 2015, the CFTC unanimously approved Regulation Automated Trading ("Regulation AT").[1] This original version of Regulation AT aimed to reduce the risks of algorithmic trading activity by imposing risk control requirements for market participants, futures commission merchants, and designated contract markets ("DCM") executing algorithmic trading orders.[2] However, Regulation AT provoked a backlash from market participants.[3] While commenters strongly supported CFTC's efforts to regulate algorithmic trading, most voiced concerns regarding its scope and reach. The key requirements of Regulation AT were (i) registration of algorithmic traders, (ii) establishment of risk control measures, and (iii) requirements of source code preservation.[4] This memo proceeds by first describing the three main regulatory requirements. Then, it outlines subsequent developments in the timeline of Regulation AT and concludes by spelling out the regulatory efforts being made by other U.S. and foreign regulators. This last section of the memorandum covers, at a high level, alternative proposals or policy solutions for handling the same types of issues Regulation AT is aimed at solving.

Key Regulatory Requirements of Regulation AT

Registration

Regulation AT introduced rules for determining whether a trader was an "algorithmic trader." This development would force otherwise unregistered trading firms to register with the CFTC so long as they have direct electronic access to the market and operate algorithmic trading systems. The CFTC hoped that this regulation and the SEC's FINRA registration requirement[5] would together mean that all algorithmic traders would be brought within regulators' reach.[6] Now, even the smallest market participant (five total trades per day) would be subject to registration if that trader used algorithms to perform the trades.

[1] *CFTC Unanimously Approves Proposed Rule on Automated Trading,* U.S. Commodity Futures Trading Commission (Nov. 24, 2015), https://www.cftc.gov/PressRoom/PressReleases/pr7283-15 [https://perma.cc/R5R5-LCRV].

[2] *Id.*

[3] CFTC Stirs Outrage Over Algo Trading Source Code Proposals, FINEXTRA (04, Nov., 2016), https://www.finextra.com/newsarticle/29718/cftc-stirs-outrage-over-algo-trading-source-code-proposals [https://perma.cc/4LL2-82XE].

[4] Woodward Megan, The Need for Speed: Regulatory Approaches to High Frequency Trading in the United States and the European Union, Vanderbilt Journal of Transnational Law 50, no. 5 1359, 1384 (2017).

[5] *Id.* at 1381.

[6] *Id.*

The CFTC argued that the regulation was justified because the marketplace is "too linked to fail."[7] They stated that because a single malfunction could have a devastating impact, the breadth of the registration requirement was critical to ensuring that *all* firms using trading algorithms were subject to Regulation AT.[8] Commentators, however, strongly opposed the broad reach of the registration requirements. One of the strongest critics of Regulation AT, CFTC Commissioner Christopher Giancarlo, stated that by capturing and unduly burdening small market participants, Regulation AT would be erecting further barriers to entry into this market.[9] Moreover, many commenters believe that the CFTC registration requirement was needless because the CFTC *already* has sufficient legal authority to impose requirements on non-registrants[10] trading on U.S. futures markets if the nature of their trading is "disruptive."[11]

Risk Control Measures

In terms of risk control measures, Regulation AT imposed maximum order message and order size parameters, in addition to standards for the development, testing and monitoring of algorithmic trading systems.[12] These are aimed at limiting the volume or quantity of items in any given transaction and throttle or control excessive messages being sent to the electronic order book. To counter the disruptive practice of algorithms being directly tested in the actual market, the regulation required that the developmental environment of algorithms be isolated from the trading environment.[13] The regulation mandated testing of all changes to algorithmic code and tests to identify circumstances that could lead to future flash crashes.[14] A flash crash occurs when there is a rapid withdrawal of orders from a given market that is amplified (or caused) by electronic trading algorithms which lead to dramatic declines in a very short period of time. The proposed risk control measures were mostly criticized for focusing on the type of market participant, rather than the nature of the trade.[15]

Source Code Preservation

Section 1.81(a)(1)(vi) of Regulation AT required that companies create and maintain source code repositories which would include copies of all code used in the production of the algorithm as well as both all changes later made to the code and even information on "who, when and why" each specific change

[7] Tom C.W. Lin, *The New Investor*, 60 UCLA L. REV. 678, 714 (2013), https://www.uclalawreview.org/the-new-investor-2/ [https://perma.cc/M4H6-7NUC].

[8] Regulation Automated Trading, 80 Fed. Reg. 78845 (proposed Dec. 17, 2015), https://www.federalregister.gov/documents/2015/12/17/2015-30533/regulation-automated-trading.

[9] J. Christopher Giancarlo, Commissioner, CFTC, Statement Regarding Notice of Proposed Rulemaking on Regulation Automated Trading (Nov. 24, 2015), (transcript available at https://www.cftc.gov/PressRoom/SpeechesTestimony/giancarlostatement112415 [https://perma.cc/6ZAT-N43J].

[10] 7 U.S.C 6c(6) ("[T]he Commission may make and promulgate such rules and regulations as, in the judgment of the Commission, are reasonably necessary to prohibit the trading practices described in paragraph (5) and any other trading practice that is disruptive of fair and equitable trading.").

[11] Futures Industry Association (FIA), Comment Letter on Notice of Proposed Rulemaking on Regulation Automated Trading (Mar. 16, 2016), https://fia.org/sites/default/files/content_attachments/2016-03-16_Regulation_AT_Comment_Letter.pdf [https://perma.cc/LBU5-YDZE].

[12] Regulation Automated Trading, *supra* note 8.

[13] *Id* at 78857.

[14] *Id.*

[15] *Id.*

occurred.[16] However, existing recordkeeping provisions under broad administrative regulations adopted by the CFTC already require that regulated entities hold all books and records accessible and open to inspection by the CFTC and the DOJ.[17] It is possible that the CFTC and the DOJ would have access to algorithmic source code without use of a subpoena even if the algorithm was developed by a third-party outside the scope of the regulation.

Source code preservation provisions garnered the most controversy. Market participants, and even members of the CFTC, were opposed to the CFTC or the DOJ potentially having access to proprietary source code without a subpoena. "It is unconceivable that any firm should be expected to leave its intellectual property on the doorstep of the government," said Bill Harts, Chief Executive of Modern Markets Initiative.[18] As further discussed below, Regulation AT was highly criticized for having sidestepped constitutional privacy concerns, disregarding algorithms' unique nature, and unduly endangering market participants' core intellectual property.

Initial Response and Industry Backlash

A number of academics, regulators, and industry participants raised serious concerns after the initial unveiling of Regulation AT. Most of the backlash focused on the source code provisions; however, other concerns were raised related to regulatory oversaturation, duplication of efforts by other agencies, practical concerns with implementing the Regulation, and similar issues. The CFTC's General Counsel intends to incorporate many of these concerns in her analysis of the Regulation.

Supplemental Proposal and Abandonment of Regulation AT

In 2016, the CFTC issued a Notice of Supplemental Proposed Rulemaking ("Supplemental Proposal") to address some of the comments received from market participants.[19]

Registration

Regarding registration, the CFTC added a volume-based quantitative test for determining whether a trader was an algorithmic trader subject to registration.[20] However, commenters found this amendment unsatisfactory and argued that small market participants would still fall within the registration requirements because of the expanded definition of electronic trading.[21] They further argued that too many small traders would be ensnared because the volume-based test looked at the aggregate of all

[16] *Id.*

[17] 17 CFR § 1.31 (2017).

[18] Gregory Meyer & Philip Stafford, *US Regulators Propose Powers To Scrutinize Algo Traders' Source Code*, FINANCIAL TIMES (DEC. 1, 2015) https://www.ft.com/content/137f81bc-944f-11e5-b190-291e94b77c8f [https://perma.cc/8HJQ-CQEC].

[19] Regulation Automated Trading, 81 Fed. Reg. 85334 (proposed Nov. 25, 2016), https://www.cftc.gov/sites/default/files/idc/groups/public/@lrfederalregister/documents/file/2016-27250c.pdf.

[20] *Id.* at 85336.

[21] Futures Industry Association (FIA), Comment Letter on Supplemental Notice of Proposed Rulemaking regarding Regulation Automated Trading (May. 1, 2017), https://fia.org/sites/default/files/content_attachments/2017-05-01_CFTC_RegAT_0.pdf [https://perma.cc/VR7E-N4A3]; ISDA, Comment Letter on Supplemental Notice of Proposed Rulemaking regarding Regulation Automated Trading (May. 1, 2017), https://www.isda.org/a/ZniDE/supplemental-reg-at-comment-letter-isda-05-01.pdf [https://perma.cc/KV4P-UPWT].

electronic trading without considering the scale or frequency of activity.[22] On the other side, many regulators *also* found the increased size requirement unsatisfactory. They believed this new definition still left too many small entities unregulated which would still lead to large-scale catastrophic events based on the extremely interconnected nature of the market.[23]

Source Code

The CFTC pushed back on the opposition to the source code provisions but also eased some requirements. The CFTC again emphasized that it receives confidential information on a daily basis and handles "sensitive, proprietary and trade secret information" under strict rules.[24] The Supplemental Proposal continued to require source code preservation, however, under a set of rules separate from those generally applicable to books and records.[25] Specifically, the Commission could only access source code via subpoena or by a special call authorized by the Commission ("Enhanced Special Call"). Furthermore, the CFTC would use specifically tailored means of access to ensure the source code remains secured. The procedure would include on-site inspection of the market participant, the use of computers disconnected from the network, and the provision of records stored on secure storage media.[26]

However, many opponents doubted the sufficiency of these changes. For example, they argued that the Enhanced Special Call still leaves market participants with less protection than a normal subpoena.[27] Faced with a subpoena, the subpoenaed party can move to quash, challenge its scope, or apply for a protective order for additional confidential obligations on the CFTC. In contrast, the Enhanced Special Call provides none of these protections. Commenters re-emphasized that no policy concerns could justify such unfettered access to proprietary information.[28] Commissioner Giancarlo echoed these concerns, stating that this would "[g]ive unchecked power to the CFTC to decide if, when and how property owners must turn over their source code."[29] Commissioner Giancarlo noted "no subpoena means no due process of law," thereby highlighting the importance of the subpoena process in striking a balance between the rights of property owners and the unlimited power of the government.[30] Moreover, he heavily criticized the "Special Call" process, stating that "a few additional" bureaucratic hurdles could not undermine the rights of property owners.[31] Opponents fear that allowing the CFTC to adopt such practices would encourage other regulators, domestic and foreign, to require similar access.

[22] *Id.*

[23] *See generally* Tom C.W. Lin, *The New Market Manipulation*, 66 EMORY L.J. 1253, 1280-92 (2017).

[24] Regulation Automated Trading, *supra* at note 19.

[25] *Id.* at 85337.

[26] *Id.*

[27] ISDA, *supra* note 21, at 6.

[28] *Id.*

[29] J. Christopher Giancarlo, Commissioner, CFTC, Statement of Dissent Regarding Supplemental Notice of Proposed Rulemaking on Regulation Automated Trading (Nov. 4, 2016), https://www.cftc.gov/PressRoom/SpeechesTestimony/giancarlostatement110416 [https://perma.cc/R7P5-FDKR].

[30] *Id.*

[31] *Id.*

Third-Parties

The CFTC also responded to criticism of proposing onerous requirements upon third-party developers of trading algorithms to be used by market participants. The Supplemental Notice highlighted that the use of third-party systems should not serve as an excuse for market participants to circumvent compliance and regulatory standards for algorithmic trading. However, recognizing the practical difficulties of the requirement, the Supplemental Notice permitted market participants to satisfy the development and testing requirements by: (i) obtaining a certificate that the third party is complying with Regulation AT requirements and (ii) conducting due diligence regarding the accuracy of the certification. Dissatisfied, the industry labeled this as "untenable" because it would require them to monitor developers. This would only be possible if developers consented to providing their users with access to their proprietary source code. One industry group labeled it "regulatory overkill" to both require market participants to obtain a certificate saying its developers were compliant, while also checking the veracity of the underlying facts.[32] Others were worried that market participants lacked the appropriate expertise to perform such functions. Some found impractical the requirement for recertification following every material change to source code, arguing that third-party software was renewed and changed regularly and that it would be difficult to determine what constituted a "material" change under the Regulation.[33]

CFTC Internal Debate and Cessation of Regulation AT

After unveiling the Supplemental Proposal, the CFTC then voted to approve the modified version on November 4, 2016. CFTC Commissioner Giancarlo dissented from the majority vote approving the modified regulation.[34] He gave weight to the possible constitutional challenge to such a rule, concluding that the time spent and expenses incurred in fighting that challenge would be a "sad waste of American taxpayer money."[35] The Commissioner went on to note that the laws prohibiting the release of trade secrets, which were cited by the CFTC in the Supplemental Notice, did nothing to assure that source code would be secure. Highlighting that the CFTC had also been known to suffer from data breaches, he posited that the rules must include specific confidentiality assurances such as on-site inspection of source code and its return to the proprietor once reviewed.[36] Given the opposition from both within the CFTC and from market participants, the CFTC subsequently abandoned Regulation AT.[37]

Other Regulatory Efforts

It is important to catalogue and characterize similar efforts being made by other regulators to address alleged negative effects of algorithmic trading and HFT. These efforts are being pursued both by

[32] *Id.* at 5.

[33] FIA, *supra* note 21.

[34] *See* Giancarlo, *supra* note 29.

[35] *Id.*

[36] *Id.*

[37] *CFTC commissioner: plans to seize algo trading source code are "D-E-A-D",* FINEXTRA RESEARCH (Oct. 5, 2017), https://www.finextra.com/newsarticle/31157/cftc-commissioner-plans-to-seize-algo-trading-source-code-are-d-e-a-d [https://perma.cc/UV8D-6H89].

parallel domestic agencies or regulators as well as foreign counterparts to U.S. financial regulators. Importantly, some academics believe that the current U.S. regulatory framework, considered holistically, has already endowed regulators with sufficient authority and ability to combat the negative effects of HFT.[38] Still others believe that both industry and government have severely overstated the importance of regulation of HFT within financial markets as well.[39]

Domestic Regulation

CFTC's Spoofing Prohibition

Section 747 of the Dodd-Frank Act amended the Commodity Exchange Act to prohibit disruptive trading practices in general and spoofing in particular.[40] The CFTC has since successfully enforced the prohibition on multiple occasions, despite doubts regarding its enforceability with regard to the difficulty of proving intent.[41]

U.S. Securities and Exchange Commission

Recognizing that financial regulators are now essentially "overseeing technology companies"[42] and with a view to address high frequency trading, the SEC adopted Regulation Systems Compliance and Integrity ("Reg SCI"),[43] which sought to reduce the number of trading system issues such as failures, disruptions, delays, errors, or other operational problems with automated systems. Reg SCI also paved the way for the SEC to strengthen oversight of the overall technology infrastructure of US securities markets.[44] Under Reg SCI, these "SCI entities" such as self-regulatory organizations (*e.g.,* FINRA), clearing agencies and alternative trading systems, were required to design, implement and maintain IT policies ensuring that their systems operated in the manner intended and complied with federal securities laws and rules. Reg SCI also provided instructions responding to or correcting errors in the event of a system disruption. The regulation received an overall positive response and was praised for fostering collaboration amongst market participants.[45] However, there was also a widespread belief that the regulation did not go far enough given the ever-increasing use of automated technologies.[46]

To address the Flash Crash, the SEC adopted market-wide circuit breakers that either temporarily halt or close markets if trading if the S&P 500 Index falls below certain thresholds calculated daily based

[38] See Kevin O'Connell, Has Regulation Affected the High Frequency Trading Market?, 27 Cath. U. J. L. & Tech. 145 (2019).

[39] *See* Bloomberg, *Source Code and Chicken Indexes*, 1-2, 9-10 (October 5, 2019).

[40] 7 U.S.C. § 6c(a)(5) (2012) (outlawing "spoofing," a strategy similar to HFT strategies).

[41] Megan Woodward, The Need for Speed: Regulatory Approaches to High Frequency Trading in the United States and the European Union, Vanderbilt Journal of Transnational Law 50, no. 5 1359, 1381 (2017).

[42] Dave Michaels, *Machine Trading Needs More Oversight, Departing SEC Official Says*, THE WALL STREET JOURNAL https://www.wsj.com/articles/machine-trading-needs-more-oversight-departing-sec-official-says-11545404400 [https://perma.cc/Q7QA-J54B].

[43] *Spotlight on Regulation Systems Compliance and Integrity,* SEC, https://www.sec.gov/spotlight/regulation-sci.shtml [https://perma.cc/P4VU-Q8CV] (last visited May 16, 2019).

[44] *Id.*

[45] Woodward, *supra* note 41, at 1378-9.

[46] Woodward, *supra* note 41, at 1379.

on the prior day's closing price.[47] The SEC also amended the trading rules, as contained in the National Market System Plan, for single-stock circuit breakers, using a "limit-up" and "limit-down" mechanism to determine the thresholds for acceptable trading within a given tier of stock.[48] However, during the Flash Crash, it became apparent that the circuit breakers backfired, which prompted the SEC to consider modifying the rules to address current shortcomings.[49]

To address transparency issues, the SEC has also proposed the establishment of a "Consolidated Audit Trail" ("CAT") to improve the ability of the SEC and other industry regulators to oversee trading within the securities markets.[50] Most notably, it would lift the veil on activities in dark pools and other alternative trading platforms. Dark pools are private exchanges or arenas for securities trading that restrict access to their exchange and are known for their lack of transparency. The SEC would require that national securities exchanges, broker-dealers and self-regulated entities report "order lifecycles," the entire progression beginning with ordering a trade and ending when that trade is fully completed and billed, for equities and options to a central repository. These reporting requirements are more exhaustive than any previous requirements and include information regarding order cancellations, the identity of customers, and prices.[51] These new SEC regulations, embodied in Rule 613, also require that each order, broker-dealer, and national securities exchange be assigned a unique code in order to provide regulators with the capacity to not only track the lifecycle of individual orders but also link them to the respective broker-dealer or national exchange.[52] The CAT would greatly enhance the power of the SEC to accurately reconstruct market events and would give private parties a tool to analyze HFT manipulation to establish causation and intent.[53] However, due to technical difficulties, it is years behind schedule. Former SEC Commissioner Kara Stein termed the CAT the "Hubble Telescope" for securities markets".[54]

Financial Industry Regulatory Authority (FINRA)

In 2016, the SEC approved a rule proposed by FINRA which requires all persons associated with a FINRA member, who are also primarily responsible for the design, development, modification or supervision of algorithmic trading strategies, to register as "Security Traders."[55] The rules subject these persons to qualification exams and continuing education requirements. FINRA recognized that developers were largely unaware of the securities rules governing the products they were designing.[56] By educating

[47] *Investor Bulletin: Measures to Address Market Volatility,* SEC (July 1, 2012), https://www.sec.gov/oiea/investor-alerts-bulletins/investor-alerts-circuitbreakersbulletinhtm.html [https://perma.cc/Y28L-GQHN].

[48] *Id*.

[49] *See* Investopedia, *Circuit Breaker*, https://www.investopedia.com/terms/c/circuitbreaker.asp [https://perma.cc/4NWH-3Y8T].

[50] *See* Rule 613 (Consolidated Audit Trail), SEC, https://www.sec.gov/divisions/marketreg/rule613-info.htm [https://perma.cc/U4VX-F7DF] (last visited May 16th, 2019).

[51] 17 CFR § 242.613 (2012).

[52] *See* SEC, *supra* note 50.

[53] *See* Morelli, *supra* note 26, at 53.

[54] *Supra* note 13.

[55] SEC Approves Rule to Require Registration of Associated Persons Involved in the Design, Development or Significant Modification of Algorithmic Trading Strategies, FINRA (2016), http://www.finra.org/industry/notices/16-21 [https://perma.cc/5V6L-7XK4].

[56] *SEC approves FINRA rule requiring registration of algorithmic trading developers*, BLOOMBERG (Apr. 20, 2016), https://www.bloomberg.com/professional/blog/sec-approves-finra-rule-requiring-registration-of-algorithmic-trading-developers/.

developers, FINRA hoped to reduce the incidence of inadequate risk management controls or failures to check for order accuracy.[57]

Some commenters on Regulation AT have posited that other regulatory efforts (*e.g.,* Reg SCI, CAT) combined with the CFTC's spoofing provision in the Dodd-Frank bill and the new FINRA registration requirements are sufficient to address algorithmic trading concerns and specifically eliminate the need for direct access to source code.[58]

Foreign Regulatory Efforts

European Union: Markets in Financial Instruments Directive II (MiFID II)

The European Union began closer regulation of algorithmic trading, and HFT in particular, by supplementing its prior regulation in January 2018. It requires that investment firms notify regulators that they are engaging in algorithmic trading[59] and sets forth standards for determining which activities constitute HFT.[60] Similar to the SEC's CAT, the EU's Markets in Financial Instruments Directive II (MiFID II) requires that an algorithmic trader maintain and make available records of all orders placed including cancellations, executed orders, and quotations on trading venues.[61] Furthermore, analogous to CFTC's Regulation AT, MiFID II provides that a regulator may require an algorithmic trader to provide, *on an ad hoc basis*, information regarding its algorithmic trading strategies. The rule further provides that the regulator may, *at any time*, request further information without describing the scope of information that can be requested.[62] MiFID II, thereby, potentially allows regulators to request source code without a subpoena, however, that has not yet come to pass.[63] Some believe this suggests the U.S. ought to reconsider Regulation AT. However, one current CFTC Commissioner, Brian Quintenz, rejected "automatically adopt[ing] comparable regulatory requirements," especially warrantless access to source code.[64] He rejected the concept of a "one-size-fits-all" regulatory ideal and stated that different jurisdictions must be free to adopt regulation tailored to their unique history and market structures.[65]

[57] *Id.*

[58] Holly A. Bell, Mercatus Center, Comment Letter on Notice of Proposed Rulemaking on Regulation Automated Trading (Mar. 16, 2016), https://www.mercatus.org/publication/potential-effects-reg-unintended-risks-and-diminished-cooperation-market-participants [https://perma.cc/5S6N-2PGU].

[59] Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2009/92/EC and Directive 2011/61/EU (MiFID II), Article 17(2), https://ec.europa.eu/info/law/markets-financial-instruments-mifid-ii-directive-2014-65-eu_en.

[60] Article 4(1)(40), MiFID II Directive.

[61] Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2009/92/EC and Directive 2011/61/EU (MiFID II), Article 17(2), https://ec.europa.eu/info/law/markets-financial-instruments-mifid-ii-directive-2014-65-eu_en.

[62] 52 Article 17(2), MiFID II. *See also* Hogan Lovells, MiFID II, Algorithmic and High-Frequency Trading for Investment Firms (Dec. 2016), https://www.hoganlovells.com/~/media/hogan-lovells/pdf/mifid/new_mifid_update_31_dec_2016/5466119v1mifid-ii-algorithmic-trading-29122016lwdlib01.pdf.

[63] *See* Danny Busch, *MiFID II: Regulating High Frequency Trading, Other Forms Of Algorithmic Trading And Direct Electronic Market Access*, 10, L. and Fin. Markets Rev. 72, 76 (2016), https://doi.org/10.1080/17521440.2016.1200333.

[64] Brian Quintenz, Commissioner, CFRC, Remarks at the Institute of International Bankers Membership Luncheon: Deference for Different Approaches (June, 2018), https://www.cftc.gov/PressRoom/SpeechesTestimony/opaquintenz14 [https://perma.cc/8W2V-R3GP].

[65] *Id.*

Germany: High Frequency Trading Act ("HFT Act")

In 2013, Germany enacted the HFT Act, which requires HFTs to register with Germany's Financial Supervisory Authority and become licensed as a bank or financial trading institution. The licensing requirement applied not only to companies located in Germany, but also to any company directly or indirectly trading on a market subject to German regulation.[66]

The HFT Act also required that firms "tag" each algorithm with a unique code so that regulators can identify which particular algorithm made any given trading decision. German regulators consider the "algorithm-tagging" rule a better alternative to direct source access. These German authorities pointed to confidentiality concerns, the low efficacy of source code access, and practical difficulties inherent in monitoring frequently amended or updated code as reasons for adopting their alternative approach. Tagging algorithms also dissipates the concern that experts will seek to be hired by the regulator with the express purpose of stealing code. A recent study[67] analyzing Germany's algorithmic tagging approach found that although it may not provide regulators with a full picture of algorithmic trading, it better equips regulators to investigate potential manipulative practices.[68] The study found that while tagging is not perfect for monitoring *all* high frequency algorithms, there has been a net improvement in algorithmic transparency after the measure was implemented.[69]

[66] See Holly A. Bell & Harrison Searles, An Analysis of Global HFT Regulation Motivations, Market Failures, and Alternative Outcomes 8-9 (Mercatus Center, Working Paper No. 14-11, 2014).

[67] *See* Alex Walsh, *Evaluating Germany's Success in Regulating High-Frequency Trading* The Regulatory Review (Oct. 25, 2016), https://www.theregreview.org/2016/10/25/walsh-germany-regulating-high-frequency-trading/ [https://perma.cc/T4E6-D92K].

[68] *Id.*

[69] *See generally,* Nathan Coombs, *What is an algorithm? Financial regulation in the era of high-frequency trading,* 45 ECONOMY AND SOCIETY J. 278, 278-302 (2016), https://doi.org/10.1080/03085147.2016.1213977 [https://perma.cc/96MY-YHRX].

Appendices

1. U.S. Commodity Futures Trading Commission, *CFTC Unanimously Approves Proposed Rule on Automated Trading*, Press Release (Nov. 24, 2015), https://www.cftc.gov/PressRoom/PressReleases/pr7283-15 [https://perma.cc/R5R5-LCRV].
2. U.S. Commodity Futures Trading Commission, *Statement of Dissent by Commissioner J. Christopher Giancarlo Regarding Supplemental Notice of Proposed Rulemaking on Regulation Automated Trading*, Press Release (Nov. 4, 2016), https://www.cftc.gov/PressRoom/SpeechesTestimony/giancarlostatement110416 [https://perma.cc/R7P5-FDKR]. [Constitutionality Concerns, Disclosure Issues]
3. Benjamin Bain, *Flash-Boys Regulation Fight Returns to U.S. Derivatives Agency*, BLOOMBERG (Feb. 14, 2018), https://www.bloomberg.com/news/articles/2018-02-14/flash-boys-regulation-fight-returns-to-u-s-derivatives-agency.
4. Woodward, Megan, *The Need for Speed: Regulatory Approaches to High Frequency Trading in the United States and the European Union,* Vanderbilt Journal of Transnational Law 50, no. 5 (2017): 1359, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3203691. [HFT Benefits, HFT Costs, Regulatory Landscape, International Perspectives]
5. Lin, Tom C.W., *The New Market Manipulation,* Emory Law Journal 66, no. 6 (2017): 1253-63, 1265-1305, 1310-14, http://law.emory.edu/elj/content/volume-66/issue-6/articles/the-new-market-manipulation.html. [Market Manipulation, HFT Costs]
6. Michael Morelli, *Regulating Secondary Markets in the High Frequency Age: A Principled and Coordinated Approach*, 6 Mich. Bus. & Entrepreneurial L. Rev. 79, 1-7, 13, 20-58 (2016), https://repository.law.umich.edu/mbelr/vol6/iss1/4/. [HFT Benefits, HFT Costs]
7. Bloomberg, *Source Code and Chicken Indexes,* 1-2, 9-10 (October 5, 2019), https://www.bloomberg.com/opinion/articles/2016-11-07/source-code-and-chicken-indexes. [HFT Relevance]
8. Kevin O'Connell, *Has Regulation Affected the High Frequency Trading Market?*, 27 Cath. U. J. L. & Tech 145, 172 (2019): 152-164, 167-9, https://scholarship.law.edu/jlt/vol27/iss2/7/. [HFT Relevance, Regulatory Landscape, Alternative Regulatory Bodies, Self-Regulation]
9. City of Los Angeles, Calif. v. Patel, 135 S. Ct. 2443, 2454 – 57, 2459 – 64 (2015). [Constitutionality Concerns]
10. Thomas Laser, *Regulation Automated Trading: CFTC Source Code Turnover Provision is Unnecessary and Dangerous to U.S. Markets*, 4 J. Marshall Global Mkt. L. J. 37 (2016): 45, 48-50, https://repository.jmls.edu/cgi/viewcontent.cgi?article=1019&context=globalmarkets. [Constitutionality Concerns]
11. U.S. Commodity Futures Trading Commission and U.S. Securities and Exchange Commission, "Executive Summary," *Findings Regarding the Market Events of May 6, 2010*, Report, 1-8 (September 30, 2010), https://www.sec.gov/news/studies/2010/marketevents-report.pdf. [Flash Crash, HFT Costs, Market Interconnectedness]
12. Loren Selznick & Carolyn LaMacchia, *Cybersecurity: Should The Sec Be Sticking Its Nose Under This Tent?*, 2016 U. Ill. J.L. Tech. & Pol'y, 35, 35-8, 56-61 (2016),

http://illinoisjltp.com/journal/wp-content/uploads/2016/06/Selznick.pdf. [Information Security, Disclosure Issues, Government Security Issues]

13. Annette L. Nazareth & Margaret E. Tahyar, *Transparency and Confidentiality in the Post Financial Crisis World--Where to Strike the Balance*?, 1 Harv. Bus. L. Rev. 145,145-8, 154-6, 158-63, 176-8, 188-93 (2011), http://www.hblr.org/download/HBLR_1_1/Nazareth_Tahyer-Transparency_Confidentiality.pdf. [Information Accuracy; Disclosure Issues; Information Security; Regulatory Culture]
14. United States Department of Justice, U.S. Attorney's Office, Eastern Division of New York, *Former Senior Employee at FDIC Convicted of Embezzling Confidential Documents* (Dec. 11, 2018), https://www.justice.gov/usao-edny/pr/former-senior-employee-fdic-convicted-embezzling-confidential-documents.
15. Cheng-Yun Tsang, *From Industry Sandbox to Supervisory Control Box: Rethinking the Role of Regulators in the Era of Fintech*, 2019 U. Ill J.L. Tech. & Pol'y 355, 370-1, 402-3 (2019), http://illinoisjltp.com/journal/wp-content/uploads/2019/11/Tsang.pdf. [Regulatory Landscape, Regulatory Capacity]
16. Margaret Tahyar, *Are Bank Regulators Special?*, TCH Banking Perspectives: Bank Policy Institute, https://www.theclearinghouse.org/banking-perspectives/2018/2018-q1-banking-perspectives/articles/are-bank-regulators-special [https://perma.cc/42XS-5T8U] (last visited May 5, 2019). [Regulatory Culture, Disclosure Issues]

HARVARD
LAW SCHOOL | The Case Studies

CSP056
APRIL 2020

Regulating Crypto Assets: Securities and Commodities

AMY AIXI ZHANG

Memorandum

DATE: April 18, 2020

TO: Research Assistant

FROM: Managing Director, Bipartisan Policy Center

RE: Policy platform on the regulation of digital assets

Introduction

The past few years have seen a surge in the adoption of crypto asset technologies. Labelled with various names, including "virtual assets," "digital tokens," "digital coins," "digital currencies," "cryptocurrencies," "convertible virtual currencies," crypto assets have been widely debated by institutional investors and retail consumers alike. Hundreds of new start-ups have proposed business models utilizing distributed ledger technology. Even legacy financial institutions like Fidelity,[1] Mastercard,[2] Visa,[3] and JP Morgan[4] have acknowledged the benefits of new technologies like blockchain. Most famously, Facebook announced its controversial proposal for a new digital currency that would replace all currency as a global medium of exchange.[5]

Retail investors embraced crypto assets long before financial institutions.[6] At its peak in January 2018, the total market cap of all crypto assets was a record high $800 billion, equaling a tenth of the value

[1] About Us - Fidelity Digital Assets, (last visited Jan. 16, 2020), https://www.fidelitydigitalassets.com/about-us.

[2] Mastercard Blockchain to Bring Visibility to Food Systems, Oct. 27, 2019, https://newsroom.mastercard.com/press-releases/mastercard-blockchain-to-bring-visibility-to-food-systems/.

[3] Visa Goes Live With Blockchain-Powered Business Payments Service, Jun 11, 2019, https://www.coindesk.com/visa-goes-live-with-blockchain-powered-business-payments-service.

[4] J.P. Morgan Global, Blockchain And Distributed Ledger, (last visited Jan. 16, 2020), https://www.jpmorgan.com/global/blockchain.

[5] Mike Isaac and Nathaniel Popper, *Facebook Plans Global Financial System based on Cryptocurrency,* N.Y. Times, June 18, 2019, https://www.nytimes.com/2019/06/18/technology/facebook-cryptocurrency-libra.html?module=inline.

[6] CoinMarketCap Global Charts, (last visited Nov. 4, 2019), https://coinmarketcap.com/charts/.

Written by Amy Aixi Zhang, under the supervision of Howell E. Jackson, James S. Reid, Jr., Professor of Law at Harvard Law School. Case development at Harvard Law School is partially funded by a grant from Dechert LLP. Cases are developed solely as the basis for class discussion. They are not intended to serve as endorsements, sources of primary data, legal advice, or illustrations of effective or ineffective management.

Copyright ©2020 President and Fellows of Harvard University. No part of this publication may be reproduced, stored in a retrieval system, used in a spreadsheet, or transmitted in any form or by any means—electronic, mechanical, photocopying, recording, or otherwise—without permission. To order copies or permissions to reproduce materials please visit our website at casestudies.law.harvard.edu or contact us by phone at 617-496-1316, by mail at Harvard Law School Case Studies Program, 1545 Massachusetts Avenue – Areeda 507, Cambridge, MA 02138,or by email at HLSCaseStudies@law.harvard.edu.

of all gold in the world. But the volatility soon after was stunning; just a few months later the market spiraled down to $250 billion.

The same enthusiasm that accelerated market growth attracted numerous bad actors as well; the amount of cryptocurrency stolen or scammed in 2018 rose to $1.7 billion.[7] Crypto assets created generous wealth for early adopters, but brought sweeping losses to newer holders.

To maintain secure growth of the marketplace, participants are calling for the development of proper financial, legal and technological infrastructure. U.S. regulators—unlike other countries—have not banned the trading of crypto assets, but instead have sought comment from companies and investors to develop critical regulatory oversight. Just as federal, state and international regulators together secure the financial system, they must maintain a safe and fair infrastructure for the transfer of digital assets.

Currently, the U.S. does not have a comprehensive regulatory policy to treat digital assets. Instead, a mix of federal, state and local laws and regulations overlap additional layers of rules from self-regulated organizations (SROs) and internal company compliance procedures. The complexity and lack of clarity has chilled experimentation and dissuaded many financial technology start-ups and companies from pursuing innovations in this space.

The numerous government agencies responsible for stabilizing the crypto asset marketplace include the Federal Reserve, the Internal Revenue Service (IRS), and the Treasury Department's Financial Crimes Enforcement Network (FinCEN). However, the Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC) have been two of the most active regulatory agencies.

Still, gaps remain. Some have argued that regulators will be unable to maintain adequate oversight due to insufficient jurisdictional authority and have proposed that Congress step in to bolster agencies' authority and provide clarity. The most topical issue for the marketplace is still the trading of securities and commodities crypto assets and some experts estimate that more than $1 trillion in Bitcoin transactions were cleared in 2018.[8]

The Bipartisan Policy Center (BPC) is concerned about the widespread adoption of digital asset technologies because the current regulatory environment is insufficiently equipped to protect participants such as consumers and retail investors, who are most susceptible to fraud and volatility.[9] As you know, the BPC is a Washington, DC-based think tank dedicated to fostering bipartisanship. BPC reconciles the policy positions of advocates, corporations, and policy experts to design proposals and solutions for Congress.

Our team would like to draft a smart reform package that presents clear guidance to Congress and financial regulators on how best to treat the crypto asset industry. We need your help to brief our team on the industry and relevant considerations before we begin drafting. Your research will be critical to ensuring our team presents a fair and accurate policy proposal.

[7] Gertrude Chavez-Dreyfuss, *Cryptocurrency thefts, scams hit $1.7 billion in 2018,* Reuters, Jan. 29, 2019, https://www.reuters.com/article/us-crypto-currency-crime/cryptocurrency-thefts-scams-hit-1-7-billion-in-2018-report-idUSKCN1PN1SQ.

[8] Marsh and McLennan Cos., FireEye, Circle, Report|Crypto-Assets, *Crypto-Assets and Blockchain Technology On the Brink of Legitimacy?,* Jan. 2019, https://www.fireeye.com/content/dam/fireeye-www/partners/pdfs/rpt-marsh-fireeye-crypto-paper.pdf.

[9] Ted Knutson, *Elizabeth Warren Lays Into Crypto*, Oct 11, 2018, https://www.forbes.com/sites/tedknutson/2018/10/11/elizabeth-warren-cryptocurrency-is-easy-to-steal/#235486801249.

Assignment

Please prepare a presentation that provides an overview of the crypto asset industry and the regulatory perimeters of the SEC and CFTC. Your briefing should present the benefits and costs of crypto asset technologies and outline all the relevant considerations Congress should examine.

The memorandum below offers some background information on the crypto asset industry, the current regulatory regime, and recent Congressional developments. I have also listed a set of briefing questions that can frame your presentation. Finally, an appendix with additional readings will guide your analysis; while you are free to complete additional research, all information you need is included in these readings.

In your presentation, please make sure to consider all relevant parties including consumers, investors, startups and legacy financial institutions.

Crypto Asset Industry

Origins of Crypto Assets

To understand crypto assets, one must first understand the origins of cryptocurrency. In 2009, pseudonymous software developer Satoshi Nakamoto created Bitcoin, the first cryptocurrency to be widely used. Initial adoption was driven by a variety of characters including internet architects, anarchists, futurists, encryption experts, government skeptics and, later, criminals. Early adopters were often fueled by anti-establishment sentiment that sought financial independence from government systems and instability. By combining pre-existing technologies—cryptography, peer-to-peer networking, and distributed ledger technology—in a unique way, these cryptocurrencies did not require a central government or institution to maintain the system or ensure its accuracy. While we will not explore all the technologies, for your background Appendix 1 explains the fundamentals of blockchain and Appendix 2 the crypto classifications.

The basics of distributed ledger technology (DLT) are simple to understand. Though the technology is more complex, for our purposes you need only understand the fundamentals. The term DLT refers to a method of creating a shared, immutable and chronological record of transactions. Simply described, it is a database that allows multiple sites—countries or institutions—to access and write onto a continuous ledger.[10] Think of it as an always-accessible record of transactions where every user must agree to the recording of each new transaction. Once the transaction is verified and recorded onto the ledger, no participant can meddle with its history. A type of DLT called blockchain, uses cryptography to allow each participant on the network to write on the ledger in a secure way.[11] While readings in the appendices below dive deeper into specific technologies that underpin blockchain (i.e. public and private key cryptography, hashing, digital signatures), the most important feature of DLTs is the elimination of a central authority. You'll often read that blockchains are "decentralized." Many crypto assets do not have

[10] Richard Brown, *Distributed Ledger Technology: beyond block chain,* UK GOVERNMENT OFFICE OF SCIENCE (2016), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf.

[11] Steven Norton, *CIO Explainer: What Is Blockchain?*, WALL ST. J. (Feb. 2, 2016), https://blogs.wsj.com/cio/2016/02/02/cio-explainer-what-is-blockchain/.

a central institution, unlike fiat currencies which are controlled by a central bank, or credit and debit cards managed by card network companies like Visa, Mastercard, etc. Positively, there are no barriers to entry and anyone is able to install the requisite software, exchange fiat currency for Bitcoin, and begin transacting without the permission of a private bank or government institution. Users together keep copies of the ledger, verify new transactions, and issue new currency. Theoretically, users can trust that the system remains secure and fair without a central authority. Realistically, intermediaries are often hacked[12] and systems can be compromised.[13] Yet regulators are not able to identify an institution to audit or punish for wrongdoing.

Soon after Bitcoin, other developers began creating alternative cryptocurrencies that used distributed ledger systems including Ripple, Tezos, Ethereum, Zcash and others. All were different versions of the same underlying technology: a decentralized payment system that could automatically generate new currency and verify new transactions. After the successful launch of these cryptocurrencies, many recognized an application of distributed ledgers to other types of assets and transactions beyond fiat currency. New "tokens" were invented to represent products or services (e.g., Basic Attention Token, 0x). Other cryptocurrencies, known as stablecoins, were designed to be pegged to traditionally involatile currencies like the U.S. dollar or gold. Some systems used tokens to represent ownership of real estate, intellectual property rights, or products in a supply chain. This process of converting a real-world asset or value into a digital representation became known as "tokenization" where each type of token mapped back to the data of a particular kind of asset. And because DLT ensures all transactions and trading of the token were immutable and accurate, users are assured that the "token," a digital representation of a gift card, a painting, some currency, a bond, etc., cannot be forged or questioned.[14]

Costs and Benefits of a Crypto Asset Industry

Allowing for financial players to tokenize and use crypto assets presents a number of benefits. Because tokens can be traded on secondary markets of the issuer's choice, tokenization provides liquidity. Transacting with tokens is also often faster and cheaper than traditional markets for the same assets, because parts of the exchange process are automated and fewer intermediaries are needed. Trading tokens is also more transparent, because the ledger is an open record of ownership and token holders' rights and legal responsibilities are known and embedded in the token. Barriers to entry are low, so tokenization opens trading to a broader range of buyers and sellers. Finally, tokenization allows for fractional ownership; because tokens are highly divisible, investors can purchase representations of small percentages of the underlying assets.[15]

But widespread tokenization and use of crypto assets would also create significant obstacles, especially for regulators. Security regulations are technology agnostic; rules apply to tokenized assets

[12] Davey Winder, *How Hackers Stole $1B From Cryptocurrency Exchanges In 2018*, FORBES (Dec. 31, 2018), https://www.forbes.com/sites/daveywinder/2018/12/31/how-hackers-stole-1b-from-cryptocurrency-exchanges-in-2018/#7bff86c74d87.

[13] Michael MacDonald, *Investigation of Quadriga cryptocurrency debacle turns up only $28 million in assets*, FINANCIAL POST (May 13, 2019), https://business.financialpost.com/technology/blockchain/investigation-of-quadrigacx-cryptocurrency-debacle-turns-up-28-million-in-assets.

[14] Stephen O'Neal, *Tokenization, Explained*, COINTELEGRAPH (Jun. 2, 2019), https://cointelegraph.com/explained/tokenization-explained.

[15] Deloitte, *The tokenization of assets is disrupting the financial industry*, INSIDE MAGAZINE, Issue 19, Part 2, https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/financial-services/lu-tokenization-of-assets-disrupting-financial-industry.pdf.

based on how the token is used and not on the underlying technology. Rules that restrict token creation, use, and sales would prevent the free movement of these tokens and undermine the accessibility and liquidity benefits described above. At the same time, without clear rules or guidance from regulators, the crypto asset industry is vulnerable to hacking and scams that could harm investors and hamper the token economy. Market manipulation has the potential to run rampant; both the SEC and CFTC have charged dozens of entities for misinformation and fraud. The U.S. Justice Department has initiated a criminal probe pertaining to crypto manipulation.[16]

At the same time, many are concerned with the technological and governmental infrastructure of a crypto asset industry. Linking tokens permanently to the underlying asset represents a dilemma many developers are working to solve. While many supply chain tokenization projects claim to provide users with tokens that represent items in a supply chain (i.e. food, diamonds, interests in funds, etc.) proof that a specific token is connected to a specific real-life asset is challenging. Separately, issues with governing the crypto asset industry, including designating final arbiters of disputes, developers to maintain the technology, custodians for storing tokens, and intermediaries who can ensure settlement of trades have yet to be resolved.

Financial institutions are also obligated by anti-money laundering and know-your-customer rules to report suspicious activity to regulators. But in a token economy, business interactions can be anonymous and hidden. A safe and functioning crypto asset industry will require advances in technology, revised rules and standards, and new operational measures in order for companies to comply. As described in further detail below, the current regulatory regime does not sufficiently address these issues.

Ready for Regulation: Classifying Crypto Assets

To understand the set of regulations that would apply to the crypto asset industry, we must first understand the relevant factors. As tokenization grew in popularity, thousands of different types of tokens were created, and many argued that crypto assets were not subject to regulation because they were new financial instruments that did not fit conventional statutory definitions. In recent years, regulators have noted that financial regulations are technology-agnostic; revolutionary digital ledger technology does not preclude regulation of digital assets. Instead, the nature of the digital asset-related activity was a key factor in determining requirements.[17]

As a result, categorizing the different use cases for crypto assets has become critical. Early thought leaders taxonomized various tokens using existing definitions of "commodity," "security," and "currency," while others have created new categories like "utility token," "payment tokens," "asset token," etc.[18] Courts and regulators used similar descriptions and underlying principles to define various categories of

[16] Matt Robinson and Tom Schoenberg, *U.S. Launches Criminal Probe into Bitcoin Price Manipulation*, BLOOMBERG (May 24, 2018), https://www.bloomberg.com/news/articles/2018-05-24/bitcoin-manipulation-is-said-to-be-focus-of-u-s-criminal-probe.

[17] *Leaders of CFTC, FinCEN, and SEC Issue Joint Statement on Activities Involving Digital Assets,* U.S. Sec, and Exch. Comm. Public Stmt. (Oct.11, 2019), https://www.sec.gov/news/public-statement/cftc-fincen-secjointstatementdigitalassets#_ftn4.

[18] *What are the different types of cryptocurrency?*, EXODUS, (last visited Jan. 22, 2020), https://support.exodus.io/article/1084-what-are-the-different-types-of-cryptocurrency; CryptoAsset Classifications, Basic Attention Tokens (BAT), INTELLIGENT TRADING FOUNDATION (last visited Jan. 22, 2020), https://intelligenttrading.org/guides/cryptoasset-classifications/#utility-tokens-basic-attention-tokens-(bat); Adam Haeems, *What is a crypto-asset?,* BABB, Medium.com (Apr. 27, 2020), https://medium.com/babb/what-is-a-crypto-asset-1f0fcc517887.

assets they encountered.[19] None of these classifications have been deemed the official definition by Congress. Agencies drafted their own definitions and drew their own regulatory perimeters.

Carefully distinguishing the various types of crypto assets is critical because regulatory treatment of a particular crypto asset depends on how it is defined. A different set of regulations and agencies will apply differently to alternate definitions of crypto assets.

Generally, most definitions to date distinguish between three types of crypto assets. First, currency or exchange tokens are the most recognizable crypto assets, like Bitcoin and Ethereum, used as a means of payment. Second, utility or consumer tokens represent use of or access to a blockchain-based application or service. For example, users of Siacoins can use the tokens on a blockchain network solely to purchase and sell storage space. For our purposes, we focus on the third category: asset-backed tokens, which are tokens pegged to real-world units of value. Specifically, our focus is on tokens that are related to securities and commodities.[20] For more clarity, you'll need to read SEC and CFTC guidance on definitions of these crypto assets available in Appendices 3 and 4.

SEC, CFTC and Congress: Regulating and Legislating Crypto Assets

To recommend a detailed policy proposal for the SEC and CFTC, we must understand their respective regulatory boundaries. We can then decide whether we should recommend that the boundary be expanded, contracted, supplemented, or clarified.

Various companies began using tokenization to create coins that represented access to services and products of the company. Companies would issue the tokens much like a company issued shares. Though the tokens typically did not represent actual ownership in the company, investors would purchase these tokens because they were likely to rise in value as the company developed its product and because they could later be sold on a secondary market. Companies would initiate a new blockchain using the underlying protocol of various cryptocurrencies and then send the tokens directly to a buyer's digital wallet with their address or through a crypto exchange.

The Initial Coin Offering (ICO) craze was a headline-grabbing new option for raising capital. The first token sale was held by Mastercoin in July 2013.[21] Ethereum raised approximately $2.3 million with a token sale in 2014. The surge in ICOs occurred in 2017 when a new web browser called Brave generated

[19] Crypto Law Corner: Descriptions of "Crypto Assets", WINSTON AND STRAWN LLP (2019), https://www.winston.com/images/content/1/5/v2/159397/Crypto-Law-Corner-Description-of-Crypto-Assets.pdf.

[20] ABA IDPPS Jurisdiction Working Group "Digital and Digitized Assets: Federal and State Jurisdictional Issues" (Mar. 2019). Section 2(a)(1) of the Securities Act of 1933 and Section 3(a)(10) of the Securities Exchange Act of 1934 defines the term "security" as "any note, stock, treasury stock, security future, security-based swap, bond, debenture, evidence of indebtedness, certificate of interest or participation in any profit-sharing agreement, collateral-trust certificate, preorganization certificate or subscription, transferable share, investment contract, voting-trust certificate, certificate of deposit for a security, fractional undivided interest in oil, gas, or other mineral rights, any put, call, straddle, option, or privilege on any security, certificate of deposit, or group or index of securities (including any interest therein or based on the value thereof), or any put, call, straddle, option, or privilege entered into on a national securities exchange relating to foreign currency, or, in general, any interest or instrument commonly known as a 'security', or any certificate of interest or participation in, temporary or interim certificate for, receipt for, guarantee of, or warrant or right to subscribe to or purchase, any of the foregoing." [Emphasis added]. Even if an instrument is not considered on its face a "security" because it does not take the form of a stock, bond, etc., the definition of "security" contains a "catch-all" term—namely, "investment contract"—that will include instruments with the same substantive features of financial instruments expressly named as securities in the definition.

[21] Laura Shin, *Here's The Man Who Created ICOs And This Is The New Token He's Backing,* FORBES (Sep. 21 2017), https://www.forbes.com/sites/laurashin/2017/09/21/heres-the-man-who-created-icos-and-this-is-the-new-token-hesbacking/#1ee981441183.

over $35 million in under thirty seconds. The average amount of funding rose to hundreds of millions of dollars and, by November 2017, there were over 50 offerings every month. Overall, ICOs raised over $5 billion in 2017 for nearly 800 deals.[22] For companies, the amount of funds involved were typically much greater than funds generated from a crowdfunding campaign and allowed companies greater creative latitude in their business models.

But even amidst the heady environment of loose investing, many voiced their wariness of ICOs and the likelihood that these unregulated offerings would be penalized. As crowdfunding attorney Amy Wan noted in her 2017 post: "*If it walks like a duck and quacks like a duck, its [sic] probably a duck*."[23] In other words, although tokens may not represent ownership in the same way as traditionally regulated securities, the form and function of these crypto assets would nonetheless be subject to federal securities laws. Indeed, the SEC in subsequent years created a Cyber Unit and filed dozens of enforcement actions and cease-and-desist orders against companies for fraud and for using ICOs for the unregistered raising of funds.

SEC Jurisdiction

In order to regulate crypto assets, the SEC must have proper jurisdiction and authority. The Securities Act of 1933 grants the SEC authority to regulate only those assets that are deemed securities. Many ICO issuers have claimed that their tokens are not considered "securities," and are therefore not subject to SEC oversight. Due to the varying characteristics and types of crypto assets, whether a particular crypto asset is a "security" is a fact-intensive inquiry that must be applied on a case-by-case basis.

The SEC Chairman and staff members have stated that the Commission will apply the test and standards formulated by the well-known Supreme Court case *SEC v. W.J. Howey Co.*, which renders the offering of a token as a security-offering subject to the Securities Act.[24] The test has four prongs: is there (1) an investment of money, (2) in a common enterprise, (3) with the expectation of profit, (4) from the managerial efforts of others.[25] See Appendix 8 for examples of its application. Relevant factors include the manner in which the token is offered or distributed.[26] If a token is deemed a security, then its offering must comply with securities law requirements, including registration requirements, cybersecurity requirements, and requirements for policies that prevent fraud and market manipulation. Additionally, any exchange, intermediary trading, or handling is also subject to securities laws.

Using this standard, the SEC has pursued a number of avenues for regulation. The SEC first applied the *Howey* test to digital assets in 2017, finding that the sale of Decentralized Autonomous Organization digital tokens ("DAO tokens") was an unregistered security offering.[27] Since this first pursuit of a

[22] Blockchain Startups Absorbed 5X More Capital Via ICOs Than Equity Financings In 2017, CBINSIGHTS (Jan. 18, 2018), https://www.cbinsights.com/research/blockchain-vc-ico-funding/.

[23] Amy Wan, *Why Your Initial Coin Offering Is Probably Regulated By Securities Law*, CROWDFUND INSIDER (Mar. 6, 2017), https://www.crowdfundinsider.com/2017/03/96598-initial-coin-offering-probably-regulated-securities-law/.

[24] SEC v. W.J. Howey Co., 328 U.S. 293 (1946).

[25] *Id.*, 298-300.

[26] William Hinman, *Digital Asset Transactions: When Howey Met Gary (Plastic)*, (speech, San Francisco, CA, Jun. 14, 2018), https://www.sec.gov/news/speech/speech-hinman-061418.

[27] *SEC Issues Investigative Report Concluding DAO Tokens, a Digital Asset, Were Securities,* U.S. SEC, AND EXCH. COMM. PRESS RELEASE (Jul. 25, 2017), https://www.sec.gov/news/press-release/2017-131.

cryptocurrency company, the SEC has brought dozens of enforcement actions against individuals and companies for a broad swathe of securities law violations, including fraudulent activity, failure to register a token offering, and improper touting of an offering.[28]

In December 2017, SEC Chairman Jay Clayton issued a statement explaining that a vast majority of ICOs are structured as securities offerings because investors bought tokens solely to profit from a later rise in value of the token, which derived from the company's business model.[29] The SEC next applied *Howey* to digital assets in *Munchee Inc.* and concluded that the ICO was an unregistered securities offering because the tokens were marketed as an investment in the company.[30] A summary of the actions can be found in Appendices 8 and 12.

Surprisingly, the SEC's William Hinman, Director of the Division of Corporation Finance, stated that a crypto asset at first deemed a security can "over time, become something other than a security."[31] Bitcoin and Ethereum, he noted, were no longer securities because the *Howey* tests second prong was not satisfied: the network was sufficiently decentralized and could exist without a "common enterprise." His speech became the beginnings of a framework for determining whether a consumer token sale is exempt from securities laws, though questions remain (discussed below). For a comprehensive explanation of the SEC's current treatment of crypto assets, see Appendices 10, 11 and 12.

Similar to regulation over issuances of securities, the SEC also has jurisdiction over financial securities and derivatives market intermediaries, like exchanges and trading platforms, to protect investors and prevent fraud and manipulative trading practices. However, most new crypto intermediaries have failed to register with the SEC. For more information, please see Appendix 13. There are currently over 200 cryptocurrency exchanges operating throughout the world.[32] To date, only one entity has registered its ICO with the SEC and no exchanges or trading platforms are currently registered with the SEC.

CFTC Jurisdiction

If a crypto asset is not deemed a security, then it may fall under the jurisdiction of the Commodity Futures Trading Commission (CFTC). Established in 1974, the CFTC oversees the U.S. derivatives market. To understand how crypto assets can apply to derivatives markets, you must understand some basic plumbing of the derivatives market.

Derivatives are contracts whose value derives from an underlying commodity. The commodities markets are expansive and include everything from agricultural commodities, like wheat and corn, to metals and energy, like gold and gasoline. Today, commodities also encompass securities, foreign currencies, interest rates and other financial assets. Derivatives are contracts between two parties that

[28] Cyber Enforcement Actions: Digital Assets/Initial Coin Offerings, U.S. SEC, (last visited Jan. 22, 2020), https://www.sec.gov/spotlight/cybersecurity-enforcement-actions.

[29] Chairman Jay Clayton, Statement on Cryptocurrencies and Initial Coin Offerings, U.S. SEC (Dec. 11, 2017), https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11.

[30] See Order Instituting Cease-and-Desist Proceedings, pursuant to section 8A of the Securities Act of 1933, Making Findings, and Imposing a Cease-and-Desist Order, U.S. SEC (Dec. 11, 2017), https://www.sec.gov/litigation/admin/2017/33-10445.pdf.

[31] Hinman, *supra* note 26.

[32] CoinMarketCap, Exchanges — All, (last visited Jan. 22, 2020), https://coinmarketcap.com/.

commit both to an exchange of cash, goods or securities in the future for a pre-settled price. No payment is required upfront, but the contract allows for swift remedial action in the event of a default.

In this way, derivatives allow traders in various commodities to manage their risk. Since commodity prices fluctuate and market participants cannot predict the price of a commodity at the time the supply chain requires it, a company uses derivatives to hedge its commodity exposure. A beer company might lock in the price of wheat so that regardless of future increases or decreases in price profits remain stable. Derivatives enable enterprises to run large-scale operations without bearing the commensurate large-scale risks. Farmers, manufacturers, producers, municipalities, pension funds, etc. all rely on derivatives trading to hedge risk and participate in the market.[33] The most common forms of derivatives are futures, forwards, options, and swaps.

As allowed by the 1963 Commodity Exchange Act (CEA) definition of a "commodity," — which paints a broad brush — CFTC deemed cryptocurrencies to be "commodities." In May 2018, the agency published guidance asserting its jurisdiction over virtual currency derivative transactions. "Bitcoin and other virtual currencies are properly defined as commodities,"[34] the CFTC noted, and a court later agreed.[35]

It's important to note that the CFTC can regulate derivative products involving a commodity, but has limited power in regulating the "cash market" or "spot market" for the commodity itself.[36] For example, while the CFTC has jurisdiction over wheat futures contracts, it has less power to regulate the trading of wheat itself. Applied to crypto assets, this means that the CFTC can regulate derivative products derived from cryptocurrencies—like futures or options contracts based on Bitcoin and Ethereum—as well as the firms providing derivatives custody or advisory services. But the CFTC has restricted jurisdiction over the buying and selling of Bitcoin and Ethereum itself.

Similar to the SEC, the CFTC has actively pursued crypto asset companies that failed to comply with regulatory requirements.[37] The CFTC has also actively brought enforcement actions against fraud and manipulation in cryptocurrency spot markets.[38] In response, some firms have sought direct approval to allow cryptocurrency derivatives trading on their platforms to avoid punitive enforcement actions for failing to register with the CFTC. Bitcoin futures trading was launched by the Chicago Board Options Exchange (CBOE) and the Chicago Mercantile Exchange (CME) during the peak of the crypto bull market in December 2017, though the CBOE stopped adding new contracts in March 2019.[39] Institutional exchange LedgerX received approval from the CFTC to allow the trading of regulated swaps and options contracts on its platform. To further efforts to prevent fraud in the marketplace, the CFTC issued a policy

[33] In Defense of Derivatives: From Beer to the Financial Crisis, CATO INSTITUTE (SEPTEMBER 2015).

[34] ABA Digital and Digitized Assets: Federal and State Jurisdictional Issues, ABA IDPPS JURISDICTION WORKING GROUP (MARCH 2019).

[35] *CFTC v. My Big Coin Pay, Inc.*, 334 F. Supp. 3d 492 (D. Mass. 2018).

[36] The CFTC regulates the swaps and futures markets, and retains general enforcement authority to police fraud and manipulation in cash or 'spot' commodities markets, *see, e.g.*, 7 USC §§ 6c(a), 9, 12(a)(5), 15; 17 CFR § 180.1.

[37] *See* Latham & Watkins, *CFTC Brings Significant Enforcement Action Against Online Cryptocurrency Exchange, Client Alert No 1980* (Jun. 20, 2016), www.lw.com/thoughtLeadership/ CFTC-brings-significant-enforcement-action- against-online-cryptocurrency-exchange.

[38] See, e.g., CFTC Release PR7714-18, CFTC Charges Multiple Individuals and Companies with Operating a Fraudulent Scheme Involving Binary Options and a Virtual Currency Known as ATM Coin, CFTC (Apr. 18, 2018), www.cftc.gov/PressRoom/PressReleases/7714-18.

[39] Elijah Bradley, *Derivatives in Crypto, Explained*, COINTELEGRAPH (Jul. 10, 2019), https://cointelegraph.com/explained/derivatives-in-crypto-explained.

of offering monetary rewards for information regarding “pump-and-dump” schemes.[40] See Appendices 16, 17 and 18 for a comprehensive explanation of the CFTC’s current treatment of crypto assets.

Congress

An absence of guidance from regulators has spurred actions on numerous fronts in Congress. The number of entities lobbying on blockchain issues almost tripled from a dozen in the fourth quarter of 2017 to 33 a year later.[41] Most are asking Congress and agencies to provide greater clarity around the jurisdictions and powers of the SEC and CFTC. In July 2019, SEC Chairman Clayton and CFTC Chairman Christopher Giancarlo testified before the Senate Banking Committee and noted that the regulators were still unsure whether their agencies had sufficient authority over the cryptocurrency markets.

A number of efforts illuminate options for Congress. First, seven Congressman penned a letter to the Director of the National Economic Council requesting that the Administration hold a forum on blockchain technologies, and support innovation and development of blockchain as an emerging technology.[42] Though the letter had no specific recommended actions, it noted that the current regulatory environment was stifling innovation, and that the United States should engage with the private sector, academia, and policymakers to research and promote blockchain technologies.

A faction of lobbying groups, Senators and other advocates believe cryptocurrencies should not be regulated under the SEC and should instead fall under the CFTC and Federal Trade Commission. Action was taken by Congress in 2018 when the Token Taxonomy Act, proposed in the House of Representatives in 2018, and re-introduced in 2019, sought to amend the Securities Act of 1933 and the Securities Exchange Act of 1934 “to exclude digital tokens from the definition of a security.” Each would have exempted cryptocurrencies from securities law and proposed that the SEC offer tax-related changes for those doing transactions with cryptocurrency.

Problems with the Existing Regulatory Regime

It is obvious that both the SEC and CFTC have been active enforcers of securities and commodities laws in their pursuit of fraudulent and manipulative behavior. However, solely regulating through enforcement actions and cease-and-desist letters is not sustainable, nor the most effective use of resources. Inadequacies remain in the current system, as discussed below.

Lack of Clarity in Current Laws

Although the SEC has attempted to provide clarity through numerous enforcement actions and lawsuits, determining whether a cryptocurrency is a security and how to apply the *Howey* test remains a

[40] *Customer Advisory: Beware Virtual Currency Pump-and-Dump Schemes*, CFTC, (last visited Jan. 20, 2020), https://www.cftc.gov/sites/default/files/idc/groups/public/@customerprotection/documents/file/customeradvisory_pumpdump0218.pdf.

[41] Theodoric Meyer, *Inside the blockchain lobbying boomlet*, POLITICO (Mar. 18, 2019), https://www.politico.com/newsletters/politico-influence/2019/03/18/inside-the-blockchain-lobbying-boomlet-549283.

[42] Amy Davine Kim, Chief Policy Officer, Chamber of Digital Commerce, *Seven U.S. Members of Congress Urge Administration to Support Blockchain Technology*, CHAMBER OF DIGITAL COMMERCE (May 24, 2019), https://digitalchamber.org/seven-u-s-members-of-congress-urge-administration-to-support-blockchain-technology/.

developing area in federal securities regulation. For example, SEC Director Hinman noted that tokens deemed securities may no longer qualify as securities, but it remains unclear when this shift occurs and when the SEC makes this determination. Second, companies remain confused as to whether token sales conducted outside the U.S. fall under the SEC's jurisdiction. And third, because the SEC has stated that Bitcoin and Ethereum are not securities, under current law a trading platform that trades only these crypto assets would not be required to register. However, if an exchange offers trading of other currencies, as many do, how should it be required to register with the SEC? Will such an exchange be required to bifurcate its operations? These questions generate confusion, weakens investor protection, and stifles innovation.

Similarly, although the CFTC has proactively brought enforcement actions against companies for failure to comply, its jurisdiction is also limited. Though the CEA definition of "commodities" broadly encompasses many types of crypto assets, the CFTC has limited jurisdiction over the "cash market" for the commodity. But the trading of Bitcoins for other crypto assets or cash is the most active type of transaction in the industry, and therefore the most susceptible to volatility and deceit. Though the CFTC is allowed to enforce against fraud and manipulation in cash markets and bring certain types of actions, it cannot set sorely needed standards.

Jurisdictional Conflicts Between the SEC and CFTC

Whether a particular crypto asset falls squarely into legal definitions of securities and commodities remains a difficult question to answer. If a crypto asset is labeled a commodity under the CEA definition, the more complicated question is whether the crypto asset is also labeled a security. The CFTC has jurisdiction over certain segments of the *securities-based derivatives* markets, but the SEC is responsible for oversight and regulation of the *cash* markets. In other words, since the CFTC has taken the position that Bitcoin and Ether are commodities under the CEA, the CFTC has jurisdiction over any derivative—a swap, future, other option, etc.—that uses Bitcoin or Ether as underlying commodities.

It's the same application of jurisdiction to derivatives of other commodities like grain, oil, etc., and the SEC has not challenged the CFTC's position. But most trading of cryptocurrencies current takes place on the cash markets, and the SEC would be responsible for the trading of Bitcoin and Ether for cash. Uncertainty remains as to how the SEC and CFTC would allocate jurisdiction for Bitcoin and Ether and how other crypto assets will be classified.

Inapplicability of Current Rules to Digital Assets

Today's regulations serve the current financial infrastructure, but the rise of cryptocurrency as an asset class questions foundational assumptions. Though we take for granted the security and trust guaranteed by exchanges, intermediaries, and parties today, these assumptions do not apply perfectly to a digital asset infrastructure.

For one, our current system for trading assumes a secure way of holding, moving, and protecting our assets. But digital-only assets depend on infrastructure that does not directly align with the traditional financial model. An oft-cited example is "custody." Traditional methods for custodying assets like cash, securities, and objects are modelled off traditional paper-and-safe approaches in banking. Any institutional investor holding more than $150,000 in assets to place these assets under control of a "qualified custodian" that stores assets in designated accounts for safe keeping until needed.

To ensure that assets are secured and not prone to misuse, misappropriation, or financial insecurity like insolvency or financial reverses, security rules require custodians to comply with disclosure rules and surprise audits. SEC rules define custody as "holding, directly or indirectly, client funds or securities, or having any authority to obtain possession of them."[43] But traditional custodians are not naturally equipped to safely store digital assets.

First, custody rules require custodians to legally own or physically hold customers' assets and maintain them free of lien at a good control location. But digital asset ownership does not parallel physical possession; storage relies on a private key infrastructure and possession of a digital asset can distinguish between types of storage (i.e. cold vs. hot), methods for identity verification (i.e. biometrics, access password, etc.), and assurances of exclusive control.

Second, traditional rules around "finality," "clearing," and "settlement" of asset transfers also do not perfectly parallel transfers of crypto assets. Finality is the assurance that a transaction cannot be altered, reversed, or cancelled after completion. But finality on a blockchain or digital ledger can be gradual, not instantaneous, because it takes time for transactions in blocks to be confirmed.[44] Similarly, legal transfer requires third parties to perform clearing and settlement activities. Clearly defining these requirements in the context of crypto assets will allow businesses to comply with regulations and maintain the safety of their networks.

And finally, the technology required to handle digital assets would require significant technological enhancements for traditional custodians. In recent years, few companies have succeeded in providing wallet storage solutions that process, manage, and hold tokens in compliance with securities rules.[45]

Financial institutions seeking exposure to crypto assets are also subject to regulations that discourage illicit activity. Existing anti-money laundering (AML), know-your-customer (KYC) and combatting the financing of terrorism (CFT) laws allow regulators to track suspicious activity. Businesses would need to articulate to regulators the nature of their crypto asset activities, reasons for the activity, and how the business is managing risk exposure. But some tokens build anonymity into an infrastructure that doesn't provide the required transparency without sophisticated tools. Tokens like Monero and Dash, for example, offer less transparency of transacting parties than Bitcoin or Ethereum. Some companies offer anonymity through "washing" or "tumbling" services that obscure the provenance of transactions.[46] These services disrupt conventional risk-assessment rules and regulations.

[43] 17 CFR 275.206(4)-2(d)(2).

[44] Binance, *Finality*, Binance Academy, https://www.binance.vision/glossary/finality.

[45] Rachel Wolfson, *Custodial Solutions Are Latest Innovation in Cryptocurrency Ecosystem as Seen by Coinbase and Others*, Forbes. (Sep 20, 2018), https://www.forbes.com/sites/rachelwolfson/2018/09/20/custodial-solutions-are-latest-innovation-in-cryptocurrency-ecosystem-as-seen-by-coinbase-and-others/#3e3d9572171c.

[46] Mixers and tumblers services mix tokens from different transactions and provide new tokens to clients. These services obfuscate sending and receiving addresses and trails to the original source, thereby improving the anonymity of transactions.

Briefing

This memo has given you a broad overview of the relevant players and costs that attend the benefits of widespread adoption of crypto assets. The Appendices below include many articles that will help you build a more extensive understanding. Not every reading is required for you to build a strong presentation, but these materials will allow you to attain a strong understanding of topics you choose to spotlight. Please review these materials and get ready to brief the BPC policy team.

In particular, the Managing Director is eager to hear your thoughts on the following:

- What is distributed ledger technology? What is blockchain technology? What is a crypto asset?
- What is the current state of the crypto asset industry?
  - What are the various use cases and types of crypto assets?
- How do existing legal definitions delineate crypto assets?
  - What types of uses should be considered securities?
  - What types of uses should be considered commodities?
  - What are some use cases that are difficult to classify and categorize?
- What are the regulatory perimeters of the SEC and CFTC?
  - How does the SEC and CFTC enforce against fraud and manipulation in the marketplace?
  - Given these regulatory perimeters, why do certain crypto asset use cases create conflict between the SEC and CFTC?
- What are the concerns regulators and legislators should consider when formulating a policy?
  - Who are the relevant players affected by a crypto asset regime?
  - What are the costs and benefits of crypto asset technology?
  - What are policy considerations BPC should highlight? (i.e. responsible innovation, minimize fraud, protect consumers and investors, regulatory clarity, etc.)
- What is our final recommendation for Congress?
  - Should we ask Congress to clarify the classification of crypto assets? What sorts of tokens and their uses should be classified as securities? As commodities? How will these definitions change the regulatory boundaries of the SEC and CFTC?
  - Should we dissuade Congress from federal action and instead recommend retaining power with state regulatory and legislative bodies? (i.e. state Bitcoin Licenses, etc.)
  - Should we encourage agencies to coordinate on specific topics? Are there any, other than state and local regulatory bodies or standard-setting groups, that are better equipped to address?

Appendices

Background

1. A Reuters Visual Guide Blockchain Explained
   http://graphics.reuters.com/TECHNOLOGY-BLOCKCHAIN/010070P11GN/index.html
2. Crypto Classification: Security vs. Commodity, HACKERNOON
   https://hackernoon.com/crypto-classification-security-vs-commodity-decf2d78c4a1
3. IMF, "FinTech Notes: Regulation of Crypto Assets" (Provides a strong summary of the risks of crypto assets, and the current regulatory landscape. Though long, it is helpful to read the entire report carefully, as it can give you a very adequate understanding of the landscape.)
4. Compliance Monitor, "A path for consumer tokens – the SEC and CFTC analysis" (With deeper analysis than the IMF report, this paper then dives deeper into the role of the SEC and CFTC in regulating crypto assets. Provides a strong primer to the relevant legal issues you need to address in your briefing.)

SEC

Background

5. What is an ICO?, Investopedia
   https://www.investopedia.com/news/what-ico/
6. Silicon Valley is obsessed with ICOs — here's why, Vox.com
   https://www.vox.com/2017/9/19/16243110/initial-coin-offering-ico-explained-what-is-money-bitcoin-digital-currency
7. Intro to Tokenized Assets and Security Tokens
   https://hackernoon.com/tokenized-assets-security-tokens-and-stos-ae72dc0e275e
8. Howey Test, What Is the Howey Test?, Findlaw.com
   https://consumer.findlaw.com/securities-law/what-is-the-howey-test.html
9. Samuel Falkon, "The Story of the DAO—Its History and Consequences", Medium.com
   https://medium.com/swlh/the-story-of-the-dao-its-history-and-consequences-71e6a8a551ee

Enforcement Actions

10. The DAO Report, "Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO."
    https://www.sec.gov/litigation/investreport/34-81207.pdf
11. Munchee, In the matter of Munchee Inc.: Cease and Desist
    https://www.sec.gov/litigation/admin/2017/33-10445.pdf

Statements/Guidance

12. Public Statement: Statement on Digital Asset Securities Issuance and Trading

https://www.sec.gov/news/public-statement/digital-asset-securites-issuuance-and-trading

13. Guidance by the SEC, Framework for "Investment Contract" Analysis of Digital Assets (April 3, 2019)

    https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets#_edn1

14. Public Statement Leaders of CFTC, FinCEN, and SEC Issue Joint Statement on Activities Involving Digital Assets

    https://www.sec.gov/news/public-statement/cftc-fincen-secjointstatementdigitalassets

CFTC

Background

15. CFTC Chairman Christopher Giancarlo on Regulating Crypto, Andreessen Horowitz interview

    https://a16z.com/2019/09/17/cftc-chairman-crypto-christopher-giancarlo-crypto-regulatory-summit/

Statements/Guidance

16. CFTC Chairman Confirms Ether Cryptocurrency Is a Commodity

    https://www.coindesk.com/cftc-chairman-confirms-ether-cryptocurrency-is-a-commodity

Enforcement Actions

17. MY BIG COIN PAY, INC. et al.

    https://www.cftc.gov/sites/default/files/2018-10/enfmybigcoinpayincmemorandum092618_0.pdf

    Proposals and Considerations for Policy Recommendations

18. Tim Massad, Former CFTC Commissioner, "It's Time to Strengthen the Regulation of Crypto-Assets," (March 2019) (print) [69 pages] (Provides well-evidenced examples of current regulatory gaps in crypto asset regulation. Though much of the introduction can be skipped if you have a strong understanding of crypto assets based on readings above, this reading adequately summarizes the relevant issues, describes the strengths and weaknesses of current SEC and CFTC regulatory perimeters, and suggests potential solutions that you can analyze.)

19. ITIF, "A Policymaker's Guide to Blockchain," Principles to Advance Blockchain [60 pages] (Provides example use cases for crypto assets to help round out your understanding of the industry, and provides additional policy considerations you can address in your briefing. There is no need to read the entire report. Pages 29 to 37 are most relevant.)

20. "Silicon Valley Is Into Bitcoin. It Wants to Keep Washington Out," The Wall Street Journal, April 19, 2018

    https://www.wsj.com/articles/cryptocurrency-firms-investors-seek-exemption-from-sec-oversight-1524130200?mod=e2twp

21. CNBC, Crypto industry leaders warn Congress: Figure out regulation, or watch innovation leave the US, Sept. 25, 2018

https://www.cnbc.com/2018/09/26/crypto-leaders-to-congress-figure-out-regulation-or-innovation-leaves.html

22. Deloite, "The tokenization of assets is disrupting the financial industry. Are you ready?"
https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/financial-services/lu-tokenization-of-assets-disrupting-financial-industry.pdf

Political Environment

23. Congress Questions The SEC On Libra, Cryptocurrency And "The Whole Blockchain Phenomenon"
https://www.forbes.com/sites/jasonbrett/2019/09/28/congress-questions-the-sec-on-libra-cryptocurrency-and-the-whole-blockchain-phenomenon/#3c50b93d5135

Optional

24. "Descriptions of 'Crypto Assets,'" Winston & Strawn, LLP (Provides a summary of the most recent and relevant financial regulatory agency complaints, announcements, guidance, and memos for reference if you desire to complete additional research.)
https://www.winston.com/images/content/1/5/v2/159397/Crypto-Law-Corner-Description-of-Crypto-Assets.pdf

PART III

CONSUMER PRODUCTS & PROTECTIONS

HARVARD LAW SCHOOL | The Case Studies

CSP054
APRIL 2020

Employee Benefits — Emergency Savings Account

ADAM SPIEGEL

Memorandum

DATE: February 2020
TO: Junior Associate
FROM: Senior Partner
RE: Emergency Savings Accounts – Commonwealth

I just learned about a great *pro bono* opportunity from the Executive Director of Commonwealth, an organization dedicated to improving the financial stability and opportunity of people in the United States.[1] She told me about an exciting project they are working on around emergency savings accounts. I would like your help analyzing the legal and policy issues that arise from their three options. So that Commonwealth can better advise potential partners, the goal is to recommend whether to proceed with any of the options and provide recommendations for how to navigate the legal and policy challenges associated with each of the three options.

This memo includes the following:

- Background on Commonwealth
- Background on Financial Insecurity in the United States
- Current FinTech Solutions
- Commonwealth's Design Options
- Legal and Policy Considerations
- Briefing Questions
- Appendices

[1] *Our Story*, COMMONWEALTH, https://buildcommonwealth.org/about/our_story (last visited Nov. 4, 2019).

Written by Adam Spiegel under the supervision of Howell E. Jackson, James S. Reid, Jr. Professor of Law at Harvard Law School. Case development at Harvard Law School is partially funded by a grant from Dechert LLP. Cases are developed solely as the basis for class discussion. They are not intended to serve as endorsements, sources of primary data, legal advice, or illustrations of effective or ineffective management.

Copyright © 2020 President and Fellows of Harvard University. No part of this publication may be reproduced, stored in a retrieval system, used in a spreadsheet, or transmitted in any form or by any means—electronic, mechanical, photocopying, recording, or otherwise—without permission. To order copies or permissions to reproduce materials please visit our website at casestudies.law.harvard.edu or contact us by phone at 617-496-1316, by mail at Harvard Law School Case Studies Program, 1545 Massachusetts Avenue – Areeda 507, Cambridge, MA 02138, or by email at HLSCaseStudies@law.harvard.edu.

Background on Commonwealth

Commonwealth is a nonprofit that works "to build solutions to financial challenges faced by financially vulnerable people."[2] To do so, Commonwealth identifies challenges, such as uncertain income and expenses, debt, savings, and financial capabilities. Commonwealth then advises on projects that "demonstrate the real-world application of a specific solution," such as Children's Savings Accounts, Prize-Linked Savings, and SaveYourRefund.[3] The majority of Commonwealth's projects relate to increasing savings for low-income Americans. This new project involves emergency savings accounts as an employee benefit and, therefore, fits right into their portfolio of projects. Your analysis of the possible proposals will be incredibly helpful as Commonwealth thinks about where to allocate its resources and, if they decide to pursue this project, how to make it as effective as possible.

Background on Financial Insecurity in the United States

In its 2017 Report on the Economic Well-Being of U.S. Households, the Federal Reserve Board found that four in ten adults self-reported that they would borrow money or sell something in order to cover a $400 emergency payment.[4] A study of the expenses of low-income households found that low-income households spent 41% of their income on housing and then the next 30% on food and transportation.[5] With health care and clothing accounting for another 10% of income, low-income households have limited earnings left over for savings or emergency expenses.[6]

The rise of income variability compounds the problem faced by those with low income, with those households experiencing a 10% increase or decrease in half the months of the year.[7] This income volatility, combined with a very small or no asset cushion, can lead to severe financial stress when households are faced with an unexpected expense.[8] The Federal Reserve Board found that the major causes of income volatility are irregular work schedules, payment through bonuses or commissions, temporary unemployment, and seasonality of work.[9]

Most products available to low-income households dealing with financial insecurity are what Todd Baker of Columbia Law School refers to as "high-cost, short-term, small-dollar credit" products.[10] These

[2] *Our Work*, COMMONWEALTH, https://buildcommonwealth.org/work (last visited Nov. 4, 2019).

[3] *Id.*

[4] BOARD OF THE FEDERAL RESERVE SYSTEM., REPORT ON ECONOMIC WELL-BEING OF U.S. HOUSEHOLDS IN 2017, 1–56, 2 (May 2018), https://www.federalreserve.gov/publications/files/2017-report-economic-well-being-us-households-201805.pdf.

[5] *See* Diane Whitmore Schanzenbach, Ryan Nunn, Lauren Bauer and Megan Mumford, *Where Does All the Money Go: Shifts in Household Spending Over the Past 30 Years,* Brookings Institute: The Hamilton Project. Fig. 1. (Jun. 2, 2016), https://www.hamiltonproject.org/papers/where_does_all_the_money_go_shifts_in_household_spending_over_the_past_30_y.

[6] *Id.*

[7] Todd Baker, *FinTech Alternatives to Short-Term Small-Dollar Credit—Helping Low-Income Working Families Escape the High-Cost Lending Trap*, Working Paper, HARVARD KENNEDY SCHOOL: MOSSAVAR-RAHMANI CENTER FOR BUSINESS AND GOVERNMENT, 1-89, 7 (May 18, 2017), https://www.hks.harvard.edu/centers/mrcbg/publications/awp/awp75.

[8] *Id.*

[9] BOARD OF THE FEDERAL RESERVE SYSTEM., REPORT ON ECONOMIC WELL-BEING OF U.S. HOUSEHOLDS IN 2015, 1–155, 19 (May 2016) https://www.federalreserve.gov/2015-report-economic-well-being-us-households-201605.pdf.

[10] Baker, *supra* note 7, at 8.

include payday loans, auto title loans, and bank overdraft protection.[11] These products are usually available to people who have little or no credit history but tend to come with high fees.[12]

Current FinTech Solutions

For customers with little or no credit history, there have been, until recently, limited alternatives to high-cost, short-term, small-dollar credits. A number of FinTech solutions have recently appeared which aim to lessen income volatility and high-cost credit options.[13] These FinTechs focus on one or more of the interlocking problems affecting low-income Americans, including: Savings Solutions, Income/Expense Variable Management, Financial/Cash Flow Management, and Digital Credit Access/Cost Improvement Lenders, to name a few.[14] Some FinTech solutions, like Qapital, use behavioral economics to gamify saving and encourage Americans to save more.[15] Other solutions, like PayActiv, allow early access to already-earned wages in advance of payday for a small fee.[16] Still other FinTechs, like Brightside, provide a combination of services, including checking and savings accounts.[17] Most importantly, Brightside offers conversations with live financial assistants to advise customers about their financial choices.[18]

Qapital markets its services directly to consumers and offers a full-service banking app along with investing and savings features, charging between $3-$12 per month for a suite of services.[19] It offers its services through third party banks and brokers. In contrast, PayActiv is embedded in a company's payroll system.[20] It allows employees to access in their periodic paycheck up to $500 of the money they have earned but have not yet received.[21] Specifically, if an employee is paid every two weeks, they can borrow the money they have earned over the course of the two weeks through PayActiv before they receive their paycheck.[20] PayActiv charges a $5 fee for each pay period an employee uses the service, which would be a high APR depending on the amount of pay accessed, although less than the typical $25 fee charged by payday lenders.[21] PayActiv is repaid through automatic payroll deductions, making defaults much lower than defaults for payday lenders.[22] PayActiv allows for automatic payroll deductions to be sent directly to a savings account to help employees save or cover emergency expenses.[23] Brightside also works with employers to provide their solutions to employees.[24]

[11] *Id.*

[12] *Id.* at 17.

[13] Baker, *supra* note 7 at 42.

[14] *Id.*

[15] QAPITAL, https://www.qapital.com/ (last visited Nov. 4, 2019) ("[S]aving for something special is fun. Qapital helps you get there with Goals and Rules — two clever ways to supercharge your saving with little effort.").

[16] Anne Tergesen, *Some Companies Offer a New Benefit: Payroll Advances and Loans*, WALL STREET JOURNAL, Sept. 2, 2019, https://www.wsj.com/articles/some-companies-offer-a-new-benefit-payroll-advances-and-loans-11567416601.

[17] *Why Choose Us*, BRIGHTSIDE, https://www.gobrightside.com/#why-choose-us (last visited Nov. 4, 2019).

[18] *Id.*

[19] *About Us*, QAPITAL, https://www.qapital.com/about-us/ (last visited Nov. 4, 2019).

[20] *Id.*

[21] *Id.*

[22] *Id.*

[23] EVEN, https://even.com/ (last visited Jan. 4, 2020).

[24] Brightside, *supra* note 17.

SalaryFinance, a U.K.-based and employer-sponsored FinTech now operating in the U.S., found that its employee installment lending, savings programs, and financial management "significantly increases financial system access for many employees who would be forced to rely on payday loans, bank overdrafts and other very high-cost and unattractive alternatives."[25] The same study also looked at the impact of PayActiv and its $5 fee-lending model, and concluded that it should also have similar effects because it was offering credit at lower rates than the high-cost alternatives.[26] Some academics have argued that employers should use some of these new products to do more to help their employees deal with financial insecurity.[27]

Helping employees deal with financial instability may be valuable for an employer's bottom line.[28] One of the largest costs for employers can be employee turnover, with turnover costs estimated at 16% of annual salary for high-turnover, low-paying jobs.[29] Many consumer-facing industries struggle immensely with high employee turnover, with estimates of annual turnover rates of 59% for retail generally and 30-45% for call-center employees.[30] It is also expected that improving the financial stability of employees would reduce absenteeism and improve employee performance.[31]

The SalaryFinance study also found evidence suggesting that a FinTech firm that combats the financial instability of workers can reduce the turnover rate of employees.[32] The study compared employer's historical turnover rate with their turnover rate when partnered with SalaryFinance and found a reduction in turnover.[33] Moreover, the study found that employees who used SalaryFinance were less likely to leave the employer than employees who did not use SalaryFinance.[34] While the study did not have perfect controls and other possible explanations cannot be ruled out, the findings suggest that helping employees combat financial instability can reduce turnover, thereby improving an employer's bottom line. Similar results were found in the study when looking at the FinTech PayActiv.[35]

Therefore, an emergency savings program may be appealing to employers because of the potential reduction in turnover and decreased costs, and to employees because of an increased ability to save for emergencies and unexpected expenses.

[25] Todd H. Baker and Snigdha Kumar, The Power of the Salary Link: Assessing the Benefits of Employer-Sponsored FinTech Liquidity and Credit Solutions for Low-Wage Working Americans and their Employers, Working Paper, Harvard Kennedy School: Mossavar-Rahmani Center for Business and Government, 1-19, 9 (May 9, 2018), https://www.hks.harvard.edu/sites/default/files/centers/mrcbg/working.papers/88_final.pdf.

[26] *Id.* at 10-11.

[27] Timothy Ogden and Jonathan Morduch, Too Many Americans Suffer from Financial Instability. Their Employers Can Help Fix It. Harvard Business Review, Dec. 14, 2017, https://hbr.org/2017/12/too-many-americans-suffer-from-financial-instability-their-employers-can-help-fix-it.

[28] Baker, *supra* note 25, at 13.

[29] *Id.* at 11.

[30] *Id.* at 10–11.

[31] Baker, *supra* note 7, at 57.

[32] Baker, *supra* note 25, at 12.

[33] *Id.*

[34] *Id.*

[35] *Id.* at 16.

Commonwealth's Design Options

Commonwealth is an advisor and consultant to employers and FinTechs as they try to provide emergency savings for employees. In that role, Commonwealth is looking to stimulate market solutions to these issues, not attempting to subsidize an emergency savings program on a long-term basis. The potential economic incentives for each of the three design options, therefore, will be discussed briefly along with the description of the option. Commonwealth would like to better understand the legal and policy challenges associated with emergency savings accounts, including both the legal and regulatory environments, as well as the potential effectiveness of its strategy. This is particularly important because FinTechs generally do not have the resources and expertise to work through the relevant legal issues and convince management at large companies to take up emergency savings accounts. Commonwealth, then, can play an important role in overcoming barriers for both entities to stimulate a market solution to this issue. With that goal in mind, Commonwealth is currently considering three different design options, with distinct positives and negatives.

Highly-Integrated FinTech

The first option would be a highly-integrated FinTech. A highly-integrated FinTech would be integrated into the employer's payroll system and would allow employees to sign up to automatically deduct a certain percentage of their income to be invested and held in an emergency savings account.[36] The funds would be held in an FDIC insured account.[37] One large benefit of the highly-integrated FinTech solution is the ability for automatic payroll deductions for deposit into the employee savings account. The benefit of automatic savings would mean that employees do not have to consciously decide each month to save. Savings would increase, just as the percentage of employee enrollment and investment increases when 401(k) retirement accounts require employee opt-out instead of employee opt-in.[38] However, this design option would likely require the most investment of time and resources from an employer to integrate its system with a FinTech. Additionally, employers may not control their own payroll system and may, instead, use a company such as ADP.[39] This means that companies like ADP would have the opportunity to integrate an emergency savings option into their system, which would allow employers to then add it as a component of their payroll system. Although the technical costs and hurdles to this sort of integration are likely high, research has shown that there are significant benefits for both employees and employers when employees have increased financial stability and savings.[40] It might be difficult to convince employers that the benefits outweigh the costs in the event that the costs of implementation

[36] Tergesen, *supra* note 16 (describing how PayActiv is able to provide lower cost loans because it has access to payroll information and can automatically deduct the required payments from the following paycheck).

[37] The FinTech would partner with a bank to offer and hold the savings account, ensuring that the account has deposit insurance. Another method is to hold the account as a Brokerage Cash Management Account, which has a more complicated set of contracts and partnerships to provide the standard suite of banking services and deposit insurance. Another method is to hold funds in a non-deposit account that can be accessed with a debit card which, however, would not provide deposit insurance.

[38] Dan Kadlek, *These Simple Moves By Your Employer Can Drastically Improve Your Retirement*, MONEY (May 12, 2015), http://money.com/money/3854692/retirement-401k-simple-choices-merrill-lynch/.

[39] ADP, https://www.adp.com/ (last visited Jan 2., 2020).

[40] Baker, *supra* note 25, at 2–3.

are high. However, because many employers use the same large payroll companies, getting a large payroll company to integrate a savings account into its system could reach a large number of employees.

The long-term economic viability of this plan would likely be driven by banks' desire for stable deposits. While individual emergency savings accounts may fluctuate in value, a bank having a large number of emergency savings accounts would likely result in a relatively large pool of stable deposits. Banks may then have an incentive to support the development and maintenance of the emergency savings program. Separately, a payroll company like ADP would likely have an interest in innovating to provide new features to employers in order to compete with other payroll companies for business.

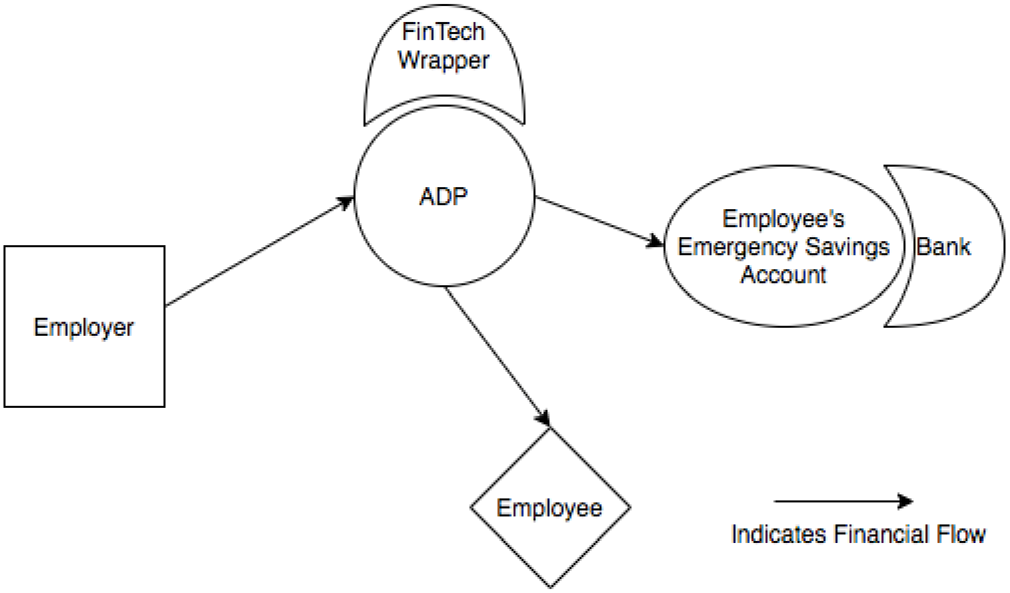


Figure 1. Highly-Integrated FinTech Diagram

Retirement Account Sidecar Savings Account

The second option would be to add an Emergency Savings Account sidecar to current employer-sponsored retirement plans and have the plan be administered by retirement account administrators such as John Hancock. This option would still allow for high-integration and automatic payroll deductions, but would impose an additional burden on retirement account administrators. The plan would allow an employee to fund the savings account with after-tax income and then, when that account reached a set amount with which the employee is comfortable, the income stream would be directed into the employee's retirement savings account.[41] The "sidecar" option would be limited to employees of employers who have an employer-sponsored retirement plan.

The long-term economic viability of this option would likely be driven by the incentives of the retirement administrators. Retirement administrators have an interest in attracting more employees to

[41] Amanda Umpierrez, Mechanics of Implementing a Sidecar Savings Account: Keeping retirement plan contributions rolling in while also allowing employees to save for emergencies, PLAN SPONSOR (Oct. 22, 2019), https://www.plansponsor.com/in-depth/mechanics-behind-implementing-sidecar-savings-account/.

open retirement accounts, including younger and lower-income workers who are less likely than older and higher-income employees to have retirement accounts. By offering emergency savings programs, more employees would be using accounts with retirement administrators, providing more customers for the retirement account administrators.

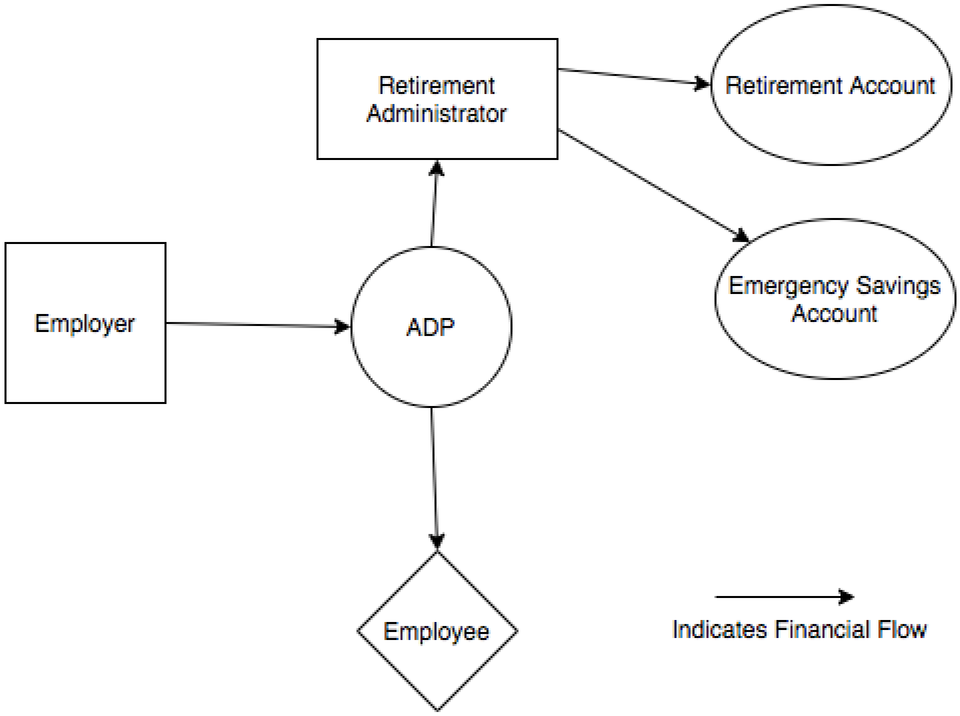


Figure 2. Retirement Account Sidecar Savings Account Diagram

Low-Integration FinTech

The third option would be for employers to recommend a low-integration FinTech, such as Qapital, to their employees. Because the service would not be fully integrated, the technical costs of this option would be much lower. It is possible that employees could still make automatic payroll deductions to a Qapital savings account, but that would depend on each employer's—and Qapital's—willingness to do so. At the very least, employers would function as a method of informing employees of the services of FinTechs and how they can help improve an employee's financial wellbeing. Nevertheless, because the costs of implementation for employers would be relatively low, more employers may be willing to participate in this type of program. Costs to employees would likely be higher with this option because savings apps tend to charge user fees for their services.

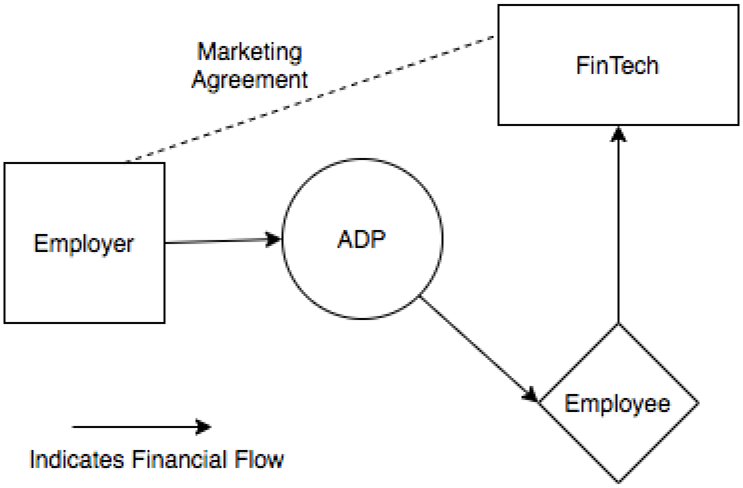


Figure 3. Low-Integration FinTech Diagram

Summary

Commonwealth wants a proposal that will maximize the effectiveness of any savings program and will reach the greatest number of low-income Americans. The option of using retirement account administrators may not be able to reach as many low-income Americans because it requires employers to be offering retirement plans. There are benefits to that approach, however, because these potential partners already have the infrastructure to automatically deduct income from payroll and direct it to a savings account, particularly retirement account administrators such as John Hancock. The other two options would not be limited to the employees who work for employers that already provide retirement plans.

Commonwealth Design Options Summary:

- High-Integration between FinTech and employer's payroll system;
- Sidecar Savings Account Integrated with Retirement Account Administrator like John Hancock; and
- Low-Integration with FinTech (such as Qapital) where the employer encourages employees to sign up but provides little or no additional integration. The employer effectively "sponsors" a FinTech for its employees.

Key Legal Considerations

The following legal considerations arise when reviewing Commonwealth's proposal. For each of the legal considerations that follow, Commonwealth wishes to learn the pros and cons of each of the three design options that Commonwealth is considering, and how they can advise partners about the legal issues involved, including any legal or regulatory uncertainty. A comprehensive understanding of each of the potential legal benefits or hurdles would allow Commonwealth to provide the best guidance to employer and FinTech partners. The legal issues that need consideration include:

- Federal Reserve Board's Regulation D;
- State and Federal Money Transmitter Laws;
- Electronic Funds Transfer Act;
- ERISA;
- Student Loan Payment IRS Private Letter Ruling;
- Wage Garnishment; and
- Asset Limits for Eligibility for Certain Public Benefits.

Regulation D

The Federal Reserve Board is required under Section 19 of the Federal Reserve Act to impose reserve requirements on certain deposits and other liabilities of depository institutions.[42] Regulation D implements this reserve requirement and defines which institutions and deposits are subject to reserve requirements.[43] The regulation identifies transaction accounts, which are accounts from which the account holder is permitted to "make transfers or withdrawals by negotiable or transferable instrument, payment order of withdrawal," or by certain other means.[44] These types of accounts (and certain others) are subject to reserve requirements, the level of which depends on the amount of a depository institution's transaction accounts.[45]

In contrast, savings accounts are not subject to reserve requirements.[46] However, savings accounts have a monthly limit of six "convenient" transfers and withdrawals.[47] Any transfer or withdrawal made by check or debit card, or any automatic withdrawal, count against the limit of six transfers.[48] Withdrawals made in person at a bank, by mail, from an ATM, or withdrawal requests initiated by telephone but disbursed by mailed check, do not count against the limit.[49]

It is an important design priority for Commonwealth to call the accounts savings accounts and to allow unfettered access for employees. This fits with Commonwealth's mission of encouraging savings by Americans and having those funds be available to employees in an emergency, however often one arises. In addition, as a marketing matter, less complexity associated with the account could increase adoption of emergency savings accounts by employees. Further, some psychology studies have shown that savings increases peace of mind and overall well-being.[50] Calling it a savings account may also have additional benefits.

[42] Compliance Guide to Small Entities: Regulation D: Reserve Requirements of Depository Institutions, BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM, https://www.federalreserve.gov/supervisionreg/regdcg.htm (last visited Nov. 4, 2019).

[43] *Id.*

[44] *Id.* (citing 12 CFR § 204.2).

[45] Compliance Guide, *supra* note 42.

[46] *Id.*

[47] *Id.*

[48] *Id.*

[49] *Id.*

[50] Cory Stieg, *Millennials who buy less and save more are happier*, CNBC (Oct. 10, 2019), https://www.cnbc.com/2019/10/10/study-millennials-who-buy-less-and-save-more-are-happier.html.

There are a number of provisions that regulate advertising and other information that is provided to customers of depository institutions. These provisions are known as Regulation DD, which are promulgated by the Consumer Financial Protection Bureau in order to implement the Truth in Savings Act.[51] A key concern is whether the account may be associated with the term "savings" if the account is designed as a transaction account.[52] It is not clear what the relationship between Regulation D, which regulates depository institutions, and Regulation DD, which regulates advertising and disclosures to customers of depository institutions actually is, but it is an important consideration for this project.

Questions related to Regulation D

1. Should the Emergency Savings Account be a transaction account or a savings account?
2. If it should be a transaction account, can it still be called an "emergency savings account"?

Money Transmitter Laws

Federal money transmitter laws and regulations are overseen by the Financial Crimes Enforcement Network (FinCen) of the U.S. Treasury.[53] Each state, except Montana, has its own version of a money transmitter law.[54] The goal of the Federal money transmitter laws and FinCen is to "safeguard the financial system from illicit use, combat money laundering, and promote national security."[55] Commonwealth wants to know if any part of this project could make the employer a money transmitter, which would require registering with FinCen under the Money Laundering Suppression Act of 1994[56] and obtaining a state license.[57]

Questions related to money transmitter laws

1. By creating an emergency savings account for employees, would employers become subject to money transmitter laws and, therefore, need to register with FinCen and state regulators?
2. Is it sufficient that employer's payroll processors, such as ADP, are already registered as money transmitters?

[51] 12 CFR § 1030.1(a).

[52] One interesting puzzle related to this issue is Wal-Mart's prepaid card that offers a prize-linked "savings Vault account" along with the card. Based on the cardholder agreement, the money loaded onto the prepaid card is held at a custodial account at Green Dot Bank. The account is a transaction account. But owners of the card also get a "savings Vault account" that allows the user to set aside a portion of the card's balance. This portion of the balance cannot be accessed from the card directly. The Service Agreement for the MoneyCard Vault notes that the account "is not an independent account or card. It is a separate part of your card that is set aside and cannot be accessed by your card directly. The Vault is not a savings account, and it does not pay interest." It is not clear how Wal-Mart is able to use the word "savings" for what appears to be a transaction account.

[53] *Mission*, FINANCIAL CRIMES ENFORCEMENT NETWORK, https://www.fincen.gov/about/mission (last visited Jan. 4, 2020).

[54] FinTech Survey: Money Transmission, George Washington Center for Law, Economics, and Finance, http://www.fintechsurvey.org (last visited Jan. 4, 2020).

[55] FINANCIAL CRIMES, *supra* note 52.

[56] *Fact Sheet on MSB Registration Rule*, FINANCIAL CRIMES ENFORCEMENT NETWORK, https://www.fincen.gov/fact-sheet-msb-registration-rule (last visited Jan. 4, 2020).

[57] FinTech Survey, *supra* note 53.

Electronic Fund Transfer Act

The Electronic Fund Transfer Act of 1978 was designed to protect consumers who engage in electronic funds transactions.[58] These services include "transfers through automated teller machines, point-of-sale terminals, automated clearinghouse systems…and remote banking programs."[59] It creates a number of penalties for, among other things, unauthorized transfers of funds.[60]

For our purposes, regulations were adopted governing how employers use direct deposit and electronic transfers.[61] We want to determine whether we would run afoul of these provisions by how we design the emergency savings account.

The Consumer Financial Protection Bureau (CFPB) is responsible for overseeing the Electronic Fund Transfer Act.[62] The CFPB has two programs that might be useful for us to resolve any regulatory uncertainty surrounding the EFTA: the Compliance Assistance Sandbox and the No-Action Letter Policy.[63] The Compliance Assistance Sandbox allows companies to obtain a safe harbor for innovative products when it is not clear whether three laws apply: the Electronic Fund Transfer Act, the Truth in Lending Act, and the Equal Credit Opportunity Act.[64] The No-Action Letter policy is a bit broader and allows companies to get a commitment that the CFPB will take no enforcement action against a company for a particular potential violation of a consumer law.[65] To date, there has been at least one No-Action Letter provided by the CFPB.[66] Two years later, the CFPB provided a report on the success of the No-Action Letter and their monitoring of Upstart, the company that requested and received the No-Action Letter.[67]

Questions related to the Electronic Fund Transfer Act

1. Would any of the three options be at risk of violating the Electronic Fund Transfer Act?
2. If so, should we apply to the CFPB to resolve any potential regulatory uncertainty?

ERISA

The Employee Retirement Income Security Act of 1974 sets "minimum standards for most voluntarily established retirement and health plans in private industry to provide protection for

[58] Fed. Res. Sys., *Electronic Fund Transfer Act*, BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM, 1 (2018), https://www.federalreserve.gov/boarddocs/caletters/2008/0807/08-07_attachment.pdf.

[59] *Id.*

[60] *Id.* at 12.

[61] 12 C.F.R. 1005.10(e).

[62] CFPB, *Electronic Fund Transfers (Regulation E); Amendments*, CFPB, https://www.consumerfinance.gov/policy-compliance/rulemaking/final-rules/electronic-fund-transfers-regulation-e/ (last visited Nov. 4, 2019).

[63] *Innovation*, CFPB, https://www.consumerfinance.gov/about-us/innovation/ (last visited Nov. 4, 2019) (providing overview of both programs).

[64] CFPB, *Policy on the Compliance Assistance Sandbox*, CFPB (Sept. 10, 2019), at 3, https://files.consumerfinance.gov/f/documents/cfpb_final-policy-on-cas.pdf.

[65] *Id.*

[66] CFPB, *CFPB Announces First No-Action Letter to Upstart Network*, CFPB, Sept. 14, 2017, https://www.consumerfinance.gov/about-us/newsroom/cfpb-announces-first-no-action-letter-upstart-network/.

[67] CFPB, *An update on credit access and the Bureau's first No-Action Letter*, CFPB, Aug. 6, 2019, https://www.consumerfinance.gov/about-us/blog/update-credit-access-and-no-action-letter/.

individuals in these plans."[68] ERISA establishes a number of requirements on plans and "provides fiduciary responsibilities for those who manage and control plan assets."[69] Being a fiduciary creates a number of requirements, including to "run the plan solely for the interest of participants and beneficiaries and for the exclusive purpose of providing benefits and paying plan expenses."[70] Moreover, "[f]iduciaries must act prudently and must diversify the plan's investments in order to minimize the risk of large losses."[71]

In sum, the costs of being a fiduciary for an employer would be high. If it seemed likely that participation in an employee benefit plan that created emergency savings accounts would lead to fiduciary responsibilities, Commonwealth is concerned that some employers might not participate at all to avoid the potential legal risks. We will want to figure out if this plan is subject to ERISA, and if it is, how we might be able to structure it so that employers won't become fiduciaries, or risk becoming fiduciaries.

Questions related to ERISA

1. Would creating an emergency savings account for employees subject an employer to fiduciary responsibilities under ERISA?
2. If it might, is there a way to structure the account so that does not happen? If so, how?

Student Loan IRS Private Letter Ruling

Recently, a private company asked the Internal Revenue Service (IRS) for a Private Letter Ruling to pursue an innovation in its retirement plan.[72] The company wanted to allow employees to make Student Loan Payments but not lose out on the employers' 401(k) matching contribution.[73] Under the plan, if an employee made student loan payments in the amount of at least 2% of the employee's salary, the company would provide a matching payment of 5% of salary to the employee's 401(k) account.[74] If the employee does not meet the 2% threshold, she can meet the threshold by making contributions to her 401(k) account.[75] Moreover, enrolling in this version of the plan does not prevent the employee from making payments to her 401(k) account generally.[76]

Commonwealth is interested in whether employers can possibly build on this innovative scheme by providing an employer matching contribution to a 401(k) plan if the employee contributed to the emergency savings account, which might create additional incentives for employees to enroll in an emergency savings account. This, in turn, might give employers reason to invest in setting up a program

[68] Dep't of Labor, *Employee Retirement Income Security Act (ERISA)*, U.S. DEP'T OF LABOR, https://www.dol.gov/general/topic/retirement/erisa (last visited Nov. 4, 2019).

[69] *Id.*

[70] *Id.*

[71] *Id.*

[72] Camilo Maldonado, *IRS Ruling Allows Company to Match Employees' Student Loan Payments Into Their 401(k)*, FORBES (Aug. 29, 2018), https://www.forbes.com/sites/camilomaldonado/2018/08/29/irs-ruling-allows-company-to-match-employees-student-loan-payments-into-401k/#34ce72e62861.

[73] *Id.*

[74] *Id.*

[75] *Id.*

[76] *Id.*

because this extra incentive might give the employer enough enrollees for the program to be valuable in reducing turnover.

The program would be somewhat similar to the plan described in the IRS Private Letter Ruling. If employees contribute some percentage of their income to an emergency savings account, an employer would then make matching payments to the employees 401(k) account. This possibility might be easier if we integrate with retirement account administrators, but it could still be done through a FinTech integrated into an employer's payroll system. It is even possible, theoretically, to engineer this program through a low-integration FinTech, although the monitoring of savings actually made would be more difficult.

There are a number of ways to go in this direction. First, Commonwealth could rely on the existing IRS Private Letter Ruling as permitting experimentation with 401(k) plans, and then employers could create the program to allow matching if an employee puts funds toward the employee's emergency savings account. Second, employers could apply to the IRS for a Private Letter Ruling to resolve any uncertainty around whether the proposed plan would pass muster. Third, it is possible that the whole idea might be overly complicated and run afoul of the law.

Questions about IRS Private Letter Ruling

1. Could the IRS Private Letter Ruling be relied upon by employers to structure their own twist on a 401(k) matching contribution?
2. Would it be appropriate for each employer to apply to the IRS for a Private Letter Ruling about the specifics of its plan?
3. Should employers be encouraged to pursue a 401(k) matching contribution for the emergency savings account?

This question brings an additional complication, which may be a complication with the creation of any emergency savings account offered to employees. To qualify for various tax deductions and credits, the IRS requires that a company's 401(k) plan does not discriminate in favor of high-income workers.[77] To do so, the IRS employs a number of non-discrimination tests.[78] In its Private Letter Ruling, the IRS noted that student loan payment matching contributions would not be considered for 401(m) non-discrimination testing purposes.[79] However, what it called the true-up matching contribution (matching for an employee's contribution to a 401(k) plan) was considered matching contributions for 401(m) testing.[80]

This treatment of true-up matching could create a potential problem for employers. If they implement a matching program and too many low-income employees opted-in to it, the employer's 401(k) plan may appear to be discriminating in favor of high-income employees because, as low-income employees divert funds to emergency savings, the pool of employees left in the 401(k) plan would be high-

[77] 401(k) Nondiscrimination Tests Explained, PLAN SPONSOR, Dec. 1, 2014, https://www.plansponsor.com/401k-nondiscrimination-tests-explained/.

[78] *Id.*

[79] I.R.S. Priv. Ltr. Rul. 2018-33012 (May 22, 2018), at 2.

[80] *Id.*

income employees who would not be inclined to take advantage of the emergency savings accounts. This possibility could scare off employers from participating in any program that Commonwealth proposes if a program would encourage low-income employees to drop out of an employer's 401(k) plan. It is not clear how much of an effect the creation of an emergency savings account employee benefit would have on the nondiscrimination issue, but Commonwealth would like your input on the question.

Questions about 401(m) non-discrimination testing

1. Should employers be concerned about whether the creation of an emergency savings account could jeopardize their non-discrimination tests for their 401(k) plans?
2. Is there a way that employers might be able to avoid this issue?

Wage Garnishment

Employers have certain responsibilities when one of their employee's wages are being garnished due to a court order.[81] These include withholding the amount that is being garnished.[82] Both state and federal laws regulate the percentage of a person's income that can be garnished for wages, usually depending on the purpose of the wage garnishment, *e.g.*, child support, student loans.[83] Diverting some of an employee's income to an emergency savings account could pose a problem if that means the money is no longer being held for wage garnishment. It could create a clash between claims to income.

Question about Wage Garnishment

1. Will creating an emergency savings account program worsen the issues faced by employers relating to wage garnishment?

Asset Limits for Eligibility for Certain Public Benefits

Finally, the target population for this innovation is low-income Americans. There are a number of public benefit programs in the United States that have asset limits (on top of the income limits necessary to qualify for the programs) that can prevent Americans with assets greater than a particular threshold from receiving benefits.[84] Because our target population might be eligible for these programs, we do not want the creation of an emergency savings account to jeopardize the benefits upon which some low-income Americans rely. As an added complication, states can impose their own asset limits.[85] There is no federal asset limit for Temporary Assistance for Needy Families (TANF), but states can impose one.[86] For

[81] *Employers Responsibilities for Wage Garnishment*, BENEFIT MALL, https://employers.benefitmall.com/blog/employer-responsibilities-wage-garnishment (last visited Nov. 4, 2019).

[82] *Id.*

[83] Dep't of Labor, *Fact Sheet #30, Federal Wage Garnishment Law, Consumer Credit Protection Act's Title III*, U.S. DEP'T OF LABOR, (Oct. 2019), https://www.dol.gov/whd/regs/compliance/whdfs30.htm.

[84] Maureen Pirog, Edwin Gerrish and Lindsey Bullinger, *TANF and SNAP Asset Limits and the Financial Behavior of Low-Income Households*, PEW CHARITABLE TRUSTS, 1–30, 2, Sept. 2017, https://www.pewtrusts.org/-/media/assets/2017/09/tanf_and_snap_asset_limits_and_the_financial_behavior_of_low_income_households.pdf.

[85] *Id.*

[86] *Id.*

Supplemental Nutrition Assistance Program (SNAP), there is a federal asset limit of $2,250 in liquid assets or $3,250 if the household includes an elderly individual or individual with disabilities.[87] However, states can relax the federally imposed asset limit, and many have.[88]

Questions about Asset Limits for Public Benefits

1. How can an employer's emergency savings program avoid jeopardizing an employee's asset limits?
2. How can we prevent fear of reaching the asset limit from reducing the number of employees who are interested in signing up for the program?

Briefing Questions

Before sending you off to research, I just wanted to reiterate the two main objectives of this assignment. There are a number of questions related to each of the legal considerations described above and you should endeavor to answer them. Those answers should inform your advice for the two most important questions to which Commonwealth would like answers. These answers will help them better advise employers, FinTechs, and other partners on this project. The two broad questions are:

1. Should Commonwealth move forward with encouraging employers to provide emergency savings accounts as a benefit to their employees?
2. What are the legal and policy benefits and complications for each of the three options? Which seems to be the best option to choose?

Attached to this memorandum, you will find a number of appendices provided to aid your analysis. Thank you for taking on this assignment. I am looking forward to your proposal.

[87] *Id.*

[88] *Id.*

Appendices

Background on Financial Instability

1. Anna Bahney, *40% of Americans can't cover a $400 emergency* expense, CNN MONEY (May 22, 2018), https://money.cnn.com/2018/05/22/pf/emergency-expenses-household-finances/index.html.
2. Jay Lindsay, *Is the $400 problem best solved by financial education or behavioral science?*, FEDERAL RESERVE BANK OF BOSTON (Jul. 1, 2019), https://www.bostonfed.org/news-and-events/news/2019/07/fighting-the-400-dollar-problem-with-financial-education-and-behavioral-science.aspx.

Current FinTech Solutions

3. Timothy Ogden and Jonathan Morduch, *Too Many Americans Suffer from Financial Instability. Their Employers Can Help Fix It*, HARVARD BUSINESS REVIEW (Dec. 14, 2017), https://hbr.org/2017/12/too-many-americans-suffer-from-financial-instability-their-employers-can-help-fix-it.
4. Anne Tergesen, *Some Companies Offer a New Benefit: Payroll Advances and Loans*, WALL STREET JOURNAL (Sept. 2, 2019), https://www.wsj.com/articles/some-companies-offer-a-new-benefit-payroll-advances-and-loans-11567416601.
5. Todd H. Baker and Snigdha Kumar, *The Power of the Salary Link: Assessing the Benefits of Employer-Sponsored FinTech Liquidity and Credit Solutions for Low-Wage Working Americans and their Employers*, Working Paper, 1-19, 9, HARVARD KENNEDY SCHOOL: MOSSAVAR-RAHMANI CENTER FOR BUSINESS AND GOVERNMENT, 1-89, 7 (May 9, 2018), https://www.hks.harvard.edu/sites/default/files/centers/mrcbg/working.papers/88_final.pdf.

Commonwealth's Design Options

6. Amanda Umpierrez, Mechanics of Implementing a Sidecar Savings Account: Keeping retirement plan contributions rolling in while also allowing employees to save for emergencies, PLAN SPONSOR (Oct. 22, 2019), https://www.plansponsor.com/in-depth/mechanics-behind-implementing-sidecar-savings-account/.
7. Teresa Ghilarducci, Workplace Retirement Coverage Drops And The System Continues to Fail, FORBES (Oct. 15, 2018 5:44 PM), https://www.forbes.com/sites/teresaghilarducci/2018/10/15/workplace-retirement-plan-coverage-continues-to-drop-and-fail/#26efb4eb62e4.

Key Legal Issues

Regulation D

8. FEDERAL RESERVE BOARD, CONSUMER COMPLIANCE HANDBOOK: REGULATION D (2011), https://www.federalreserve.gov/boarddocs/supmanual/cch/int_depos.pdf.

9. Kate Ashford, *How Regulation D Affects Your Savings Account*, MAGNIFY MONEY (April 18, 2019), https://www.magnifymoney.com/blog/banking/regulation-d/.
10. Computation of required reserves, 12 C.F.R. § 204.4 (2018).
11. Authority, purpose, coverage, and effect on state laws, 12 C.F.R. § 1030.1 (2019) (providing overview of Regulation DD issued to implement Truth in Savings Act).
12. Definitions, 12 C.F.R. § 1030.2 (2019).
13. General disclosure requirement, 12 C.F.R. § 1030.3 (2019).
14. Advertising, 12 C.F.R. § 1030.8 (2019).

Money Transmitter Laws

15. 18 U.S.C. § 1960 (prohibiting unlicensed money transmitting businesses).
16. 31 C.F.R. § 1010.100(ff) (providing definition of Money Services Businesses).

Electronic Fund Transfer Act

17. Bill Fray, *Electronic Fund Transfer Act*, DEBT.ORG, https://www.debt.org/credit/your-consumer-rights/electronic-fund-transfer-act/, (last visited Nov. 4, 2019).
18. Preauthorized transfers, 12 C.F.R. 1005.10(e) (2016).
19. Consumer Financial Protection Bureau, Comment for 1005.10 Preauthorized Transfers 10(e)(2) (2019), https://www.consumerfinance.gov/policy-compliance/rulemaking/regulations/1005/Interp-10/#10-e-1-Interp-4-i.
20. Alan S. Kaplinsky, *CFPB finalizes product sandbox proposal and changes to trial disclosure, no-action letter policies; discloses plans to propose interpretive letter program*, BALLARD SPAHR CONSUMER FINANCE MONITOR (Sept. 12, 2019), https://www.consumerfinancemonitor.com/2019/09/12/cfpb-finalizes-product-sandbox-proposal-and-changes-to-trial-disclosure-no-action-letter-policies-discloses-plans-to-propose-interpretive-letter-program/.
21. Upstart Network, Inc., CFPB No-Action Letter (Sept. 14, 2017).
22. Patrice Ficklin and Paul Watkins, *An Update on credit access and the Bureau's first No-Action* Letter, CONSUMER FINANCIAL PROTECTION BUREAU, (Aug. 6, 2019), https://www.consumerfinance.gov/about-us/blog/update-credit-access-and-no-action-letter/.

ERISA

23. 29 U.S.C. § 1002 (defining "employee welfare benefit plan").
24. 29 U.S.C. § 1003 (describing what plans are covered by ERISA).
25. 29 CFR § 2510.3-1 (providing guidance on definition of "employee welfare benefit plan").
26. The Alpha Group, *ERISA Compliance FAQs: What is an ERISA plan?*, LEGISLATIVE BRIEF (Nov. 2014),
27. https://www.thealphaga.com/portals/16/assets/pdf/erisa_compliance_faqs_what_is_an_erisa_plan.pdf.

28. U.S. Dep’t of Labor, Field Assistance Bulletin No. 2004-01 (Apr. 7, 2004) (discussing whether health savings accounts are subject to ERISA as “employee welfare benefit plans”).

Student Loan IRS Private Letter Ruling

29. I.R.S. Priv. Ltr. Rul. 2018-33012 (Aug. 17, 2018).

30. Craig P. Hoffman, *401(k) Student Loan Matching Program — Private Letter Ruling 2018-33012*, Trucker Huss (Jun. 2019), https://www.truckerhuss.com/2019/06/401k-student-loan-matching-programs-private-letter-ruling-2018-33012/.

31. Patty Kujawa, *Student-Loan Matching Hits Snags*, Workforce (Jul. 22, 2019), https://www.workforce.com/2019/07/22/student-loan-matching-hits-snags/.

32. Internal Revenue Service, *Understanding IRS Guidance – A Brief Primer* (last updated Nov. 6, 2019), https://www.irs.gov/newsroom/understanding-irs-guidance-a-brief-primer.

33. Robert W. Wood, *No Virginia, You Can’t Rely on IRS Rulings*, Forbes (Oct. 10, 2010 9:10 AM), https://www.forbes.com/sites/robertwood/2010/10/07/no-virginia-you-cant-rely-on-irs-rulings/#668412a95911.

34. Internal Revenue Service, 401(k) Plan Fix-It Guide (Jun. 18, 2019).

35. *Safe Harbor 401(k): The 2019 Guide for Business Owners*, Guideline (Jul. 1, 2019), https://www.guideline.com/blog/safe-harbor-401k-plan/.

Wage Garnishment

36. U.S. Dep’t of Labor, Wage & Hour Div., Fact Sheet #30: The Federal Wage Garnishment Law, Consumer Credit Protection Act’s Title III (CCPA) (Nov. 2016).

37. Top Tax Staff, *An Employer’s Guide to IRS Wage Garnishment*, Tax Matters – The Top Tax Defenders Blog (Dec. 12, 2019), https://www.toptaxdefenders.com/blog/an-employers-guide-to-irs-wage-garnishment.

Asset Limits for Public Benefits

38. Jessica Gehr, *CLASP Policy Brief: Eliminating Asset Limits: Creating Savings for Families and State Governments*, The Center for Law and Social Policy (Apr. 2018), https://www.clasp.org/sites/default/files/publications/2018/04/2018_eliminatingassetlimits.pdf

39. Maureen Pirog, Edwin Gerrish and Lindsey Bullinger, *TANF and SNAP Asset Limits and the Financial Behavior of Low-Income Households*, A Report to The Pew Charitable Trusts (Sept. 2017), https://www.pewtrusts.org/-/media/assets/2017/09/tanf_and_snap_asset_limits_and_the_financial_behavior_of_low_income_households.pdf.

HARVARD
LAW SCHOOL | The Case Studies

CSP057
MARCH 2020

Machine Learning in the Underwriting of Consumer Loans

YINAN LIU AND TALIA GILLIS

Memorandum

DATE: March 2020

TO: Senior Counsel

FROM: Director for the Office of Innovation at Consumer Financial Protection Bureau

RE: Disparate Impact Analysis for Algorithmic Decision Making

On February 11, 2019, President Trump issued an executive order[1] launching the American AI Initiative following up on the recommendations of the 2018 White House Summit on Artificial Intelligence for American Industry.[2] The initiative will focus the resources of the Federal government to establish America's place as the global leader in artificial intelligence (AI). One of the key areas of emphasis of this initiative is on setting AI governance standards, and ensuring that advances in AI will improve quality of life for the American people.[3]

The ability to access credit is a critical component for the quality of life for American families and individuals so that they have the opportunity to climb the economic ladder, build wealth, and achieve economic stability. In September 2018, our Bureau, the Consumer Financial Protection Bureau ("CFPB" or "Bureau") held a symposium, *Building a Bridge to Credit Visibility,*[4] aiming at expanding access to credit for consumers who face barriers to accessing credit. The Bureau estimates that 26 million Americans are "credit invisible" and that another 19 million people lack sufficient credit history, *i.e.*, "unscorable," which imposes on those consumers to substantial barriers to accessing credit or higher costs for credit. This

[1] Executive Office of the President, *Executive Order on Maintaining American Leadership in Artificial Intelligence* (February 11, 2019), https://www.whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/.

[2] The White House Office Of Science And Technology Policy, *Summary Of The 2018 White House Summit On Artificial Intelligence For American Industry* (May 10, 2018), https://www.whitehouse.gov/wp-content/uploads/2018/05/Summary-Report-of-White-House-AI-Summit.pdf.

[3] The White House Office Of Science And Technology Policy, *Accelerating America's Leadership in Artificial Intelligence* (February 11, 2019), https://www.whitehouse.gov/articles/accelerating-americas-leadership-in-artificial-intelligence/.

[4] Patrice Ficklin and J. Frank Vespa-Papaleo, *Building a bridge to credit visibility - a report on the CFPB's credit visibility symposium*, CFPB (July19, 2019), https://www.consumerfinance.gov/about-us/blog/report-credit-visibility-symposium/.

Written by Yinan Liu and Talia Gillis under the supervision of Howell E. Jackson, James S. Reid, Jr., Professor of Law at Harvard Law School. Case development at Harvard Law School is partially funded by a grant from Dechert LLP. Cases are developed solely as the basis for class discussion. They are not intended to serve as endorsements, sources of primary data, legal advice, or illustrations of effective or ineffective management.

Copyright © 2020 President and Fellows of Harvard University. No part of this publication may be reproduced, stored in a retrieval system, used in a spreadsheet, or transmitted in any form or by any means—electronic, mechanical, photocopying, recording, or otherwise—without permission. To order copies or permissions to reproduce materials please visit our website at casestudies.law.harvard.edu or contact us by phone at 617-496-1316, by mail at Harvard Law School Case Studies Program, 1545 Massachusetts Avenue – Areeda 507, Cambridge, MA 02138, or by email at HLSCaseStudies@law.harvard.edu.

burden falls upon almost 20% of the entire U.S. adult population. Credit invisibility affects some groups more than others. According to the Bureau's report, about 27-28% of minority populations are either credit invisible or have unscorable credit records. Young consumers and new immigrants are also more likely to be credit invisible.

These differences in credit access are sometimes the result of credit market discrimination. Specifically, lenders may have denied loans to some borrowers solely on the basis of race, ethnicity, and other personal traits.

More recently, the increased use of machine learning in the underwriting of consumer loans raises concerns about whether possible discriminatory use of big data is resulting in denial of equal credit access protection.[5] More specifically, alarms have been raised about whether data from historical discriminatory practice may be used to train a biased algorithm.

The Bureau is interested in identifying and regulating potential discrimination caused by machine-learning algorithms. At the same time, the Bureau also wants to encourage new strategies and innovation, including using machine-learning algorithms, to explore alternative data to improve the credit risk assessment process, and help provide affordable and sustainable credit to the "invisible" population.

The Bureau requests that a team of staff attorneys brief the Board on potential legal frameworks for supervising and enforcing algorithmic accountability in credit lending practice. The team has suggested two possible frameworks to regulate the use of machine learning algorithms. The first option is to adopt an *ex post* approach, following a new five-element burden-shifting framework proposed by the United States Department of Housing and Urban Development ("HUD") in 2019. The second option is to adopt an *ex ante* approach, a preclearing framework which evaluates lenders' algorithms before their deployment.

There is an internal debate within the legal team about which framework might be better for regulating discriminatory lending. We have been asked to evaluate the two proposals. To that end, please analyze the potential legal and policy issues that could arise from the two frameworks. Please carefully weigh each against the merits and demerits of maintaining the status quo.

Background

The Federal Fair Lending Laws

The federal fair lending laws—the ECOA[6] and the FHA[7]—prohibit discrimination in credit transactions, including but not limited to transactions related to residential real estate.

[5] Executive Office of the President, *Big Data: Seizing Opportunities, Preserving Values*, EXECUTIVE OFFICE OF THE PRESIDENT (May 1, 2014), https://bigdatawg.nist.gov/pdf/big_data_privacy_report_may_1_2014.pdf; Standing Committee of the One Hundred Year Study of Artificial Intelligence, *Artificial Intelligence and Life in 2030, One Hundred Year Study on Artificial Intelligence, Report of the 2015 Study Panel* 7 (Sept. 2016), https://ai100.stanford.edu/sites/default/files/ai_100_report_0831fnl.pdf.

[6] Equal Credit Opportunity Act, 15 U.S.C 1691, *et seq*. The CFPB has issued regulations under ECOA, known as Regulation B, 12 C.F.R. Part 1002 (2019).

[7] The Fair Housing Act, 42 U.S.C. 3601, *et seq*.

Fair Housing Act (FHA) of 1968

Title VIII of the Civil Rights Act of 1968, the Fair Housing Act (FHA), prohibits discrimination in the sale, rental, or financing of dwellings and in other housing-related activities on the basis of race, color, religion, sex, disability, familial status, or national origin.

Congress gave HUD the authority and responsibility for administering the FHA and the power to make rules to carry out the Act.

Equal Credit Opportunity Act (ECOA) of 1974

The ECOA prohibits creditors from discriminating against credit applicants on the basis of race, color, religion, national origin, sex, marital status, age, an applicant's receipt of income from a public assistance program, or an applicant's good-faith exercise of any right under the Consumer Credit Protection Act.

It is worth to note that the language used in FHA and ECOA are different. Under Section 804(a) of the FHA, it includes a result-oriented language "or otherwise make unavailable." However, ECOA does not have such language. This difference is important in understanding the Supreme Court's decision in *Housing and Community Affairs v. Inclusive Communities Project* in 2015, which will be discussed in more details later.

The Home Mortgage Disclosure Act (HMDA)

The Home Mortgage Disclosure Act (HMDA) requires many financial institutions to maintain, report, and publicly disclose loan-level information about mortgages. The public data are modified to protect applicants' and borrowers' privacy[8]. The data helps shed light on lending patterns that could be discriminatory.

Traditional Credit Pricing Practice

Traditional risk-based pricing was introduced in the late 1980s to expand credit access to American consumers. Each borrower has unique characteristics that influence the probability of default on a loan. Risk-based pricing in consumer finance tailors the price and terms of a loan based on each borrower's likelihood of repayment.

Two tools were developed to help lenders pierce the fog of uncertainty surrounding each new loan applicant, which made the widespread of risk-based pricing possible. First, credit reports issued by a third-party credit bureau "institutionalize the sharing of consumer payment data," and "reduced the cost of assessing borrower risk."[9] Second, statistical credit scoring evaluates default risks, generates specific predictions and summarizes it to be a numerical score. It gave lenders a powerful tool for rapidly and consistently evaluating loan applications while reducing processing costs. Instead of rejecting applicants with high risk, lenders can accept them and charge an appropriately higher price for the loan to cover the extra risk.

[8] 12 U.S.C. Chapter 29.

[9] Center for Capital Markets, Risk-based Pricing in Consumer Lending, https://www.centerforcapitalmarkets.com/wp-content/uploads/2013/08/CCMC_RiskBasedPricing_FINAL_to_post_10_24_2014.pdf.

Studies from Stanford and the University of Pennsylvania (Wharton) illustrate how risk-based pricing helped a lender mitigate both adverse selection and moral hazard through the adjustment of both interest rates and loan terms based on borrower risk.[10] The use of credit report data and credit scoring to prescreen borrowers brought in more lenders and the competition between lenders helped reduced finance charge rate and annual fees. This in turn helps expanding credit availability across all consumer loans.

However, despite its role in improving credit availability and affordability, critics of credit scoring have alleged that scoring models actually have an adverse effect on certain demographic groups. In a 2007 Report to Congress on the impact of credit scoring, the Federal Reserve concluded that (1) the increase in credit availability appears to hold for the population overall as well as for major demographic groups, including those of different races and ethnicities, and (2) it is true that different demographic groups have substantially different credit scores, on average.[11]

However, variables that have predictive value for credit risk will often also be correlated with demographic characteristics. Barring use of all such variables in credit scoring would undermine completely the use of credit scoring. “Risk-based pricing, by its very nature, leads to disparities based on credit characteristics, and if those discrepancies are deemed impermissible, and lenders are pushed to flatter pricing, the very consumers the government seeks to protect–high-risk borrowers–stand to lose the most.”[12]

Thus, in this case study, we will focus on changes in disparities as a result of the adoption of a new pricing method—for example, whether the move from traditional credit pricing to algorithmic credit pricing decreased or increased disparities or whether the use of social media data increases disparities, rather than an absolute level of disparity.[13] For example, In a recent update, the CFPB described how an algorithmic lender, Upstart, had demonstrated that it provides cheaper loans than under traditional lending models and accepted applicants who would have been rejected under those models.[14]

The Role of the Consumer Financial Protection Bureau (CFPB)

The Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (“Dodd-Frank Act”) transferred the authority to implement the ECOA to the CFPB. The CFPB prohibits discriminatory practice under the ECOA. In 2012, the CFPB announced that “[c]onsistent with other federal supervisory and law enforcement agencies, the CFPB reaffirms that the legal doctrine of disparate impact remains applicable…to enforce compliance with the ECOA…”[15] On May 21, 2018, the CFPB issued a statement

[10] Adams, W., L. Einav, and J. Levin (2009): “Liquidity Constraints and Imperfect Information in Subprime Lending.” American Economic Review, 99(1): 49–84; Einav, L., M. Jenkins, and J. Levin (2012): “Contract Pricing in Consumer Credit Markets.” Econometrica, 80(4): 1387–1432; Einav, L., M. Jenkins, and J. Levin (2013): “The Impact of Credit Scoring on Consumer Lending.” RAND Journal of Economics, 44(2): 249–274.

[11] Board of Governors of the Federal Reserve System (2007): Report to Congress on Credit Scoring and Its Effects on the Availability and Affordability of Credit. Submitted to the Congress pursuant to section 215 of the Fair and Accurate Credit Transactions Act of 2003; August 2007.

[12] Center for Capital Markets. Risk-based Pricing in Consumer Lending. https://www.centerforcapitalmarkets.com/wp-content/uploads/2013/08/CCMC_RiskBasedPricing_FINAL_to_post_10_24_2014.pdf

[13] Talia B. Gillis, Discrimination Stress-Testing. Draft

[14] Patrice Ficklin and Paul Watkins, An update on credit access and the Bureau’s first No-Action Letter. https://www.consumerfinance.gov/about-us/blog/update-credit-access-and-no-action-letter/

[15] *CFPB Bulletin 2012-04 (Fair Lending)*, CFPB, (Apr. 18, 2012), http://files.consumerfinance.gov/f/201404_cfpb_bulletin_lending_discrimination.pdf.

indicating its intent to reexamine requirements of the ECOA in light of recent Supreme Court case law addressing the availability of disparate-impact legal theory under the Fair Housing Act ("FHA").[16]

Congress in section 1021(a) of the Dodd-Frank Act established the CFPB's statutory purpose as ensuring that all consumers have access to markets for consumer financial products and services and that markets for consumer financial products and services are fair, transparent, and competitive.[17] The CFPB has jurisdiction over banks, credit unions, securities firms, mortgage servicing operations, and other financial companies operating in the United States. The Bureau is responsible for monitoring markets for consumer financial products and services to identify risks to consumers and the proper functioning of such markets.

In particular, the Bureau has focused on fair lending, by providing oversight and enforcement of federal laws intended to ensure "fair, equitable, and nondiscriminatory access to credit for both individuals and communities."[18] The CFPB has issued regulations under the ECOA, known as Regulation B[19] and regulations under the HMDA, known as Regulation C.[20] These regulations provide the substantive and procedural framework for fair lending.

Interagency Cooperation

As required by the Dodd-Frank Act, the Bureau's Office of Fair Lending coordinated fair lending regulatory, supervisory, and enforcement activities with other Federal agencies and State regulators to promote consistent, efficient, and effective enforcement of federal lending laws, including but not limited to the ECOA.[21] The CFPB is authorized to bring public enforcement actions against any person, subject to the CFPB's supervisory or enforcement authority, for violations of the ECOA. The Dodd-Frank Act expressly authorizes the CFPB to conduct joint investigations with the U.S. Department of Justice ("DOJ") in matters relating to fair lending. The CFPB is also required to refer certain violations of the ECOA to the DOJ for possible enforcement actions.[22]

Unlike the ECOA, the CFPB does not have supervisory authority over the FHA under the Dodd-Frank Act.[23] The CFPB cooperates with the U.S. Department of Housing and Urban Development ("HUD") to further the purposes of the FHA.

Under the Dodd-Frank Act, Congress also transferred HMDA rulemaking authority and other functions to CFPB. Regulation C, 12 C.F.R. part 1003, implements the Home Mortgage Disclosure Act. HMDA agencies include both the CFPB and HUD, as well as other federal agencies, such as the Office of

[16] CFPB, *Statement of the Bureau of Consumer Financial Protection on enactment of S.J. Res. 57*, CONS. FIN. PROT. BUR. (May 21, 2018), https://www.consumerfinance.gov/about-us/newsroom/statement-bureau-consumer-financial-protection-enactment-sj-res-57/; *see* CFPB, *Fall 2018 Regulatory Agenda Preamble*, CONS. FIN. PROT. BUR. (Aug. 30, 2018), https://www.reginfo.gov/public/jsp/eAgenda/StaticContent/201810/Preamble_3170.html.

[17] 12 U.S.C. 5511(a).

[18] 12 U.S.C. § 5493(c)(2)(A).

[19] CFPB Equal Credit Opportunity Act (Regulation B) (2019), 12 CFR Part 1002.

[20] CFPB Home Mortgage Disclosure (Regulation C) (2020), 12 CFR Part 1003.

[21] Dodd-Frank Act § 1013(c)(2)(B) (codified at 12 U.S.C. § 5493(c)(2)(B)).

[22] CFPB, Consumer Financial Protection Bureau and Justice Department pledge to work together to protect consumers from credit discrimination, CONS. FIN. PROT. BUR. (Dec. 6, 2012). https://www.consumerfinance.gov/about-us/newsroom/consumer-financial-protection-bureau-and-justice-department-pledge-to-work-together-to-protect-consumers-from-credit-discrimination/.

[23] H.R. 4173 § 1027(s) ("No provision of this title shall be construed as affecting any authority arising under the Fair Housing Act.").

the Comptroller of the Currency ("OCC"), the Federal Deposit Insurance Corporation ("FDIC"), the Federal Reserve System, the National Credit Union Administration ("NCUA").[24]

Regulation B

The ECOA is implemented by Regulation B. It contains two basic and comprehensive prohibitions against discriminatory lending practices:[25] "(1) A creditor shall not discriminate against an applicant on a prohibited basis regarding any aspect of a credit transaction; (2) A creditor shall not make any oral or written statement, in advertising or otherwise, to applicants or prospective applicants that would discourage, on a prohibited basis, a reasonable person from making or pursuing an application." Note that the regulation is concerned not only with the treatment of persons who have initiated the application process, but also with lender behavior before the application is even taken. For example, a creditor may not advertise its credit services and practices in ways that would tend to encourage some types of borrowers and discourage others on a prohibited basis. In addition, a creditor may not use prescreening tactics likely to discourage potential applicants on a prohibited basis.

Discrimination Doctrines in Lending

There are two principles of discrimination doctrines: disparate treatment and disparate impact.[26] Disparate treatment occurs when a creditor treats an applicant differently based on a prohibited basis such as race or national origin.[27] Disparate impact occurs when a creditor employs facially neutral policies or practices that have an adverse effect or impact on a member of a protected class, unless those policies or practices meet a legitimate business need that cannot reasonably be achieved by means that are less disparate in their impact.[28]

There are ongoing disputes with respect to the foundations and scope of the different doctrines. First, is disparate treatment intended to focus on lenders with animus toward protected groups? Does disparate treatment also include mere direct consideration of a protected characteristic, even when it has a rational explanation or basis? Second, is disparate impact doctrine meant to "address only covert intentional discrimination, or more broadly address the furthering of preexisting disadvantage into the credit context"?[29]

While the ECOA and the FHA do not explicitly recognize the two discrimination doctrines in the language of the law itself, the disparate impact doctrine has been recognized with respect to credit pricing by courts and agencies in charge of enforcing the laws. In *Texas Department of Housing and Community Affairs v. Inclusive Communities Project*, the Supreme Court recognized disparate impact under the FHA in 2015.[30]

[24] CFPB, *supra* note 11, at § 1003.1.

[25] 12 C.F.R. § 1002.4.

[26] Federal Fair Lending Regulations and Statutes. https://www.federalreserve.gov/boarddocs/supmanual/cch/fair_lend_over.pdf.

[27] 12 C.F.R. § 1002.4(a)-(b). *See also* official interpretation of paragraph 4(a) and 4(b) at https://www.consumerfinance.gov/policy-compliance/rulemaking/regulations/1002/4/.

[28] 12 C.F.R. Part 1002 Supp. I Sec. 1002.6(a)-2.

[29] Talia Gillis. *Discrimination Stress-Testing* (March 2020). Draft.

[30] Texas Dep't of Hous. & Cmty. Affairs v. Inclusive Communities Project, Inc., 135 S. Ct. 2507 (2015).

In *Inclusive Communities*, Justice Kennedy held that "antidiscrimination laws should be construed to encompass disparate-impact claims when their text refers to *the consequences of actions* and not just to the mindset of actors, and where that interpretation is consistent with statutory purpose."

In its analysis, the court reasoned that the phrase "or otherwise make unavailable" in Section 804(a) of the FHA is equivalent in function and purpose to "or otherwise adversely affect" in Title VII and ADEA. Justice Kennedy writes, "Congress's use of the phrase 'otherwise make unavailable' refers to the consequences of an action rather than the actor's intent." The decision states that in all "three statutes the operative text looks to results," and "this results-oriented language counsels in favor of recognizing disparate impact liability."

In addition, the majority opinion also points to four actions that confirm Congress's understanding that disparate impact liability exists under the FHA: (1) Congress passed the FHA only four years after passing Title VII and only four months after passing ADEA, all three with similar text and structure; (2) Congress passed the FHA amendments of 1988 knowing that all nine Courts of Appeals that had addressed the question concluded the FHA encompassed disparate impact claims; (3) The 1988 amendments included three exemptions to disparate impact that assume the existence of disparate impact claims under the FHA as enacted in 1968; and (4) also in 1988, Congress rejected a proposed amendment that would have eliminated disparate impact liability for certain zoning decisions. Thus, the court concluded that "This results-oriented language counsels in favor of recognizing disparate-impact liability" under FHA.

However, there are some ambiguities about disparate treatment and disparate impact under ECOA, because it includes no such "results-oriented language."

The U.S. Supreme Court also ruled that institutional policies are not contrary to the discrimination laws unless they are "artificial, arbitrary, and unnecessary barriers." The Court cautioned there must be adequate safeguards around application of disparate impact analysis to avoid setting "our Nation back in its quest to reduce the salience of race in our social and economic system," and that the "[c]ourt should avoid interpreting disparate-impact liability to be so expansive as to inject racial considerations into every housing decision" or "to second-guess" between "two reasonable approaches." In addition, the language of the FHA should not be construed to force defendants to "resort to the use of racial quotas." Disparate-impact liability must be limited so employers and other regulated entities are able to make the "practical business choices and profit related decisions that sustain a vibrant and dynamic free-enterprise system."

Although there is not an equivalent Supreme Court case with respect to ECOA, the CFPB and courts have found that the relevant statutes allow for a claim of disparate impact.[31]

Existing Discriminatory Framework

Under the existing framework, a defendant may be liable for practice with a discriminatory effect unless there is a legally sufficient justification.[32]

[31] *See, e.g.,* Ramirez v. GreenPoint Mortgage Funding, Inc, 633 F. Supp. 2d 922, 926–27 (N.D. Cal. 2008)

[32] 24 C.F.R. Part 100, Implementation of the Fair Housing Act's Discriminatory Effects Standard; Final Rule.

Discriminatory Effect

First, the government and private plaintiffs "bears the burden of proving its prima facie case that a practice" actually, or predictably: "(1) results in a disparate impact on a group of persons on the basis of race, color, religion, sex, handicap, familial status, or national origin; or (2) has the effect of creating, perpetuating, or increasing segregated housing patterns on the basis of race, color, religion, sex, handicap, familial status, or national origin."[33] Thus, plaintiffs need not allege any *intent* to discriminate against borrowers.

Legally Sufficient Justification

When the plaintiffs prove a prima facie case, the burden of proof shifts to the respondent or defendant to prove that there is a legally sufficient justification for the alleged practice. A legally sufficient justification exists where the challenged practice "(i) is necessary to achieve one or more of its substantial, legitimate, nondiscriminatory interests" of the respondent or the defendant; and "(ii) those interests could not be served by another practice that has a less discriminatory effect." A legally sufficient justification "must be supported by evidence and may not be hypothetical or speculative."[34]

Less Discriminatory Alternatives

If the defendant satisfies this burden, then the plaintiff may still establish liability by proving that the substantial, legitimate, nondiscriminatory interests could be served by a practice that has a less discriminatory effect.

Machine Learning in Lending

Basics of Machine Learning

Fueled by exponentially increasing data and compute power, machine learning is having an unprecedented impact on our everyday lives. Credit risk assessment represents one of the earliest uses of machine learning. For example, in 1992, the Bank of Scotland led an early effort to collaborate with academic researchers to apply machine learning algorithms in scoring credit-card applications and compare their performance.[35]

Machine learning is a method of using a computer to parse data, learn from it, and then make a prediction/determination based on the analysis. For example, the learning process for Random Forest,[36] a popular supervised machine learning technique, includes: (1) data gathering and cleansing; (2) splitting

[33] Inclusive Communities, supra note 20, at 2523.

[34] *Id.*

[35] R. H. Davis, D.B. Edelman and A.J. Gammerman, *Machine-learning algorithms for credit-card applications*, 4 IMA JOURNAL OF MATHEMATICS 43-51 (1992).

[36] Tony Yiu, *Understanding Random Forest: How the Algorithm Works and Why it Is So Effective*, TOWARDS DATA SCIENCE, (Jun.12, 2019), https://towardsdatascience.com/understanding-random-forest-58381e0602d2.

the data into a training dataset and a testing dataset; (3) training the model with the training dataset based on various machine learning algorithms; and (4) validating the model with the testing dataset.

Random Forest,[37]Artificial Neural Networks,[38] and Boosting[39] are three of the most popular machine learning techniques that have been adopted to credit risk assessment. Machine learning algorithms can analyze large volumes of data, and quickly and accurately identify patterns and trends that might not be apparent to a human. In addition, its performance can improve over time because of the increasing amounts of data that are processed. As more data comes in, the algorithm becomes more experienced and can then make better predictions.

Potential Benefits of Machine Learning in Lending

In 2018, Fannie Mae, one of the federally sponsored agencies that purchases and guarantees mortgages, conducted a survey of mortgage lenders and their use of machine learning ("ML") in lending.[40] The survey found that over the next two years, the use of these technologies in the mortgage industry was going to boom. Some of the key drivers of such business change include rising customer expectations, cost-saving, and operational challenges.[41]

In particular, machine learning and AI solutions are helping banks and credit lenders use alternative data to evaluate creditworthiness to increase access to credit or decrease the cost of the credit. Mortgage lenders, generally, have a large amount of data regarding the applicant at the time of underwriting. The appeal for machine learning is that it manages, from the data, to uncover complex patterns and relevant variables that were not apparent in advance. This increased insight allows lenders to view borrowers as more than a handful of numbers, as occurs with traditional lending models. Such information can be used to more accurately assess credit risk than traditional rules-based underwriting. By considering alternative data, such as payment of bills or rents, loans will be available to a wider variety of people who, although they are good candidates to repay a mortgage, would be rejected today using traditional lending models because, for example, for whatever reason they lack a traditional credit history.

Results provided from CFPB's No-Action Letter Program show that machine learning with alternative data approves 23-29% more applicants and, compared with traditional models, lowers the average annual percentage rate by 15-17% for approved loans.[42] Such expansion of credit access occurs across all tested race, ethnicity, and sex segments. In particular, consumers with incomes under $50 thousand are 13% more likely to be approved.

[37] Deloitte, *Point of View: Using Random Forest for credit risk models*, Deloitte Risk Advisory, (Sept. 2018), https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/financial-services/deloitte-nl-fsi-using-random-forest-for-credit-risk-models.pdf.

[38] Manish Bhoge, *Using the Artificial Neural Network for Credit Risk Management*, ORACLE DATA SCIENCE BLOG, (Jan. 23, 2019), https://blogs.oracle.com/datascience/using-the-artificial-neural-network-for-credit-risk-management.

[39] Jocelyn D'Souza, *A quick guide to Boosting in ML*, MEDIUM (Mar. 21, 2018), https://medium.com/greyatom/a-quick-guide-to-boosting-in-ml-acf7c1585cb5.

[40] Fannie Mae, *Mortgage Lender Sentiment Survey: How will Artificial Intelligence Shape Mortgage Lending? Q3 2018 Topic Analysis*, FANNIE MAE (Oct. 4, 2018), https://www.fanniemae.com/resources/file/research/mlss/pdf/mlss-artificial-intelligence-100418.pdf.

[41] Aseem Mital and Atul Varshneya (Tavant Technologies), *Reshaping Consumer Lending with Artificial Intelligence*, MORT. BANKERS ASSOC., https://www.tavant.com/sites/default/files/download-center/Tavant_Consumer_Lending_Artificial_Intelligence_Whitepaper.pdf

[42] Patrice Fickin and Paul Watkins, *An update on credit access and the Bureau's first No-Action Letter*, CONS. FIN. PROT. BUR. (Aug. 6, 2019), https://www.consumerfinance.gov/about-us/blog/update-credit-access-and-no-action-letter/.

Potential Challenges of Machine Learning in Lending

Despite the efficiency and accuracy gained via machine learning, it also presents certain significant potential risks.[43]

Yongqianbao (meaning, "Use Money, my pal") is an AI-based financial service app that provides small amount, short-term loans to the underbanked population in China. A Public Broadcasting Service documentary film shows that it only takes eight seconds for the Yongqianbao App to approve a loan by analyzing 5,000 features of the applicant while traditional banks only assess 10 features.[44] The 5,000 features include not only traditional credit information, but also unconventional features, such as smart phone behaviors, including what phone the borrower is using, how many calls go unanswered, and the battery level of the phone. It also uncovers some unexpected correlation: *e.g.*, how confident a borrower types in the loan application and whether the borrower keeps the cell phone charged are highly correlated to delinquency.

While such use of alternative information may help expand credit access to under-represented groups, it raises privacy concerns because of the use of invasive personal information without the borrower's awareness. Notably, Yongqianbao has also been accused multiple times for predatory lending where the annual interest rate was as high as 109.5% and for abusing its AI technology to harass borrowers' social media and phone contacts for debt collection.[45]

Even when companies do not intend to discriminate and deliberately avoid using suspect classifications like race and gender, the output of an analytical process can have a disparate impact on a protected class. An algorithm could be trained with historically biased data and simply reflect preexisting discrimination or disparities. Analytics relying on existing data could reinforce and worsen past discriminatory practices. Fair lending law has traditionally addressed this concern by limiting the consideration of protected characteristics, such as race, gender, etc. However, other correlated input information, for example, zip code, may serve as a proxy for protected characteristics, and it is difficult to exclude all such correlated information.

It is also less feasible to apply the legal doctrine of disparate treatment to the practice of algorithmic credit pricing. The ubiquity of correlations in big data, combined with the flexibility and complexity of machine learning models, means that one cannot rule out the consideration of a protected characteristic, even when formally excluded.[46]

One recent study, "False Dreams of Algorithmic Fairness: the Case of Credit Pricing,"[47] has conducted simulations highlighting concerns over approaches focusing on input scrutiny. More

[43] *See, e.g.*, Mikella Hurley and Julius Adebayo, *Credit Scoring in the Era of Big Data*, 18 YALE L. J. & TECH. 148, 168 (2016); Matthew Adam Bruckner, *The Promise and Perils of Algorithmic Lenders' Use of Big Data*, 93 CHI. -KENT L. REV. 3, 25-29 (2018).

[44] *In the Age of AI, Frontline*, PUBLIC BROADCASTING SYSTEM (Nov. 5, 2019), https://www.pbs.org/wgbh/frontline/film/in-the-age-of-ai/.

[45] *Repeatedly Banned? Exploited with Quinbao illegal collection of annualized interest rate of nearly 110%*, TOUTIAO, http://toutiao.manqian.cn/wz_9PnoVRZltf.html.

[46] *Evaluating the Fair Lending Risk of Credit Scoring Models*, CHARLES RIVER ASSOC. Feb. 2014), http://www.crai.com/sites/default/files/publications/FE-Insights-Fair-lending-risk-credit-scoring-models-0214.pdf. The concern that big data analysis might discriminate inadvertently is explicitly recognized: "Ostensibly neutral variables that predict credit risk may nevertheless present disparate impact risk on a prohibited basis if they are so highly correlated with a legally protected demographic characteristic that they effectively act as a substitute for that characteristic."

[47] Talia Gillis, *False Dreams of Algorithmic Fairness: the Case of Credit Pricing*, talk at Harvard Empirical Legal Studies, Harvard Law School (Sept. 20, 2019), available at https://scholar.harvard.edu/files/gillis/files/gillis_jmp_191101.pdf.

specifically, the author argues that because information about a person's protected characteristic is embedded in other information about the individual, it is unlikely that the formal exclusion of the protected characteristic as an input guarantees that the characteristic was not used in forming a decision. Machine learning algorithms are particularly adept at uncovering some previously unknown relationship between alternative information and the protected characteristics because of the ubiquity of correlations in big data. On the other hand, machine learning algorithms can be unstable and may find spurious correlations even when there are none.[48] It is not enough to expand the prohibited inputs to also include "proxies" for protected characteristics. It is also not clear whether a showing of correlation should be admitted as evidence to demonstrate disparate treatment.

A disparate impact assessment seeks to assess the extent of any disproportionate, adverse impact on a protected class, identifies the extent to which the use of the algorithm contributes to a legitimate organizational or social need, and explores whether there are equally effective models with lesser disparate impact.

CFPB's Initiative with Machine Learning in Lending

Regulatory uncertainty can substantially hinder the development of innovative products and services that may ultimately benefit consumers. The CFPB has been working towards improving its policies to promote innovation and facilitate compliance.

In 2017, the Bureau issued a Request for Information Regarding Use of Alternative Data and Modeling Techniques in the Credit Process (RFI).[49] The RFI sought public comments regarding the potential positive and negative consequences associated with the use of alternative data to "encourage responsible use of alternative data and lower unnecessary barrier impeding its use."

In September 2017, the CFPB issued a Non-Action Letter[50] to Upstart Network Inc., an artificial intelligence lending platform.[51] In addition to using traditional factors such as credit score and income, Upstart also evaluates consumer loan applications incorporating non-traditional sources of information, such as education and employment history. Learning from its experience with Upstart, in 2019, the CFPB updated its NAL policy as it found its prior policy "not an adequate response to the extent of innovation

[48] Robin Wigglesworth, *Spurious correlations are kryptonite of Wall St's AI rush*, FIN. TIMES (Mar. 14, 2018), https://www.ft.com/content/f14db820-26cd-11e8-b27e-cc62a39d57a0.

[49] CFPB, Request for Information Regarding Use of Alternative Data and Modeling Techniques in the Credit Process, 82 Fed. Reg. 11183 (Feb. 21, 2017), https://www.govinfo.gov/content/pkg/FR-2017-02-21/pdf/2017-03361.pdf.

[50] The authorities given to the CFPB under title X of Dodd-Frank form the basis for the CFPB's NAL policy. 81 FR 8686 (Feb. 22, 2016) [the original NAL policy]. The SEC also has a mechanism for No Action letters, which may be considered as a more case-by-case adjudication on the part of the regulation. Although Dodd-Frank does not explicitly provide the authority for NAL, they are considered under the CFPB's supervisory and enforcement discretion. For further background on the differences between adjudication versus advance rule making, see David L. Shapiro, *The Choice of Rulemaking or Adjudication in the Development of Administrative Policy*, 78 Harv. L. Rev. 921 (1964–1965). For a more recent discussion, see Yehonatan Givati, *An Incomplete Contracting Approach to Administrative Law*, 18 Am Law Econ Rev 176 (2016).

[51] CFPB Announces First No-Action Letter to Upstart Network, CFPB (Sept. 14, 2017), https://www.consumerfinance.gov/about-us/newsroom/cfpb-announces-first-no-action-letter-upstart-network/. Upstart is an artificial intelligence lending platform. In addition to using traditional factors such as credit score and income, Upstart also evaluates consumer loan applications incorporating non-traditional sources of information such as education and employment history.

occurring in markets for consumer financial products and services."[52] The CFPB also issued new Trial Disclosure Program (TDP) Policies,[53] and the new Compliance Assistance Sandbox (CAS) Policy.[54]

The new policy provides a more streamlined review process for products and services.[55] It also no longer requires applicants to show that they are likely to provide "substantial" benefit to consumers but rather a "potential" benefit.[56] Since its adoption of the new policy, the CFPB has provided NALs with respect to housing counseling agreements by Housing Counseling Agencies (HCA), which are regulated by the HUD.[57]

Under the CFPB's new TDP Policy, entities seeking to improve consumer disclosures may conduct in-market testing of alternative disclosures for a limited time upon receiving permission from the CFPB.

Under the CAS Policy, after the CFPB evaluates the product or service for compliance with relevant law, an approved applicant that complies in good faith with the terms of the approval will have a "safe harbor" from liability for specified conduct during the testing period. Approvals under the CAS Policy will provide protection from liability under ECOA and other fair lending laws.[58] The regulatory sandbox policy can be helpful for fostering incentive to innovate when the legal uncertainty as to how algorithms can comply with fair lending laws.

However, there are various legal challenges in creating sandboxes.[59] The authority to regulate financial institutions and activities is fragmentation and overlapping in the United States and there is a complex relationship between federal and state regulation.[60] The possibility that financial activity trigger enforcement from regulators other than the CFPB could potentially undermine the benefit of the sandbox, as it does not provide innovators with added certainty.

For example, the Office of the Comptroller of the Currency (OCC) has opened its own "sandbox" through a Proposed Innovation Pilot Program designed to promote its innovation initiatives, add value through proactive supervision, and continue its objective to lead fintech innovation expansion.[61] Unlike the CFPB Sandbox, entities accepted under the OCC Program will receive no immunity from complying with applicable laws and regulations.

[52] Bureau of Consumer Financial Protection, Policy on No-Action Letters, Vo. 84 No. 178, page 48229 (September 13, 2019) [hereinafter New NAL Policy]. The Final Rule can be found at: https://files.consumerfinance.gov/f/documents/cfpb_final-policy-on-no-action-letters.pdf and https://www.govinfo.gov/content/pkg/FR-2019-09-13/pdf/2019-19763.pdf.

[53] Policy to Encourage Trial Disclosure Programs, CFPB, https://files.consumerfinance.gov/f/documents/cfpb_final-policy-to-encourage-tdp.pdf.

[54] Policy on the Compliance Assistance Sandbox, CFPB, https://files.consumerfinance.gov/f/documents/cfpb_final-policy-on-cas.pdf.

[55] For example, the new policy states the intention of the CFPB to grant or deny an application within 60 days and includes a policy for obtaining NAL modifications.

[56] *See* New NAL Policy.

[57] The first NAL was issued in September 2019 and covered HUD supervised HCAs that enter agreements with consumers, as long as they comply with certain requirements such as providing consumers with a memorandum of understanding with the consumer reflecting the terms of the housing counselling. It provided a similar NAL to Bank of America in January 2020. *See:* https://www.consumerfinance.gov/about-us/newsroom/cfpb-issues-no-action-letter-to-facilitate-housing-counseling-services/.

[58] U.S. DEP'T OF TREASURY, A FINANCIAL SYSTEM THAT CREATES ECONOMIC OPPORTUNITIES (2018), https://home.treasury.gov/sites/default/files/2018-07/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financi....pdf. The Treasury recommended creating a regulatory sandbox to promote innovation.

[59] Talia Gillis, Discrimination Stress Testing. Draft.

[60] For example, one issue that can arise is the preemption of state laws, such as in the case of licensing or usury. The CFPB's approach in addressing these concerns that arise as a result of activity triggering several other regulatory bodies, is that the CFPB will coordinate with other regulators to resolve potential issues. Another initiative of the CFPB has been the creation

[61] OCC Solicits Public Comment on Proposed Innovation Pilot Program. https://www.occ.treas.gov/news-issuances/news-releases/2019/nr-occ-2019-42.html

Moreover, following the proposal for the CFPB sandbox, twenty-two state attorney generals wrote a letter to the CFPB stating that the bureau could not provide a safe harbor protecting them from enforcement action.[62] The AGs also questioned whether it would be sufficient to adopt a sandbox as a policy rather than adopting the proposal through the formal rulemaking process. The CFPB, on the other hand, considers its authority to create a sandbox policy under its supervisory and enforcement discretion provided by Dodd-Frank.

However, the CFPB has adopted several approaches to mitigate this risk by committing to engage in outreach to other federal and state regulators and to coordinate when challenges arise.[63] Moreover, the creation of the American Consumer Financial Innovation Network (ACFIN), a network of federal and state regulators to facilitate innovation, is also expected to assist in coordination.[64]

Framework Choices for CFPB

Option 1: 2019 HUD's Five-Element Burden-Shifting Framework

In August 2019, HUD proposed a new burden-shifting framework to establish discriminatory liability under the FHA.[65] This new framework replaced the previous three-step burden-shifting framework with a five-element approach. This rule is also one of the first attempts in the U.S. to determine whether an algorithm violates the FHA.

More specifically, a plaintiff's allegations that a specific, identifiable, policy or practice has a discriminatory effect must plead facts supporting five elements to establish a prima facie case: a plaintiff is required to allege that (1) "the challenged policy or practice is *arbitrary, artificial, and unnecessary* to achieve a valid interest or legitimate objective such as a practical business, profit, policy consideration, or requirement of law"; (2) there is "*a robust causal link* between the challenged policy or practice and a disparate impact on members of a protected class"; (3) the challenged policy or practice has "an adverse effect on *members of a protected class*"; (4) "the disparity caused by the policy or practice is *significant*"; and (5) "the *complaining party's alleged injury* is directly caused by the challenged policy or practice"[66] [Emphasis ours].

The defendant may rebut a claim at the pleading stage by asserting that a plaintiff has not alleged facts to support their prima facie claim. In a case when a challenged policy relies on an algorithmic model, three defenses are available to the defendant to defeat the claim.

[62] *See* Kate Berry, State AGs assail CFPB plan to build fintech sandbox, Am. Banker (Feb. 12, 2019, 4:14pm EST), available at https://www.americanbanker.com/news/state-ags-assail-cfpb-plan-to-build-fintech-sandbox.

[63] https://www.jdsupra.com/legalnews/paul-watkins-director-of-the-cfpb-s-86267/

[64] *See* announcement by CFPB, at https://www.consumerfinance.gov/about-us/newsroom/bureau-state-regulators-launch-american-consumer-financial-innovation-network/. Allen suggests a different approach in which a committee of regulators approve sandbox applications. *See* Allen, *supra* note 138, at 622. While this approach would allow for better coordination it is likely to be highly unfeasible.

[65] HUD's Implementation of the Fair Housing Act's Disparate Impact Standard. A Proposed Rule by the Housing and Urban Development Department (Aug. 19, 2019), https://www.federalregister.gov/documents/2019/08/19/2019-17542/huds-implementation-of-the-fair-housing-acts-disparate-impact-standard.

[66] *City of Miami v. Bank of America Corp.*, 137 S. Ct. 1296, 1305-06 (2017). Decided two years after *Inclusive Communities*, *supra* note 20, the U.S. Supreme Court held that Fair Housing Act plaintiffs must satisfy a "requirement" of pleading "direct" proximate causation. Under this requirement, a lender cannot be held liable under the FHA for a disparate impact where the independent actions of independent third parties break the proximate causal chain.

The first defense allows a defendant to provide an analysis showing that "the model is not the actual cause of the disparate impact alleged by the plaintiff." The defendant may "break down the model piece-by-piece and demonstrate how each factor considered could not be the cause of the disparate impact and show how each factor advances a valid objective." The plaintiff may defeat this defense by showing that "the defendant's analysis is somehow flawed, such as by showing that a factor used in the model is correlated with a protected class despite the defendant's assertion."

There are cases where defendants may not have access to the model developed by a third party. For example, government-sponsored enterprises Fannie Mae and Freddie Mac require lenders to evaluate credit risk pursuant to automated underwriting systems containing models proprietary to those enterprises. Yet, lenders have no ability to alter the models used by Fannie Mae and Freddie Mac, and lenders are not in a position to justify each element of such a model, much less the relationships among all the variables.

In this case, a second defense provides that a defendant can show that "use of the model is standard in the industry." A recognized third party, not the defendant, is responsible for creating or maintaining the model. It is being used for the intended purpose of the third party. A plaintiff may rebut this allegation by showing that the plaintiff is not challenging the standard model alone, but that the defendant's unique use or misuse of the model is the cause of the disparate impact.

A third defense allows a defendant to "prove through the use of a qualified expert that the model is not the cause of a disparate impact." A plaintiff may rebut this defense by showing that "the expert is not neutral, that the analysis is incomplete, or that there is some other reason why the expert's analysis is insufficient evidence that the defendant's use of the model is justified."

Once a plaintiff adequately alleges facts to support the prima facie claim, the defendant then has the burden to identify a valid interest/interests that the challenged policy or practice serves.

Finally, having articulated a legitimate business goal, the defendant should prevail unless the plaintiff can prove that "other tests or selection devices, without a similarly undesirable racial effect, would also serve the legitimate business interests in an equally effective manner."

Even if a policy or practice that has a disparate impact on a prohibited basis can be justified by business necessity, it still may be in violation if an alternative policy or practice could serve the same purpose with less discriminatory effect. For example, refusing to lend to all people in a heavily minority neighborhood has a disproportionate adverse impact on a protected class, but it might have a legitimate purpose, namely, to avoid making loans that could not be repaid. On average, people in red-lined neighborhoods are more likely to have bad credit risks. Thus, avoiding those neighborhoods controls credit risk, a business necessity, but may still be in violation because there are other ways of achieving the same purpose of controlling credit risk without disparate impact.

Option 2: Pre-clearing Framework: Discrimination Stress-Testing

Option 1 focus on auditing the algorithms in an *ex post* manner to ensure that it is operating properly.

However, there have been proposals that the *ex post* analysis should be supplemented by testing algorithms at the development stage for potential bias.[67] An outcome-based framework is proposed by "False Dreams of Algorithmic Fairness: the Case of Credit Pricing" and described in more details in "Discrimination Stress Testing." The framework shifts away from input scrutiny. Instead, a regulator will apply a pricing rule to a designated dataset to analyze the properties of the pricing rules. This option gives regulators more flexibility.

There are two questions the regulator should address using this framework—first, whether borrowers who are "similarly situated" are treated the same; and second, whether the pricing rule increases or decreases disparities relative to some baseline. The framework requires regulators to build a neutral database with real or hypothetical people and their characteristics, then apply a lender's pricing rule to a dataset of hypothetical borrowers, and then examine the properties of the outcome. The goal is for the regulator to examine the algorithm in an *ex ante* manner.

The testing involves three stages. At the first stage, the lender determines the input and algorithms for the pricing rule to use for credit risk assessment. This stage does not involve a regulator. At the second stage, the regulator takes the algorithm and applies it to the neutral database. The rationale for using a database is that it is difficult to analyze a prediction function in the abstract.[68] At the third stage, the regulator evaluates the outcome to determine whether the disparities created by the pricing rule amount to discriminatory conduct. The outcome metric can be credit price, or other metrics, *e.g.*, error rates.[69] The exact criteria to be used in outcome analysis will depend on what the discrimination laws aim to achieve which, unfortunately, has not been clear and agreed upon.[70]

The discrimination stress-testing can be helpful in quantifying and understanding incremental changes in access to credit as a result of AI algorithms, i.e., whether the move from traditional credit pricing to algorithmic credit pricing decreased or increased disparities.

However, it is unclear whether the lenders or the regulators should run the outcome-based analysis. There may be proprietary concern for the lenders to give their algorithms to regulators to test. It is also possible for third parties to game the algorithm by analyzing the output. On the other hand, regulators may not have the resources or manpower to run such analyses, and, if they do, it would also discourage the lender's autonomy. For lenders serving small communities, requirement of model validation may discourage them from adopting innovative products or services.

An alternative approach is to create a voluntary regime. Firms are not required to receive permission from the regulator to implement algorithmic credit pricing but can apply for regulatory approval or temporary protection from regulatory enforcement.

Challenges also exist in defining the safe harbor provided to firms when participating in the sandbox, as doing so requires the delicate balancing of competing concerns.[71] On the one hand, for a sandbox to be effective, the safe harbor provided must be significant, otherwise there is only a weak

[67] Terrell McSweeny, Comm'r, Fed. Trade Comm., Keynote Remarks at Google Tech Talk: *Tech for Good: Data for Social Empowerment*, (Sept. 10, 2015), https://www.ftc.gov/system/files/documents/public_statements/800981/150909googletechroundtable.pdf; Gillis, *supra* note 38.

[68] Talia B. Gillis and Jann L. Spiess, *Big Data and Discrimination*, 86 U. CHI. L. REV. 459 (2019).

[69] Sam Corbett-Davies and Sharad Goel, *The Measure and Mismeasure of Fairness: A Critical Review of Fair Machine Learning*, available at CORNELL UNIV. arXiv:1808.00023 [cs:CS]v2 6 (Aug. 14, 2018), https://arxiv.org/pdf/1808.00023.pdf.

[70] Gillis, *supra* note 38.

[71] Talia Gillis. Discrimination Stress Testing. Draft.

incentive to participate in the sandbox. On the other hand, safe harbors could limit the regulator's ability to act when a product or service indeed proves to be harmful or have unintended consequences.[72] Beyond the requirements for and restrictions in entering sandbox programs, such as demonstrating the potential benefit of the innovation to consumers, safe harbors can be adjusted to balance the competing policy goals. For example, limiting the time for which the safe harbor is provided means that firms do not have an ongoing exemption from complying with regulation.[73] In the United Kingdom, the continuing communication with the designated officer means that the FCA has greater visibility of the potential harm of a product and engages in softer forms of regulation even when other regulatory action is not possible.

One of the most significant potential benefits of a sandbox approach is that it may lead to more formal rulemaking with respect to algorithmic pricing lending. There is currently scant guidance on how to analyze an algorithm for the purpose of fair lending, and while algorithmic pricing is an outlier in how credit is currently priced, this is likely to change in the long term. Therefore, while in the short-term regulators may need to provide a safe policy space in which to innovate, in the long-term, regulators will need to create formal rule making.[74] Regulatory sandboxes may allow for regulators to develop the understanding and expertise needed for new regulations.[75]

Legal and Policy Considerations

Whether to choose either of the two frameworks depends on the objective and motivations of CFPB. Designing would need to take into consideration a variety of issues, as set forth below.

Ex Ante Approach or *Ex Post* Approach

Timing is an important consideration in regulatory design. One issue to consider in designing the framework is whether we should adopt an *ex ante* approach, which focuses on preventing financial harm, or an *ex post* approach, which focuses on mitigating the harm.

In an ideal world, with perfect government information, perfectly rational actors, and complete liquidity, *ex post* is equivalent to *ex ante*.[76] However, the reality is that the regulators will not have perfect information, and the actors are not always rational. The choice of an *ex ante*, as compared to an *ex post* approach, is essentially a problem of balancing factors such as the policing capacity of *ex ante* penalties, the cost of consequences to the lender resulting from its conduct compared to the cost to the lender of preventing the conduct, and the ability to know what conduct leads to adverse consequences, etc.[77]

[72] For a general discussion of the types of relief sandboxes could provide, see *Id.* at 623

[73] Other countries have chosen a more sweeping approach. For example, in Australia, ASIC provides a full exemption from licensing requirements. *See Id.*

[74] One of the concerns with sandboxes is that it may lead to regulators avoiding formal rule-making, which may be more beneficial in the long term. *See* Matthew J. Razzano, *AN UNSAFE SANDBOX: FINTECH INNOVATION AT THE EXPENSE OF CONSUMER PROTECTION?*, 2019, 139 8 (2019).

[75] Rule-making that lacks understanding and expertise could result in confusing and incoherent regulation. See *False Dreams*, Section 3.1, for a discussion of HUD's Proposed Rule on the Implementation of the Disparate Impact standard under the Fair Housing Act. For further analysis in the risks of regulating innovation before it is adequately understood, see Wu, *supra* note 124.

[76] Christine Jolls, *On Law Enforcement with Boundedly Rational Actors*, THE LAW AND ECONOMICS OF IRRATIONAL BEHAVIOR 268, 272 (Francesco Parisi and Vernon L. Smith eds.) (2005).

[77] STEVEN SHAVELL, Foundations of Economic Analysis of Law 87-91, 428-30, 479-82, 492-520, 572-78 (2004).

Ex ante regulation, such as requiring disclosure, works by reducing asymmetric information among the regulated parties and regulators and making the risks transparent to all. With an *ex ante* regulatory-based approach, there is more certainty beforehand. In addition, the regulators will have more flexibility in designing the framework. This is particularly beneficial for regulating the algorithm-based lending industry where the industry is continually upgrading their techniques with alternative data, new machine-learning algorithms, etc. Moreover, instead of focusing on the narrow question of whether a particular lender discriminated or not, *ex ante* regulation improves market analysis and the understanding in general whether credit markets are well-functioning and serve the protected groups adequately by considering the effect big data and machine learning have on market-wide access to credit.[78]

However, *ex ante* regulation is inherently limited. Complex financial markets innovate more quickly than regulators can adapt. Thus, the regulators may not have perfect information, and *ex ante* regulation cannot anticipate every cause and prevent every financial failure. This may lead to inefficient under-regulation of some, and over-regulations of others. *Ex ante* regulation that attempts to prevent all financial harms may end up impeding economic growth or undermine the market experimentation and innovation on which market growth depends.[79]

Ex post remedies initiate only after the harm has occurred, but will help prevent financial harm from spreading and becoming systemic.[80] The threat of liability forces the market players to take appropriate precautions and to internalize the expected social damages.[81] *Ex post* regulation also provides useful additional information when regulated parties are heterogeneous.[82]

However, when *ex post* liability is used exclusively, the uncertainty of legal standards will lead to inefficiencies. *Ex post* lawsuits may not always be brought against regulated parties due to the uncertainty of the legal standard,[83] or the remedy may come too late and the harm no longer can be prevented. Moreover, biased perceptions of the legal standards may also cause the regulated parties to take under- or over-precautions.

Ex post approaches and *ex ante* approaches may supplement each other as part of a comprehensive regulatory framework. For example, *ex ante* regulation can correct the inefficiencies associated with the use of *ex post* liability alone.[84]

[78] Talia Gillis, Discrimination Stress-Testing. Draft.

[79] Steven L. Schwarcz, *Systemic Risk*, 97 Georgetown L.J. 193, 217 (2008).

[80] Steven L. Schwarcz, *Ex Ante Versus Ex Post Approaches to Financial Regulation*, 15 Chapman L. Rev. 257 (Jan. 31, 2011).

[81] Charles D. Kolstad, Thomas S. Ulen and Gary V. Johnson, Ex Post Liability for Harm vs. Ex Ante Safety Regulation: Substitutes or Complements? Working Papers Series on the Political Economy of Institutions No.4, Vol. 80, Col. of Com. and Bus. Admin., Bur. of Econ. and Bus. Res., Univ. of Ill., 888-901 (Dec., 1987), https://www.ideals.illinois.edu/bitstream/handle/2142/29359/expostliabilityf1419kols.pdf?sequence%3D1.

[82] Brian Galle, *In Praise of Ex Ante Regulation*, 68 Vanderbilt L. Rev. 1715 (March 13, 2015).

[83] In the U.S. Supreme Court's landmark decision in *Wal-Mart Stores, Inc. v. Dukes*, 131 S.Ct. 2541 (2011), the Court ruled that a group of roughly 1.5 million women could not be certified as a valid class of plaintiffs in a class-action lawsuit for employment discrimination against Walmart. In this case, the plaintiffs alleged systemic pay and promotion discrimination against women. The plaintiff's sociology expert offered statistical analysis to show a corporate culture vulnerable to gender bias failed to meet this burden. In dismissing the expert's analysis, Justice Scalia's opinion focused on the expert's inability to ascertain whether 0.5 percent or 95 percent of employment decisions at Wal-Mart were determined by stereotyped thinking. The decision substantially raised the bar for plaintiffs to obtain class certification in all types of class actions, and is likely to have a substantial impact on class action law beyond the employment realm. This particularly poses challenges for future anti-discrimination class-action cases, because the Court concluded that, where Wal-Mart's policies allowed local supervisors substantial discretion over pay and promotion matters, the plaintiffs failed to identify "a common mode of exercising discretion that pervades the entire company." Wal-Mart Stores, Inc. v. Dukes

[84] *Ex ante* regulation can correct cases of under-precaution resulting from exposure to *ex post* liability alone, but it can also exacerbate over-precaution. *See* Kolstad, *supra* note 56.

Plaintiff's Burden or Defendant's Burden

Another issue to consider in designing the framework is how to properly allocate the burden of proof between plaintiffs and defendants in assessing disparate impact.

The five-element framework shifts more of the burden to the plaintiffs. It is insufficient to identify a program as a whole without explaining how the program itself causes the disparate impact, as opposed to a particular element of the program. Plaintiffs must identify the particular policy or practice rather than a one-time decision that causes the disparate impact. Without access to the algorithm and dataset, it would be extremely difficult for a plaintiff to establish a prima facie case for algorithmic decision-making. Even with access to the algorithm and dataset, the element of robust causality may be challenging to plead and prove because there is no clear distinction between correlation and causation. It is also not clear how to benchmark "an adverse effect on *members of a protected class*" of the third element according to the previous discussion on group fairness versus individual fairness.

The Court has placed special emphasis on the importance of the plaintiff's prima facie burden, warning that, ''[w]ithout adequate safeguards at the prima facie stage, disparate-impact liability might cause race to be used and considered in a pervasive way and would almost inexorably lead governmental or private entities to use numerical quotas, and serious constitutional questions then could arise.''[85]

Is it fair to ask either plaintiff or defendant to bear the burden of proof in each of these stages? For example, finding statistical disparity may be complicated by the difficulty of obtaining information about protected class status. Law often prevents the collection of protected characteristics to prevent the organization from engaging in disparate treatment. For example, ECOA and Regulation B generally prohibits a creditor from inquiring "about the race, color, religion, national origin, or sex of an applicant or any other person in connection with a credit transaction."[86] There are a few exceptions, including exceptions for applications for home mortgages covered under the HMDA, and for the purpose of "self-test."[87] This creates a Catch-22 situation that while the lenders may be prevented from engaging in disparate treatment by seeking statistical data about disparity, the plaintiffs are also prevented from establishing a prima facie case by showing that statistical disparity.[88]

On the other hand, if defendants bear the burden of proof, would it possible that such a burden would be ultimately transferred to consumers?

Conclusion

Machine learning is a significant development that will continue to have increasing applications within the mortgage lending industry. Within machine learning, mortgage lenders and underwriters are

[85] Inclusive Communities, supra note 20.

[86] 12 CFR § 1002.5(b).

[87] 12 C.F.R. § 1002.5(a)-(d) and 12 C.F.R. § 1002.13.

[88] *See* CFPB, *Using publicly available information to proxy for unidentified race and ethnicity: A methodology and assessment* (Summer, 2014). The CFPB defined an approach using surname and geographic probabilities, Bayesian Improved Surname Geocoding (BISG), to estimate the probability that each applicant belonged to a particular ethnicity and race group. These probabilities are used to assign an ethnicity and race proxy as a substitute for missing data in assessing Fair Lending risk. It is demonstrated that the BISG proxy probability is more accurate than a geography-only or surname-only proxy in its ability to predict individual applicants' reported race and ethnicity and is, generally, more accurate than a geography-only or surname-only proxy at approximating the overall reported distribution of race and ethnicity., https://files.consumerfinance.gov/f/201409_cfpb_report_proxy-methodology.pdf.

going to be more efficient and capable of expanding access to credit and lower the cost. At the same time, it is also important to ensure the use of machine learning with alternative data does not result in disparate and discriminatory treatment.

Most of the time, machine learning algorithms are viewed as a "blackbox," but they should not be handled as invisible designs. Policymakers must understand the limitations of machine learning before endorsing these tools. Machine learning needs to be effective, but also transparent, about how they are making decisions about the reasons that certain applicants are denied credit or obtain different interest rates than others.

The CFPB is dedicated to expanding fair, equitable, and nondiscriminatory access to credit and to ensuring that consumers are protected from discrimination. The CFPB remains optimistic that the financial sector will find valuable ways to employ machine learning techniques in the near future.

Briefing Questions

Having examined the proposals, please review the materials included in the attached Appendix and prepare to brief the Director. In particular, the Director is eager to know your thoughts as to the following:

- To what extent is the practical and desirable to impose a requirement of transparency or explanation in the use of algorithms in decision-making in order promote fairness?
- What are the comparative strengths and weaknesses of the two options: ex post enforcement versus an ex ante review process of some sort for algorithm driven loan underwriting?
- How well does each option align with the decision and analysis in *Inclusive Communities*?
- How might each option impact the likelihood of success of disparate impact claims brought in the future?
- What are the pros and cons for choosing between "legally sufficient justification" and "business justification" requirements in the burden-shifting framework?
- What would be a likely reaction from industry players to these proposals? Consider the following examples:
    - Civil Rights Groups
    - Local government
    - Banks
    - AI companies
- How might each option increase or decrease costs and economic burden to relevant parties?
- For the ex ante option, consider the following questions:
    - What is considered a "neutral" database for evaluating an algorithm?
    - What are the potential challenges in constructing a neutral database?
    - Will there be proprietary concern for the lenders to give their algorithms to regulator to test, or should the lenders take control of running the outcome-based analysis?
    - What principles should be used to determine who is similarly situated?

- How will each option impact credit-accessibility to underserved communities?
- Who should be liable if a practice is found discriminatory? The lender or the third-party companies who design the algorithm?

Appendices

1. Executive Order on Maintaining American Leadership in Artificial Intelligence
   https://www.whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/

Credit Invisible

2. Building a bridge to credit visibility - a report on the CFPB's credit visibility symposium
   https://www.consumerfinance.gov/about-us/blog/report-credit-visibility-symposium/

Federal Fair Lending Laws

3. Equal Credit Opportunity Act (Regulation B) 12 CFR Part 202.
4. Discriminatory Conduct Under The Fair Housing Act. 24 CFR Part 100.

Disparate Impact

5. Federal Fair Lending Regulations and Statutes. Pages 2-3
   https://www.federalreserve.gov/boarddocs/supmanual/cch/fair_lend_over.pdf

Supreme Court Caselaw

6. Texas Department of Housing and Community Affairs v. Inclusive Communities Project, Inc., 135 S. Ct. 2507 (2015).

The Role of CFPB

7. CFPB Fair Lending Report. Page 7-11, Page 15
   https://files.consumerfinance.gov/f/documents/201906_cfpb_Fair_Lending_Report.pdf

Machine Learning

8. Gentle Introduction to Machine Learning
   https://youtu.be/Gv9_4yMHFhI

Machine Learning in Lending

9. An update on credit access and the Bureau's first No-Action Letter
   https://www.consumerfinance.gov/about-us/blog/update-credit-access-and-no-action-letter/
10. An Update from CFPB on Upstart's No-Action Letter
    https://www.upstart.com/blog/an-update-from-cfpb-on-upstarts-no-action-letter

Challenges of Machine Learning in Lending

11. Request for Information Regarding Use of Alternative Data and Modeling Techniques in the Credit Process
https://www.govinfo.gov/content/pkg/FR-2017-02-21/pdf/2017-03361.pdf

Optional reading:

12. R Rahul Bhargava, "The Algorithms Aren't Biased, We Are," Medium (Jan. 3, 2018)
https://medium.com/mit-media-lab/the-algorithms-arent-biased-we-are-a691f5f6f6f2
13. Finale Doshi-Velez et al., "Accountability of AI Under the Law: The Role of Explanation," https://arxiv.org/abs/1711.01134

Ex Post Regulation and Ex Ante Regulation

14. Steven Shavell, Foundations of Economic Analysis of Law 87-91, 428-30, 479-82, 492-520, 572-78 (2004).
15. HUD's Implementation of the Fair Housing Act's Disparate Impact Standard: A Proposed Rule by the Housing and Urban Development Department on 08-19-2019
https://www.federalregister.gov/documents/2019/08/19/2019-17542/huds-implementation-of-the-fair-housing-acts-disparate-impact-standard
16. Talia Gillis, *False Dreams of Algorithmic Fairness: the Case of Credit Pricing*, talk at Harvard Empirical Legal Studies, Harvard Law School (Sept. 20, 2019), available at
https://scholar.harvard.edu/files/gillis/files/gillis_jmp_191101.pdf
17. Talia Gillis, *Discrimination Stress Testing*.

PART IV

PAYMENTS

HARVARD LAW SCHOOL | The Case Studies

CSP058
MAY 2020

Mobile Payments for the Developing World

JONATHAN GREENACRE

Memorandum

DATE: February 18, 2020

TO: Thomas Smith, Senior Attorney, World Bank Payments Division

FROM: Sally Edwards, Junior Attorney, World Bank Payments Division

RE: Mobile Payments for the Developing World

Please review the following material outlining the mobile payment systems for the developing world in an attempt to answer the following questions:

1. What type(s) of mobile payment system(s) should the World Bank encourage across its client countries and why?
2. What policy and other issues are relevant to determining whether a payment system is likely to operate effectively in specific client countries?
3. What are the main risks to users' funds stored within new mobile-payment systems to protect the user if the provider enters bankruptcy proceedings?
4. What policy issues arise when designing legal and regulatory strategies to address those risks?

Written by Jonathan Greenacre, Boston University, with comments received from Howell E. Jackson, James S. Reid, Jr., Harvard Law School, Margaret E. Tayar, Davis Polk & Wardwell, and Will Paterson, World Bank. This Case Note draws upon a range of Greenacre's work, including *What is the Role of M-Pesa in Kenya's Economy?* (current working paper), *The Roadmap Approach to Regulating Digital Financial Services*, 1 JOURNAL OF FINANCIAL REGULATION 298 (2015), *The Regulation of Mobile Money*, Oxford BLAVATNIK SCHOOL OF GOVERNMENT PATHWAYS FOR PROSPERITY COMMISSION ON TECHNOLOGY AND INCLUSIVE DEVELOPMENT (2018), and an upcoming book manuscript, *The Regulation of Mobile Money* (Cambridge University Press, forthcoming, 2020). Case development at Harvard Law School is partially funded by a grant from Dechert LLP. Cases are developed solely as the basis for class discussion. They are not intended to serve as endorsements, sources of primary data, legal advice, or illustrations of effective or ineffective management.

Copyright © 2020 President and Fellows of Harvard University. No part of this publication may be reproduced, stored in a retrieval system, used in a spreadsheet, or transmitted in any form or by any means—electronic, mechanical, photocopying, recording, or otherwise—without permission. To order copies or permissions to reproduce materials please visit our website at casestudies.law.harvard.edu or contact us by phone at 617-496-1316, by mail at Harvard Law School Case Studies Program, 1545 Massachusetts Avenue – Areeda 507, Cambridge, MA 02138, or by email at HLSCaseStudies@law.harvard.edu.

Introduction

The proliferation of mobile phones in the developing world is generating opportunities to provide payment services far beyond the banking system. Only 63% of people in developing countries have access to a bank account[1] but 78% own a mobile phone.[2]

Increasingly, non-bank firms are taking advantage of the growth of mobile phones to provide payment systems, including mobile money (particularly M-Pesa in Kenya), Alipay and, more recently, central bank currencies.

The World Bank wants to assist with the spread of new mobile payment systems among its client countries and to ensure that these payment systems are faster, cheaper and potentially safer than the cash-based payment systems typically used by low-income communities.

The World Bank needs to be consistent with several policy goals, including financial inclusion, to extend payment systems to those without a bank account, known colloquially as the "unbanked."[3] Financial inclusion is an important interest of the World Bank, because low-income communities, particularly the unbanked, appear better able to move out of poverty when they can access formal financial services.[4] Furthermore, financial inclusion is a policy goal for over 80 developing countries, making it important when considering policy trade-offs.[5]

In addition to financial inclusion, the World Bank is particularly concerned about the liquidity of payment providers and, as a consumer-protection issue, the protection of users' funds in the event of bankruptcy of such firms.[6]

The World Bank is also mindful of potential challenges that policymakers may face with implementing, monitoring, and supervising payment systems. In many developing countries, policymakers have resource constraints in relation to staffing, technology, and operating systems, impeding their ability to oversee existing payment and banking systems. Adopting new payment systems would put such constraints under additional pressure by requiring new regulatory and supervisory arrangements.

Certain new mobile payment systems have grown very quickly and realization of loss of value or liquidity risk may contribute to various forms of systemic risk. The World Bank is interested in learning more about the operation of potential systemic risks that could arise through the collapse of such mobile payment systems. The World Bank is also concerned that problems with insolvency regimes in many developing countries may mean that legal instruments used widely for new payment systems may have limited effectiveness. A key limitation with such regimes is their relative slow pace of operation. For

[1] Asli Demirgüç-Kunt, Leora Klapper, Dorothe Singer, Saniya Ansar and Jake Hess, *World Bank Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution*, WORLD BANK (2018).

[2] Laura Silver, *Smartphone Ownership is Growing Rapidly Around the World, but Not Always Equally*, PEW RESEARCH CENTER (Feb. 5, 2019), https://www.pewresearch.org/global/2019/02/05/smartphone-ownership-is-growing-rapidly-around-the-world-but-not-always-equally/.

[3] United Nations Secretary-General's Special Advocate for Inclusive Finance for Development, *The Imperative of Financial Inclusion*, UNSGSA (2015), http://www.unsgsa.org/about/financial-inclusion (last visited Sept. 29 2015).

[4] For a discussion of the apparent poverty-alleviating benefits of M-Pesa, *see* Tavneet Suri and William Jack, *The Long Run Poverty and Gender Impacts of Mobile Money*, 354 SCIENCE, 1288 (Dec. 9, 2016).

[5] *Alliance for Financial Inclusion Members*, ALLIANCE FOR FINANCIAL INCLUSION, https://www.afi-global.org/members/ (last visited Sept. 15, 2019). But consider that typically only developing countries are Members of the Alliance, which may point to differing attitudes between developing and developed countries.

[6] For a discussion of risks to users' funds stored in the shadow payment system, *see* Dan Awrey and Kristin van Zwieten, *The Shadow Payment System,* 43 IOWA LAW SCH. JOUR. OF CORP. LAW 775, 779, 805-6 (Apr. 21, 2017).

example, the World Bank estimates that the average bankruptcy proceeding in sub-Saharan Africa takes three years. The remainder of this memo outlines the basic operation of several particularly prevalent non-bank payment systems that have been launched or have been intended for launch in the developing and emerging regions of the world. These include M-Pesa in Kenya, Alipay in China, a central bank currency in Ecuador, and Facebook-backed Libra.

M-Pesa in Kenya

M-Pesa, launched in Kenya in 2007, is the world's first "mobile-money" service.[7] A customer converts cash for an electronic currency called "e-money" that is issued by Safaricom, a phone company operating as a subsidiary of Vodacom.[8] The customer performs this cash-in function at a "cash merchant," which is usually a corner store, post office, or another type of retail outlet. The cash merchant operates on behalf of Safaricom.[9] An M-Pesa account provides very similar functionality as a bank deposit—a customer can store their funds in the M-Pesa service; transfer e-money to other M-Pesa users through text messages on their mobile phone; and convert any remaining e-money in their account into cash at a cash merchant.

Cash merchants use their own reserves of e-money and cash for transactions rather than those of the phone company. To deposit funds into their account, a customer hands cash to the cash merchant. In return, the cash merchant uses the M-Pesa app on their mobile phone to send an equivalent amount of 'e-money' to the customer's M-Pesa account. A withdrawal transaction operates in reverse.

When a cash merchant needs additional e-money or cash, they transact with other actors in the M-Pesa system, particularly 'aggregators.' These are larger retail outlets, such as supermarkets, which store more substantial reserves of e-money and cash. To do so, the cash merchant and the supermarket exchange an equivalent amount of e-money for cash, much like a customer and a cash merchant. Aggregators themselves obtain additional e-money or cash from Safaricom.

M-Pesa grew rapidly, triggering the expansion of mobile money in Kenya and other developing regions. There are now around 26 million M-Pesa users in Kenya.[10] By 2018 there were 866 million mobile money accounts worldwide, overwhelmingly located in the developing world.[11]

[7] Timothy Lyman, Mark Pickens and David Porteous, *Regulating Transformational Branchless Banking*, CONSULTATIVE GROUP TO ASSIST THE POOR, (January, 2008), http://www.cgap.org/publications/regulating-transformational-branchless-banking, 1-24 (last visited Sept. 29, 2015).

[8] For the full definition of "e-money" *see* Mobile Financial Services Working Group, *Mobile Financial Services: Basic Terminology*, ALLIANCE FOR FINANCIAL INCLUSION (2013), http://www.afi-global.org/library/publications/mobile-financial-services-basic-terminology-2013 (last visited Sept. 29, 2015)): "A type of monetary value electronically recorded and generally understood to have the following attributes: (i) issued upon receipt of funds in an amount no lesser in value than the value of the e-money issued; (ii) stored on an electronic device (e.g. a chip, prepaid card, mobile phone, or computer system); (iii) accepted as a means of payment by parties other than the issuer; and (iv) convertible into cash." Note that in contracts between mobile money firms and customers, e-money is often defined as electronic monetary value depicted in the customer's mobile money account. For example, see the definition of "e-money" in Safaricom, *M-Pesa Terms and Conditions*, SAFARICOM https://www.safaricom.co.ke/images/Downloads/Terms_and_Conditions/CUSTOMER_TERMS_March_2012.pdf.

[9] Safaricom, *M-Pesa Agents*, SAFARICOM, https://www.safaricom.co.ke/personal/m-pesa/get-started-with-m-pesa/m-pesa-agents (last visited Nov. 8, 2014).

[10] Mutsa Chironga, Hilary De Grandis, and Yassir Zouaoui, *Mobile financial services in Africa: Winning the battle for the customer*, McKinsey & Company (Sept. 2017), https://www.mckinsey.com/industries/financial-services/our-insights/mobile-financial-services-in-africa-winning-the-battle-for-the-customer.

[11] Francesco Pasti, *State of the Industry Report on Mobile Money*, GSMA (2018), https://www.gsma.com/r/wp-content/uploads/2019/05/GSMA-State-of-the-Industry-Report-on-Mobile-Money-2018-1.pdf.

Safaricom launched M-Pesa in a time of high financial exclusion with widespread use of cash by the unbanked and limited competition from other firms, particularly banks. In 2007, before the launch of M-Pesa, over 81% of the population did not have a bank account and tended to use cash-based payment systems.[12] Banking outreach was limited. Kenya had 3.4 bank branches per 100,000 people, significantly lower than the global average of 11.6 branches per 100,000 people.[13] In the same year, Kenya had 4.6 ATMs per 100,000 people against a global average of 18.9.[14]

Safaricom took advantage of the very rapid spread of mobile phones in Kenya and its role as a key provider of phone services. Between 2002 and 2006, the number of mobile phones in Kenya increased from 1 million to 10 million.[15] Many of these mobile phone subscribers had a pre-existing contractual relationship with Safaricom rather than a relationship with a bank. Furthermore, M-Pesa does not require a smartphone–it can operate effectively on a comparatively rudimentary 2G mobile phone.

Safaricom and the Central Bank of Kenya (CBK), the government agency ultimately responsible for the regulation of M-Pesa, also had specific goals for the service. The system was designed to specifically target unbanked communities and achieve financial inclusion. To that end, the service would complement, rather than substitute, the bank-based payment system. This meant that M-Pesa would be a vehicle for storing and transferring a small amount of funds. However, the Kenyan banking system would perform the majority of payments (namely, those involving larger amounts of funds) and provide credit creation in the economy.

To that end, M-Pesa also grew in a relatively liberal regulatory environment, in part because of the emphasis on financial inclusion. The CBK did not design extensive regulatory frameworks for the service until 2014–seven years after its launch. Until then, Safaricom was permitted to provide the service through contractual mechanisms only, subject to extensive CBK oversight, limiting regulatory costs it might have otherwise faced. Such supervision was relatively feasible for the CBK because M-Pesa involved relatively simple private law strategies to protect customers' funds against liquidity and bankruptcy risks. Customers' funds were stored in a trust (as a means of segregating such funds from assets of Safaricom) and placed in a bank (to reduce the marginal probability of liquidity and potential bankruptcy risk). In so doing, M-Pesa did not involve credit creation of the type that tends to attract more extensive regulatory and supervisory oversight. Instead, credit creation took place in the Kenyan banking system, which was already subject to prudential regulation and oversight.

This legal arrangement helps explain the mechanisms of deposit and withdrawal transactions. When depositing funds, a customer hands over cash and the cash merchant sends e-money to them, comprising a portion of their (the cash merchant's) beneficial interest in the M-Pesa trust fund. When withdrawing funds, the customer sends a portion of e-money (comprising a portion of their beneficial interest in the M-Pesa trust fund) to the cash merchant. In exchange, the cash merchant provides an

[12] Alliance for Fin. Inclusion, *The 2010 AFI survey report on financial inclusion policy in developing countries*, ALLIANCE FOR FINANCIAL INCLUSION (2010), https://www.afi-global.org/sites/default/files/publications/afi%20survey%20report%202010-en.pdf.

[13] The International Monetary Fund, Financial Access Survey, *Commercial Bank Branches (per 100,000 adults) - Kenya*, THE WORLD BANK, https://data.worldbank.org/indicator/FB.CBK.BRCH.P5?locations=KE (last visited Sept. 15, 2019).

[14] The International Monetary Fund, Financial Access Survey, *Automated Teller Machines (ATM's) (per 100,000 adults)*, THE WORLD BANK, https://data.worldbank.org/indicator/FB.ATM.TOTL.P5 (last visited Sept. 15, 2019).

[15] Harry McGee, *How the mobile phone changed Kenya*, THE IRISH TIMES (May 14, 2016), https://www.irishtimes.com/news/world/africa/how-the-mobile-phone-changed-kenya-1.2646968.

equivalent amount of cash to the customer. Safaricom was also given broad regulatory freedom to design cash merchant arrangements that would help customers convert cash for so-called "e-money" and vice versa. Safaricom moved quickly to develop such arrangements and now has over 110,000 M-Pesa cash merchants across Kenya.[16]

Since its launch, M-Pesa has encountered a range of regulatory and policy issues. For example, the amount of M-Pesa funds stored with the trust bank deposit (which is "pooled" and stores funds received from a large number of specific M-Pesa accounts) far exceeded Kenya's deposit-insurance ceiling and M-Pesa customers' funds are virtually completely uninsured against bank failure.[17] As a result, some countries have begun to explore the introduction of pass-through deposit insurance, whereby each mobile-money account pooled within the trust bank account receives the full protection of pass-through deposit insurance. For example, on January 18, 2016, the Nigeria Deposit Insurance Corporation announced that pass-through deposit insurance would be extended to mobile money, making Nigeria the first, and currently only, country to do so.[18] The system insures each individual mobile money account up to $3,255.[19] Such regulatory strategies would appear to give similar protection for mobile money as bank deposits.

Pass-through deposit insurance raises a broader question of supervisory capability of policymakers grappling with mobile money. A number of policymakers have expressed doubt about their ability to supervise pass-through deposit insurance given their pre-existing resource constraints.

The CBK had an advantage over policymakers in other countries because it could learn about mobile money from the very beginning of the evolution of M-Pesa.[20] These regulators were involved in the launch of mobile money from its beginning in 2007 and adopted a "test-and-learn" approach that allowed them to develop regulatory insights which could be applied and evolved as M-Pesa grew.[21] Other policymakers had to deal with potential entrants wanting to launch at scale, making the test-and-learn approach less feasible.

A related challenge for mobile money revolves around the relatively slow speed of bankruptcy regimes in many countries in which the service operates. In theory, the trust arrangement means customers' funds cannot be claimed by creditors and so are available for distribution to customers. However, this arrangement cannot, in itself, ensure that such funds will be returned quickly to customers. The World Bank estimates that the average bankruptcy proceeding in Kenya takes four and a half years.[22] Customers may face a long delay in receiving their funds if their funds have been deposited with a mobile-money service when it enters bankruptcy proceedings. It is not clear what type of accelerated bankruptcy

[16] Francois De Soyres, Mohamed Abdel Jelil, Caroline Cerruti and Leah Kiwara, *What Kenya's Mobile Money Success Could Mean For the Arab World*, THE WORLD BANK (Oct. 3, 2018), https://www.worldbank.org/en/news/feature/2018/10/03/what-kenya-s-mobile-money-success-could-mean-for-the-arab-world.

[17] William G. Jack and Tavneet Suri, *The Economics of M-Pesa*, *Working Paper*, MASS. INST. OF TECH. (Aug. 2010), http://faculty.georgetown.edu/wgj/papers/Jack_Suri-Economics-of-M-PESA.pdf.

[18] Babajide Komolafe, *NDIC Issues Deposit Insurance Guidelines for Mobile Money*, VANGUARD (Jan. 18, 2016), http://www.vanguardngr.com/2016/01/ndic-issues-deposit-insurance-guidelines-for-mobile-money.

[19] Kingsley O. Nwaigwe (Deputy Director, Research Policy and International Relations Department, Nigeria), *Deposit Insurance and Mobile Money in Africa*, IADI Africa Regional Committee Conference, Zanzibar, Int'l Assoc. of Deposit Insurers (Sept. 1, 2016).

[20] *Id.*

[21] Njuguna Ndung'u, *Digital Technology and State Capacity in Kenya, Policy Paper 154*, CTR. FOR GLOBAL DEV. (AUG. 6, 2019), https://www.cgdev.org/publication/digital-technology-and-state-capacity-kenya.

[22] The World Bank, *Resolving Insolvency*, THE WORLD BANK (2018), https://www.doingbusiness.org/en/data/exploretopics/resolving-insolvency.

regime could be used to address this problem, because such regimes are normally applied to banks and other types of financial intermediaries, not non-banks providing only payment services.

A number of other issues have arisen as M-Pesa and other mobile-money services have grown and spread to other countries. For example, civil-law countries have greater challenges segregating customers' funds from other assets of the relevant mobile-money firm, because such countries often do not have trusts and therefore require alternative legal tools.[23]

More generally, the service has struggled to grow in other countries, including some of the fastest-growing developing countries and emerging markets, such as India, Indonesia, Nigeria, Mexico, and South Africa.

A range of factors appears to impede the spread and growth of mobile money. One such factor is heavy regulation, including insistence on stringent know-your-customer (KYC) rules. The closer such rules resemble KYC requirements for bank deposits, the less of a cost advantage mobile money enjoys, prohibiting its ability to reach "down-market" and serve low-income and unbanked communities. Rules also require non-banks to partner with banks, and often the bank receives the relevant mobile-payment license. Such partnerships also introduce costs because non-banks must obtain bank approval before launching and growing products. Other countries with stronger competition from banks, manifested through lower percentages of unbanked populations, also appear to impede the growth of mobile money, as people can already access many of the features inherent in mobile-money platforms through their bank accounts or their specific bank app.[24] A recent study shows that the higher the average income of a developing country, the less likelihood that third-party mobile money platforms are successful.[25]

Alipay in China

Ant Financial is an affiliate company of the Alibaba group, focusing on fintech and whose primary product is the mobile-payment service Alipay. Like a bank deposit, Alipay operates as a mobile wallet with a number of in-app services which can be used to pay for a range of services, such as taxicabs, movie tickets, and utility bills.[26] The app can also be used to transfer money to other Alipay users.[27] Customers can deposit money in their Alipay wallets, which can then be used to purchase goods or services.[28] Ant Financial also launched its own virtual credit card, Huabei, as an add-on service for Alipay users.

Customers have two options when transferring their funds using the Alipay system. One is non-instantaneous in nature, *i.e.*, transactions take place after confirmation of satisfactory receipt of service

[23] David Ramos Munoz, Javier Solana, Ross Buckley and Jonathan Greenacre, *Protecting Mobile Money Customer Funds in Civil Law Jurisdictions*, 65 INT'L & COMP. L. Q. 705 (2016).

[24] David S. Evans and Alexis Pirchio, *An Examination of Why Mobile Money Schemes Ignite in Some Developing Countries But Flounder in Most, Working Paper No. 723*, COASE-SANDOR INST. FOR L. AND ECON, UNIV. OF CHICAGO L. SCH. (March, 2015), https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=2413&context=law_and_economics.

[25] *Id.*

[26] Lily Kuo, *Digital Wallet' of Ant Financial Captivates China and beyond*, THE GUARDIAN (May 28, 2018), https://www.theguardian.com/technology/2018/may/28/digital-wallet-of-ant-financial-captivates-china-and-beyond.

[27] *Id.*

[28] Alipay, *Alipay Hong Kong Wallet Service Agreement*, ALIPAY (Aug. 2018), https://render.alipay.hk/p/s/hkwallet/agreement/service/agreed?_lang=en_us&chinfo=hk_portal#index.

or goods.[29] Until that point, the money is held in escrow. Alternatively, customers can elect for instantaneous payment where payments are quickly made, but funds are not stored in escrow.

To use Alipay, a customer opens an Alipay account on a mobile phone, which comes with an attached mobile wallet, and then uploads funds into their mobile wallet.[30] All money stored on the Alipay wallet account is stored on the Alipay system.[31] In accordance with the most recent direction of the People's Bank of China, any customer funds which are not immediately transferred to their bank accounts or used for a purchase must be stored in a dedicated custodial account in a commercial bank.[32] This is to protect customers' funds and to prevent any abuse or fraud.[33]

Alipay was first launched in 2004 as a payment mechanism for Taobao, the world's largest e-commerce marketplace. In 2010, Alipay became a third-party payment system enabling it to provide services to additional actors beyond Taobao. This practice gave Alipay the ability to serve the growing number of Chinese who are connected to the internet mainly through mobile phones.[34]

Alipay has grown significantly in China due to a number of reasons. Through particular legal arrangements, the service developed customers' trust about its reliability and security. One key mechanism involved holding customers' funds in escrow until the required transaction is complete. This mechanism helped address problems of fraud in China's e-commerce system, which was riddled with transactions in which customers were sold defective goods. Alipay overcame this issue by holding the payment in escrow until the customer indicated satisfaction with the purchase, which built the credibility of Taobao and Alipay.[35] Growing trust in online transactions, therefore, helped increase Taobao's and Alipay's business.

Alipay also enjoyed a lack of competition from banks and credit card companies in China. Credit and debit card penetration in China has been historically low.[36] Alipay facilitates payments without using cash, a credit card, or a debit card, which enabled China to leapfrog countries that relied on such instruments.

Alipay also benefited from the closed nature of China's internet system, which prevents ready access to local internet for non-Chinese companies. Stringent data-sharing norms, the lack of any privacy protections, censorship laws, and complex cybersecurity regulations serve as barriers to entry for non-Chinese firms.[37] Certain foreign firms have sought to navigate these challenges to invest in China but later withdrew. For example, Amazon entered China in 2004, but closed its operations in 2019.[38]

[29] *Id.*

[30] *Id.*

[31] *Id.*

[32] Gabriel Wildau, *Tencent and Alipay set to lose $1bn in revenue from payment rules,* FIN. TIMES (July 15, 2018), https://www.ft.com/content/b472f73c-859e-11e8-96dd-fa565ec55929.

[33] *Id.*

[34] Lerong Lu, How a Little Ant Challenges Giant Banks? The Rise of Ant Financial's Fintech Empire and Relevant Regulatory Concerns, INT'L CO. & COM. L. REV. (2018).

[35] Payments, *Alibaba: From Start to Now (And Wow)*, PYMENTS.COM (Sept. 18, 2014), https://www.pymnts.com/news/2014/alibaba-from-start-to-now-and-wow/.

[36] Lu, s*upra* note 34.

[37] Assoc. Press, *Beijing Targets Foreign Firms In Internet Crackdown*, S. CHINA MORNING POST (July 20, 2017), https://www.scmp.com/news/china/policies-politics/article/2103458/beijing-targets-foreign-firms-internet-crackdown.

[38] Arjun Kharpal, *Amazon is shutting down Its China marketplace business. Here's why it has struggled*, CNBC (Apr. 18, 2019), https://www.cnbc.com/2019/04/18/amazon-china-marketplace-closing-down-heres-why.html.

Alipay does not work on 2G mobile phones; instead, customers must use a smartphone, which enabled the Alipay service to grow because of the rapid expansion of smartphone users. China now has over 713 million smartphone users.[39]

Alipay also bundled together payment services with other financial services, particularly opportunities to access credit, to enable it to provide to customers a holistic set of financial instruments. Extension of formal credit has been comparatively low in China. In 2014, fewer than 10% of China's population had access to credit through a formal financial institution.[40] Ant Financial's credit and insurance products, offered through Alipay, bridge this gap by providing these products to anyone who has a mobile phone.

One product includes a low-cost health insurance product, dubbed "mutual protection," that covers the cost of treating 100 illnesses. The cost of the insurance is shared by all participants in the product with a cap of 188 yuan ($26) per month.[41] Customers can register for this product and make payments through the Alipay app.[42]

Ant Financial also offers an online cash management platform called Yu'e Bao, which is essentially a form of money market fund in which customers can invest through the Alipay platform.[43] This platform is directed primarily at people who have spare money in their Alipay wallets and it has grown to become the largest money-market fund in the world with assets of $233 billion.[44]

Compared to other developing countries, the People's Bank of China (PBOC), the Chinese central bank, has significantly greater institutional capability and the capacity to regulate new fintech products. The PBOC has taken a "wait-and-see" approach to Alipay and related products, enabling the bank to learn how they work and develop regulatory frameworks. For example, Alipay launched in 2004 and the PBOC did not institute regulations until 2010.[45] The PBOC developed additional regulations in 2019.[46] These regulations are not publicly available.

The sheer number of Alipay users and huge number of transactions raises complex questions around systemic risk. The service now involves one billion users worldwide with over 800 million citizens in China making 500 million transactions per day.[47] Chinese policymakers may need to determine whether Alipay is systemically important and, if so, what regulatory tools to use should it fail. These decisions are challenging partly because China's non-bank payment system is bigger than any other country and may take a form of systemic risk not seen in other jurisdictions. Furthermore, most international standards contain a central assumption that banks, not non-banks, provide payment systems, and international

[39] Lu, s*upra* note 34.

[40] Lu, s*upra* note 34.

[41] Shu Zhang, *China's Ant Financial amasses 50 million users, mostly low-income, in new health plan*, REUTERS (Apr. 12, 2019), https://www.reuters.com/article/us-china-ant-financial-insurance/chinas-ant-financial-amasses-50-million-users-mostly-low-income-in-new-health-plan-idUSKCN1RO0H5.

[42] *Id.*

[43] Georgina Lee, *China's giant Yu'e Bao money market fund riskier than US rival, Fitch says*, S. CHINA MORN. POST (Dec 15, 2017), https://www.scmp.com/business/money/markets-investing/article/2124465/chinas-giant-yue-bao-money-market-fund-riskier-us.

[44] *Id.*

[45] Lu, s*upra* note 34.

[46] Jason Lee, *China's central bank says will gradually set up rules to regulate fintech*, REUTERS (Mar. 16, 2019), https://www.reuters.com/article/us-china-pboc-fintech/chinas-central-bank-says-will-gradually-set-up-rules-to-regulate-fintech-idUSKCN1QX05V.

[47] Tingyi Chen, *The cross-border payment war of WeChat Pay and Alipay*, WALKTHECHAT (Feb. 25, 2019), https://walkthechat.com/the-cross-border-payment-war-of-wechat-pay-and-alipay/.

standards reflect this assumption. For example, the *Core Principles of Systemically Important Payment Systems* issued by the Bank for International Settlements in 2001 (BIS Principles) assume that banks, not non-banks, provide the accounts through which payments are made.[48] The BIS Principles then focus on systemic risk as taking the form of a contagion between banks and, through them, the stability of the system on financial markets.[49] Other international standards make similar assumptions.[50]

Policy questions are also informed by other policy objectives for Chinese regulators. Financial inclusion has been a stated objective and there has been recognition that Alipay's model has the potential to further this goal.[51] The PBOC has revealed that it intends to utilize fintech platforms like Ant Financial to enhance the flow of credit and reduce finance costs for businesses.[52] However, it remains unclear whether Ant Financial's products actually do help in extending financial inclusion, especially in rural areas, and what role the PBOC envisages such systems will play in reaching its goal of financial inclusion.[53] While there is not much public information about the PBOC's thinking on this issue, given the size and potential of Ant Financial and its products, there cannot be any doubt about the apparent importance of Ant Financial to the PBOC's financial-inclusion goals.

Ant Financial's products, especially Alipay, are being increasingly accepted outside China. Alipay is now available in 54 international markets, most of which are in the West and in Southeast Asia. Ant Financial's success in reaching these markets is driven primarily by the need to cater to Chinese tourists who are now the biggest global spenders.[54] Acceptance of Alipay's payment mechanism allows local businesses in these countries to readily attract Chinese tourists. Another factor for the growth of Alipay's platforms, especially within countries in The Association of Southeast Asian Nations (ASEAN), is the presence of large Chinese diasporas cropping up in the countries of this region and more individuals using Ant Financial's products to transact with their families back in mainland China.[55] Ant Financial has also been exporting its model to other countries, primarily through investments in similar financial products

[48] Comm. on Payment & Settlement Sys., *Core Principles for Systemically Important Payment Systems*, Bank for Int'l Settlements ¶ 1.1, ¶ 3.0.1 (Jan. 2001), http://www.bis.org/cpmi/publ/d43.pdf (last accessed Apr. 8 2016) (defines payment systems "as the means by which funds are transferred among banks").

[49] *Id* at ¶ 3.0.1, defines "systemic risk" as "[T]he risk that the inability of one of the participants to meet its obligations, or a disruption in the system itself, could result in the inability of other system participants or of financial institutions in other parts of the financial system to meet their obligations as they become due. Such a failure could cause widespread liquidity or credit problems and, as a result, could threaten the stability of the system or of financial markets."

[50] In particular, international standards have been issued at the level of the Financial Stability Board, Basel Committee on Banking Supervision, and International Organization of Securities Commission to identify systemic firms. Such forms can take the form of banks, traders, shadow banks, market infrastructure providers or any other type of institution. *See, e.g.*, Werner Bijkerk, Shane Worner, Rohini Tendulkar, Siddhartha Sanghi, *Systemic Risk Identification in Securities Markets*, Int'l Org. of Sec. Comm. 53 (2012); *see* Bank for Int'l Settlements, *Global Systemically Important Banks: Assessment methodology and the Additional Loss Absorbency Requirement*, (Nov. 2011) Fin. Stab. Bd., Int'l Monetary Fund, Bank for Int'l Settlement, *Guidance to Assess the Systemic Importance of Financial Institutions, Markets and Instruments: Initial Considerations*, (Oct. 2009); Financial Stability Board, Int'l Monetary Fund, Bank for Int'l Settlement 3; and Basel Comm/ on Bank'g Supervision, *'A Framework for Dealing with Domestic Systemically Important Banks*, BASEL COMM. ON BANKING SUPERVISION 2.

[51] Douglas Randall and Jennifer Chien, *Fintech As A Pathway to Financial Inclusion? The Case of China*, FINDEV GATEWAY (April 2018), https://www.findevgateway.org/blog/2018/apr/fintech-pathway-financial-inclusion-case-china.

[52] *Id*.

[53] Tyler Aveni and Joep Roest, 2017. *China's Alipay and WeChat Pay: Reaching Rural Users, CGAP Brief*, WORLD BANK (2017), https://openknowledge.worldbank.org/handle/10986/30112.

[54] John Detrixhe, *China's Ant Financial, thwarted in the US, is expanding rapidly in Europe*, QUARTZ (Mar. 15, 2019), https://qz.com/1570052/ant-financials-alipay-is-expanding-rapidly-outside-of-china/.

[55] *Id*.

like PayTM in India.[56] It is unclear whether Ant Financial will be able to grow in other countries at a similar rate as in China. Ant Financial will not enjoy the restrictions on investment that make it costly for non-Chinese companies, particularly technology firms such as Amazon and Google, to succeed in the Chinese market.

Central Bank Currency in Ecuador (2014 to 2017)

In the past few years, central banks across the world have shown a growing interest in introducing central-bank backed digital currencies. This interest has been driven by two considerations—first, the perceived need to compete with independent cryptocurrencies like Bitcoin and Libra, which could theoretically undercut the power of central banks globally;[57] and second, the goal of financial inclusion, in which digital currencies are often seen as a cost-effective means of increasing access to formal financial services.[58]

As currently designed, a centrally-backed digital currency would involve two components—first, the currency itself, a digital equivalent of the domestic fiat currency (for example, a digital dollar) which can be used to transact online; and second, a means to use this currency, normally in the form of a digital wallet or a specific digital currency account, where the currency would be stored and transactions can occur primarily through the use of mobile phones.[59]

Ecuador's government became interested in the introduction of a central bank currency—later termed Dinero Electronico (DE)—for reasons that are not immediately clear. It appears that financial inclusion was not directly relevant, even though this is a policy goal of Ecuador.[60] Some commentators have argued that the DE was a way to de-dollarize the economy. Ecuador was forced to fix the value of the Sucre (the local currency) to the U.S. dollar during a period of hyperinflation in 1999.[61]

In September, 2014, the Banco Central de Ecuador (BCE) launched DE and people could spend money in their accounts by February 2015.[62] However, the electronic money system was decommissioned in 2017.[63]

DE was designed to substitute digital currency for physical currency. Users needed to create special accounts to use the currency, which would be kept on the central bank's own balance sheet, and transfer the currency using a mobile phone app. To actually use DE, people would get special accounts registered with the BCE itself, which could be accessed and used using a mobile phone.[64] Use of DE was voluntary.

[56] Simon Mundy, *Alibaba to invest $177M in India's Paytm*, FIN. TIMES (Mar. 2, 2017), https://www.ft.com/content/5cbb69bf-a2ae-3288-8500-27656a12067b.

[57] Morten Linnemann Bech and Rodney Garatt, *Central Bank Cryptocurrencies*, BANK FOR INTL SETTLEMENTS Q. REV. (Sept. 17 2017), https://www.bis.org/publ/qtrpdf/r_qt1709f.htm.

[58] *Id.*

[59] *Id.*

[60] Larry White, *The World's First Central Bank Electronic Money Has Come - And Gone: Ecuador, 2014-18*, ALT-M (Mar. 29, 2018), https://www.alt-m.org/2018/03/29/the-worlds-first-central-bank-electronic-money-has-come-and-gone-ecuador-2014-2018/.

[61] *Id.*

[62] Detrixhe, *supra* note 53.

[63] *Id.*

[64] *Id.*

Mobile money and third-party platforms such as Alipay work within existing financial and monetary systems, whereas DE more fundamentally affected Ecuador's financial system. Policies towards DE affected the monetary policy of Ecuador, involving the regulation of money supply in the entire economy, and not any sector-specific regulations.[65]

More directly relevant, storing funds within the Ecuadorian central bank created a different risk profile than that of M-Pesa and Alipay. In theory, risks from bankruptcy are removed entirely, or at least as far as the credit rating of the Ecuadorian central bank. However, customers' funds continue to be exposed to inflation, foreign exchange risk, and appropriation by the Ecuadorian state. The Ecuadorian government established the Monetary and Financial Council to regulate the supply and use of DE, though the exact legal arrangements used to protect funds are unclear.[66]

A number of factors appeared to impede the use of DE, leading to its withdrawal three years after its launch. Its voluntary nature meant there was no immediate incentive for anyone in the country to begin using the currency.[67] Consequently, DE needed to demonstrate its value to generate the network effects required for sustainable usage and growth of the currency. Several features impeded the perceived safety and ultimate usefulness of DE. One of these was the lack of credibility of government-backed financial products, given the number of times the government of Ecuador defaulted on its bonds since 2000.[68] Furthermore, DE accounts were not denominated in Ecuador's domestic-fiat currency. Instead, the BCE issued claims to U.S. dollars that it might not be able to repay.[69] Without the necessary uptake in usage, the cost of upkeep and maintenance of the currency also proved to be prohibitively expensive for the BCE, with the organization losing money every day of the currency's operation.[70]

The BCE also faced significant policy and supervisory limitations which reduced the credibility of DE.[71] This is due to the perceived lack of independence of the central bank from the Ecuadorian government, with appointments to the BCE being seen as completely political. There was no faith in the government bank because of its previous defaults on its liabilities, the most recent being in 2008, but with eight previous defaults, including defaults in 1982, 1984, and 2000.[72]

The Ecuador government's attempt to enter the mobile banking market exemplifies the challenges of a "one-size-fits-all" model to address the needs of individual countries.

Central Bank Digital Currencies

The relatively recent advent of international policy discussions around central bank currencies highlights the range of unresolved legal and regulatory issues. One of these is the desired relationship between the new currency and the central bank's monetary policy, and its relationship to bank deposits.

[65] *Id.*

[66] Carlo C, *Ecuador's National Digital Currency Experiment Explained*, COINTELEGRAPH (Oct. 23, 2014), https://cointelegraph.com/news/ecuadors-national-digital-currency-experiment-explained.

[67] Detrixhe, *supra* note 53.

[68] *Id.*

[69] *Id.*

[70] *Id.*

[71] *Id.*

[72] Naomi Mapstone, *Ecuador defaults on sovereign bonds*, FIN. TIMES (Dec. 12, 2008), https://www.ft.com/content/7170e224-c897-11dd-b86f-000077b07658.

For example, would the currency carry interest? Would the users be required to hold accounts with the central bank or could they remain anonymous? Would any restrictions be imposed on the size of the users' balance and transactions?[73] Should these be set at a higher or lower level than bank deposits? Digital currencies may be more likely to emerge in instances in which the banking system is more trusted than the central bank and government, and takes the lead on distributing such currencies.[74]

A second issue is the relationship between the digital currency and existing physical currency. Supply of currency normally is tightly regulated to maintain its value and prevent undue inflationary tendencies. If a digital currency were to be issued alongside physical currency, the ratio of each would need to be determined within the context of a country's monetary policy.[75] Any central bank would therefore need to determine if the digital currency will be inferior to the physical currency or will eventually replace all physical currency.

A third set of issues revolve around the exact nature of the currency itself. Because of its digital nature, it could either be treated as a cash-like physical currency, or some form of a deposit.[76] Each of these comes with its own benefits and costs but will ultimately mean that digital currencies may differ between countries and make cross-border transactions more difficult.

Other developing countries have not adopted central bank-backed digital currencies. The only exception is Uruguay, which launched a pilot project in 2017. The project was abandoned after six months and there is no publicly available information about the results of the project or the reasons that the currency did not grow as desired.[77]

However, digital currencies may become more prevalent in the future in response to developments in China, which has been researching the possibility of launching its own digital currency since 2014, but has accelerated its efforts in response to Facebook's proposed currency, Libra.[78] There is very little information about the proposed Chinese currency apart from the fact that it will be powered partially through blockchain and will be dispersed through digital wallets.[79] The currency is also designed in a manner that will allow the central bank to track the movement of the currency and supervise transactions.[80]

We have been looking at the protection of funds stored in specific services. Eventually, if these specific services take off, policymakers will need to work out whether and, if so, how to make them interoperable – namely payments from one type of service (e.g. M-Pesa) made to another (e.g. to a bank account or Ant Financial account). Other countries will eventually need to work out what path to take at that juncture.

[73] Todd Keister and Daniel Sanches, *Should Central Banks Issue Digital Currency? Working Paper 19-26*, FED. RES. BANK OF PHIL. 4 (June 2019), https://philadelphiafed.org/-/media/research-and-data/publications/working-papers/2019/wp19-26.pdf.

[74] *Id.*

[75] *Id.*

[76] *Id.*

[77] *Id.*

[78] Brenda Goh and Samuel Shen, *China's proposed digital currency more about policing than progress*, REUTERS (Nov. 1 2019), https://www.reuters.com/article/us-china-markets-digital-currency/chinas-proposed-digital-currency-more-about-policing-than-progress-idUSKBN1XB3QP.

[79] *Id.*

[80] *Id.*

For example, India's Unified Payments Interface (UPI), which is designed to facilitate interoperable payments and effectively connects different payments systems, has grown quickly since it was launched in 2016 by the National Payments Corporation of India, a non-profit that is owned by India's central bank, the Reserve Bank of India, and private commercial banks.[81] The Reserve Bank of India also regulates UPI. Transfers through UPI are instantaneous and costless. And unlike Alipay, for example, UPI's open architecture allows any regulated payment service provider to use it to transfer funds between individuals and/or businesses, and FinTechs and other companies can provide UPI services through regulated payment service providers.[82] UPI's open interface also allows users to more easily manage transactions across different accounts, institutions and systems using a single bank or payments application.[83]

A unique feature of UPI, and India's digital financial infrastructure more generally, is its utilization of unique biometric identification numbers, known as Aadhaar numbers; for example, users of UPI may transfer funds using their Aadhaar number (but may also make transfers using other identification numbers).[84] In order to receive an Aadhaar number, individuals must submit basic information (e.g., name, address), a face photograph as well as certain biometric information (e.g., fingerprints, iris scans). Thus, this biometric identification program allows for authentication through an Aadhaar app and helps facilitate electronic KYC, among other things.[85] A biometric identification program presents challenges, such as those regarding data privacy, however, and other countries may not be able or politically willing to launch one.

Libra

Libra is a proposed digital currency built using blockchain technology. The Libra Association, an association established by Facebook to oversee Libra, released its first white paper outlining the proposed Libra architecture and its uses in June 2019.[86] Under the first white paper, the Libra Association's proposed currency[87] would be backed by a basket of currencies and short-term government securities.[88] Unlike Bitcoin, for example, Libra coin would not be mined but just issued by the Libra Association and bought directly by consumers through Facebook's Calibra wallet platform or partner platforms. It could then be redeemed anywhere in the world online on any service that accepts Libra, as long as a person has

[81] Saritha Rai, Google, Walmart Help Drive India Payments Past 1 Billion Transactions, Bloomberg (Nov. 1, 2019), https://www.bloomberg.com/news/articles/2019-11-01/google-walmart-drive-india-payments-past-1-billion-transactions.

[82] Derryl D'Silva, Zuzana Filková, Frank Packer and Siddharth Tiwari, *The design of digital financial infrastructure: lessons from India*, BANK OF INTERNATIONAL SETTLEMENTS (Dec. 2019), https://www.bis.org/publ/bppdf/bispap106.htm.

[83] *Id.*

[84] *Id.*

[85] *Id.*

[86] Libra Association Members, White Paper, An Introduction to Libra, v1.0 (Jun. 2019). https://libra.org/en-US/wp-content/uploads/sites/23/2019/06/LibraWhitePaper_en_US.pdf

[87] Commentators opine that Libra is not a cryptocurrency or currency, but merely a medium of exchange. *See*, Examining Facebook's Proposed Cryptocurrency and Its Impact on Consumers, Investors, and the American Financial System, Hearing before the H. Comm. on Financial Services 116th Cong. (July 17, 2019) (testimony of Meltem Demirors, Chief Strategy Officer of CoinShares, a digital asset management firm), https://www.equities.com/news/libra-is-not-a-cryptocurrency.

[88] Libra Association Members, White Paper, An Introduction to Libra, v1.0 (Jun. 2019). https://libra.org/en-US/wp-content/uploads/sites/23/2019/06/LibraWhitePaper_en_US.pdf

a smartphone and an internet connection. The Libra Association's first white paper envisioned a new global currency that would be more stable and easier to exchange across the world.

The Libra Association's first white paper raised a number of important and contentious issues. First, all modern currencies are "fiat" currencies, in that they are valuable because of backing from their respective sovereign governments. If Libra became a global standard currency, its relationship with fiat currencies would become a significant issue, as it could reduce the current power of these currencies, and with it undermine the very idea of national sovereign governments.

Second, all national currencies are issued by their respective central banks and their money supply is tightly regulated, subject to national monetary and fiscal policies. These, in turn, are closely linked to domestic issues such as inflation. While the regulators in the central banks themselves are unelected, in theory they are generally answerable to the governments of the country which, in turn, are answerable to the people. A global currency issued and run by a non-government body backed by a company with the reach and power of Facebook raises questions about potential systemic financial risks that would otherwise be addressed by national governments.[89]

Third, the first Libra white paper argued that Libra would be far more stable than traditional currencies because it will be backed by a basket of financial instruments, including a basket of currencies, and U.S. treasury securities. However, these instruments and currencies themselves are subject to volatility and market shocks, which might affect the stability of Libra.[90] This, too, could pose significant systemic financial risks without sufficient regulatory oversight.

Finally, the Libra system could also potentially undermine the centrality of banks in the financial system, the vitality of which depends on banks meeting policy and regulatory requirements such as cash reserve ratios.[91] This, in turn, controls the flow of liquidity in the market. Libra exists independently of such requirements, lowering the cost of financial transactions through its network, and possibly marginalizing the role of banks, at least in relation to payment systems.[92] Libra could also cut out banks as intermediaries with the central banks, the financial system, and the larger population by making it convenient for people to transact on the Libra system, as opposed to the traditional banking channels.[93]

Facing significant regulatory pressure, the Libra Association released a second white paper in May 2020 that scales back on its vision for Libra and instead proposes a series of single-currency stablecoins in addition to a multi-currency Libra coin that is composed of fixed amounts of single-currency stablecoins.[94] Each of the Libra single-currency stablecoins will be fully backed by a reserve consisting of cash or cash equivalents and short-term government securities denominated in the relevant currency, and the multi-

[89] Rohan Grey, *Facebook Wants Its Own Currency. That Should Scare Us All.*, THE NATION (July 22, 2019), https://www.thenation.com/article/facebook-libra-currency-digital/.

[90] Ely, B., Facebook's Libra Will Be A Nonstarter, *The Hill*, (June 24, 2019), https://thehill.com/opinion/finance/450019-facebooks-libra-will-be-a-nonstarter.

[91] Panos Mourdoukoutas, *Why Big Governments and Central Banks Want to Kill Libra and Bitcoin*, Forbes (July 16, 2019), https://www.forbes.com/sites/panosmourdoukoutas/2019/07/16/why-big-governments-and-central-banks-want-to-kill-libra-and-bitcoin/#1f055db838d5.

[92] David Z. Morris, *Facebook's Libra Currency Could Threaten the Global Financial System. Here's How*, FORTUNE (July 18, 2019), https://fortune.com/2019/07/18/facebook-libra-cryptocurrency-washington-hearings-financial-system/.

[93] *Id.*

[94] Libra Association Members, White Paper, An Introduction to Libra, v2.0 (Apr. 2020). https://libra.org/en-US/wp-content/uploads/sites/23/2020/04/Libra_WhitePaperV2_April2020.pdf

currency Libra coin will be composed of single-currency stablecoins. This design change was intended to address concerns that the Libra system could interfere with monetary sovereignty and monetary policy if it grew large enough.

Conclusion

The proliferation of mobile phones in the developing world has spurred the development of a number of mobile-payment providers and is generating opportunities to provide payment services far beyond the traditional banking system.

The World Bank will be diligent in determining the type(s) of mobile payment system(s) which should be encouraged, the policy and other issues relevant to determining whether a payment system is likely to operate effectively, the main risks to users' funds and methods available to protect the user from these risks, and the policy issues which may arise when designing legal and regulatory strategies to address those risks.

The World Bank wishes to encourage and assist in bringing mobile payment systems that are as safe or safer than current cash-based payment systems to provide the unbanked or underbanked a vehicle to improved economic circumstances.

Appendices

New Payment Systems

1. Awrey, D. and K. van Zweiten, Mapping the Shadow Payment System, SWIFT Institute Working Paper No. 2019-001 (October 2019).
2. Awrey, D. and K. van Zweiten, The Shadow Payment System, Journal of Corporation Law (43), (2017).

Mobile Money

3. Alliance for Financial Inclusion (2010), Enabling Mobile Money Transfer: The Central Bank of Kenya's Treatment of M-Pesa.
4. Claudia McKay and Rafe Mazer, *10 Myths About M-Pesa:2014 Update,* CGAP (2014).
5. Evans, D. and A. Pirchio, An Examination of Why Mobile Money Schemes Ignite in Some Developing Countries But Flounder in Most, *Coase-Sandor Institute for Law and Economics* Working Paper No.723.
6. Jack, W., and T. Suri, 'The Economics of M-Pesa', *Massachusetts Institute of Technology, Working Paper*, August 2010.
7. Suri, T. and W. Jack, The Long Run Poverty and Gender Impacts of Mobile Money, *Science*, Vol. 354, December 2016.

Libra

8. Tiffany, K., Should You Care About Facebook's Cryptocurrency?, Vox, June 19, 2019, https://www.vox.com/the-goods/2019/6/19/18691549/facebook-cryptocurrency-libra-how-does-it-work
9. Statt, N., Facebook's Calibra Is A Secret Weapon For Monetizing Its New Currency, The Verge, June 18, 2019, https://www.theverge.com/2019/6/18/18682838/facebook-digital-wallet-calibra-libra-cryptocurrency-kevin-weil-david-marcus-interview.
10. Grey, R., Facebook Wants Its Own Currency. That Should Scare Us All., The Nation, July 22, 2019, https://www.thenation.com/article/facebook-libra-currency-digital/.
11. Taskinsoy J., Facebook's Project Libra: Will Libra Sputter Out or Spur Central Banks to Introduce Their Own Unique Cryptocurrency Projects?, (July 20, 2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3423453.
12. Grey, R. and J. Dharmapalan, The Case For Digital Legal Tender: The Macroeconomic Policy Implications of Digital Fiat Currency, eCurrency (2017).
13. Ely, B., Facebook's Libra Will Be A Nonstarter, The Hill, (June 24, 2019), https://thehill.com/opinion/finance/450019-facebooks-libra-will-be-a-nonstarter.

14. Morris, D.Z, Facebook's Libra Currency Could Threaten the Global Financial System. Here's How, Fortune (July 18, 2019), https://fortune.com/2019/07/18/facebook-libra-cryptocurrency-washington-hearings-financial-system/.
15. Mourdoukoutas, P., Why Big Governments and Central Banks Want to Kill Libra and Bitcoin, Forbes (July 16, 2019), https://www.forbes.com/sites/panosmourdoukoutas/2019/07/16/why-big-governments-and-central-banks-want-to-kill-libra-and-bitcoin/#1f055db838d5.

Central Digital Currencies

16. Bartonini C., and H. Holden, Digital Currencies: Proceeding With Caution- A Survey On Central Bank Digital Currency, *BIS Paper No. 101* (January 2019).
17. Keister, T. and D. Sanches, Should Central Banks Issue Digital Currency?, *Federal Reserve Bank of Philadelphia*, Working Paper 19-26 (June 2019).
18. Adrian, T. and T. Mancini-Griffoli, From Stablecoins to Central Bank Digital Currencies, *IMFBlog* (September, 2019), https://blogs.imf.org/2019/09/26/from-stablecoins-to-central-bank-digital-currencies/.
19. Ward, O. and S. Rochemont, Understanding Central Bank Digital Currencies, *Institute and Faculty of Actuaries* (March 2019).
20. Bergara, M. and J. Ponce (2018). Central bank digital currency: the Uruguayan e-peso
21. case. *Banco Central del Uruguay*.
22. White, L., The World's First Central Bank Electronic Money Has Come- And Gone: Ecuador, 2014-18, *Alt-M*, March 29, 2018, https://www.alt-m.org/2018/03/29/the-worlds-first-central-bank-electronic-money-has-come-and-gone-ecuador-2014-2018/.
23. Goh, B. and S. Shen, China's Proposed Digital Currency More About Policing Than Progress, *Reuters*, (November 1 2019), https://www.reuters.com/article/us-china-markets-digital-currency/chinas-proposed-digital-currency-more-about-policing-than-progress-idUSKBN1XB3QP.

Ant Financial

24. Kuo, L., 'Digital Wallet' of Ant Financial Captivates China and beyond, *The Guardian* (May 28, 2018), https://www.theguardian.com/technology/2018/may/28/digital-wallet-of-ant-financial-captivates-china-and-beyond.
25. Xie, S.Y and Deng, C., China to Tighten Rules on Five Financial Giants, *World Street Journal* (November 2, 2018), https://www.wsj.com/articles/china-to-tighten-rules-on-five-financial-giants-1541246489.
26. Concepion, A., How Ant Financial Became the Largest Fintech in the World, *Applico* (March 4, 2019), https://www.applicoinc.com/blog/ant-financial-services-platform-largest-fintech-in-world/.
27. Lu, L, How a Little Ant Challenges Giant Banks? The Rise of Ant Financial's Fintech Empire and Relevant Regulatory Concerns, *International Company and Commercial Law Review* (2018).

28. Weinland, D. and S. Fei Ju, China's Ant Financial Shows Cashless is King, *Financial Times*, (April 13, 2018), https://www.ft.com/content/5033b53a-3eff-11e8-b9f9-de94fa33a81e.
29. Detrixhe, J., China's Ant Financial, Thwarted In the US, is Expanding Rapidly in Europe, *Quartz*, (March 15, 2019), https://qz.com/1570052/ant-financials-alipay-is-expanding-rapidly-outside-of-china/.
30. Randallm D. and J. Chien, Fintech As A Pathway to Financial Inclusion? The Case of China, *FinDev Gateway*, April 2018, https://www.findevgateway.org/blog/2018/apr/fintech-pathway-financial-inclusion-case-china.
31. Aveni, Tyler; Roest, Joep. 2017. China's Alipay and WeChat Pay: Reaching Rural Users. *CGAP Brief*; World Bank, Washington, DC. © World Bank. https://openknowledge.worldbank.org/handle/10986/30112 License: CC BY 3.0 IGO.
32. Lee, J., China's Central Bank Says Will Gradually Set Up Rules To Regulate Fintech, *Reuters*, March 16, 2019, https://www.reuters.com/article/us-china-pboc-fintech/chinas-central-bank-says-will-gradually-set-up-rules-to-regulate-fintech-idUSKCN1QX05V.
33. Chen, T., The Cross-Border Payment War of WeChat Pay and Alipay, *WalkTheChat*, February 25, 2019, https://walkthechat.com/the-cross-border-payment-war-of-wechat-pay-and-alipay/.

India - UPI

34. D'Silva, D., Zuzana Filkova, Frank Packer and Siddharth Tiwari, The Design of Digital Financial Infrastructure: Lessons from India, *BIS Paper No. 106* (December 2019).
35. Rai, S., Google, Walmart Help Drive India Payments Past 1 Billion Transactions, *Bloomberg* (November 1, 2019).
36. Detrixhe, J., Cashless Payments Are Growing Faster in India than Just About Anywhere Else, *Quartz India* (November 12, 2019).
37. Fintech in India- Powering Mobile Payments, *KPMG* (August 2019).
38. The State of India's Digital Payments Progress- And Future, *PYMNTS* (July 1, 2019).
39. Jones, C., India's Payments Revolution, *Financial Times* (December 16, 2019)

HARVARD LAW SCHOOL | The Case Studies

CSP045
JUNE 2020

Digital Currencies

MARGARET E. TAHYAR, JAI MASSARI, KENDALL HOWELL, AND HOWELL E. JACKSON

Memorandum

DATE: February 2, 2020

TO: Deputy Director, Federal Reserve Bank Operations and Payment Systems

FROM: Director, Federal Reserve Bank Operations and Payment Systems

RE: Fed-Issued Digital Currency

Technology firms have sparked the digital transformation of payments, introducing innovative technology that may lower the cost of transactions, but also expose consumers to new risks. In an effort to ensure sovereign currencies remain at the center of each nation's financial system, an increasing number of central banks are engaged in some type of work relating to central bank digital currency (CBDC).[1] Indeed, as Chairman Powell recently testified, Facebook's Libra Project "lit a fire" under the Federal Reserve's consideration of this topic.[2] Accordingly, in light of the rapid transformation of payments, particularly with respect to the emergence of stablecoins—cryptocurrencies designed to minimize the volatility relative to the value of another financial asset—the Board of Governors of the Federal Reserve System requested that a team of staff economists brief the Board on potential designs for a Federal Reserve digital fiat currency. The economist teams have suggested two possible designs—"Fedcoin" and "Fedcount." There is an internal debate among the staff economists about which design might be better for payment efficiencies and monetary policy implementation, with some also expressing the view that no action should be taken by the Federal Reserve System at all.

[1] Codruta Boar, Henry Holden and Amber Wadsworth, *Impending Arrival – A Sequel To The Survey on Central Bank Digital Currency*, BANK FOR INT'L SETTLEMENTS (Jan. 2020, , at 3 (2020)Of the 66 central banks surveyed for the report, nearly 80% (up from 70%) are engaged in some work related to central bank digital currency, https://www.bis.org/publ/bppdf/bispap107.pdf.

[2] Daniel Roberts, *Fed Chair Jay Powell grilled on China's cryptocurrency plans, US response*, YAHOO FINANCE (Feb. 11, 2020), https://finance.yahoo.com/news/fed-chair-jay-powell-grilled-on-chinas-cryptocurrency-plans-us-response-211840877.html.

Written by Margaret E. Tahyar, Jai Massari, Kendall Howell, Davis Polk & Wardwell and Howell E. Jackson, James S. Reid, Jr., Professor of Law at Harvard Law School. Case development at Harvard Law School is partially funded by a grant from Dechert LLP. Cases are developed solely as the basis for class discussion. They are not intended to serve as endorsements, sources of primary data, legal advice, or illustrations of effective or ineffective management.

Copyright © 2020 President and Fellows of Harvard University. No part of this publication may be reproduced, stored in a retrieval system, used in a spreadsheet, or transmitted in any form or by any means—electronic, mechanical, photocopying, recording, or otherwise—without permission. To order copies or permissions to reproduce materials please visit our website at casestudies.law.harvard.edu or contact us by phone at 617-496-1316, by mail at Harvard Law School Case Studies Program, 1545 Massachusetts Avenue – Areeda 507, Cambridge, MA 02138, or by email at HLSCaseStudies@law.harvard.edu.

Both proposals are still in their early stages, as described further below. However, given the fact that some central banks around the world, most notably China, have begun experimentation, or are considering experimentation, with central bank digital currency, we have been asked to evaluate the three proposals: Fedcoin, Fedcount, and deferral of action until a later date. To that end, I would like your help with analyzing the potential legal and policy issues that could arise from the three proposals. Your task is to consider any design recommendations to guide the Federal Reserve Board forward, carefully weighed against the merits and demerits of maintaining the status quo. Another work stream is tasked with analyzing whether the Federal Reserve System possesses legal authority for implementing CBDC in the absence of new legislation, so for now assume that such authority exists. You should, however, consider any policy issues related to the institutional independence of the Federal Reserve System and the views that the Congressional oversight committee might have about decisions made by the Board of Governors with respect to CBDC and the role of the Federal Reserve System in the political economy. As Federal Reserve Governor Lael Brainard recently stated, "Given the dollar's important role, it is essential that we remain on the frontier of research and policy development regarding CBDC."[3]

Background

Functions of Money

Sound money must fulfill three classical functions: a medium of exchange, a store of value, and a unit of account.

First, in order for an instrument to function as a medium of exchange, the instrument must be able to facilitate the sale of goods and services. The seller in a transaction must accept the instrument as a means of payment with the belief that the seller can, in turn, give the instrument to another as a means of the seller's payment for other transactions.[4]

Second, the instrument must serve as a store of value, preserving purchasing power over time. An instrument that is susceptible to depreciation, or failure to maintain its value, would not be considered sound money.[5]

Third, functioning as a unit of account requires the instrument to act as a yardstick for measuring and comparing value across goods and services, thus informing the economic decisions of its users.[6]

The Role of the Central Bank in the U.S. System

The Federal Reserve System forms the central bank of the United States. The Federal Reserve System features "(1) a central governing Board, (2) a decentralized operating structure of 12 Federal

[3] Lael Brainard, Member, Bd. of Governors of the Fed. Res. Sys., remarks at the Symposium on the Future of Payments, Stanford Graduate School of Business, The Digitalization of Payments and Currency: Some Issues for Consideration (Feb. 5, 2020), https://www.federalreserve.gov/newsevents/speech/brainard20200205a.htm.

[4] Bk. for Int'l Settlements, *Annual Economic Report*, BANK FOR INT'L SETTLEMENTS (June 2018), at 92 https://www.bis.org/publ/arpdf/ar2018e.pdf.

[5] *Id.* at 91.

[6] *Id.*

Reserve Banks, and (3) a combination of public and private characteristics"[7] (for more information about the Federal Reserve System, see Appendix Item 3). The Board of Governors of the Federal Reserve System is based in the nation's capital and supervises the 12 Federal Reserve Banks. The 12 Federal Reserve Banks "service financial institutions in 12 Federal Reserve districts."[8] Federal Reserve notes, commonly called cash, are issued by the separate regional Federal Reserve Banks, but printed by the U.S. Treasury. The 12 Federal Reserve Banks also "act as banker's banks, providing a wide variety of services such as storing currency and processing checks and electronic payments for both banking institutions and the federal government."[9] Directly accessing these payment services "requires a master account at the nearest regional Federal Reserve Bank."[10] The Federal Reserve Banks only grant master accounts to banks.

The Federal Reserve System performs a number of critical roles for the U.S. economy. First, the Federal Reserve Board is charged by Congress to "pursu[e] the goals of 'maximum employment, stable prices, and moderate long-term interest rates.'"[11] Second, "[t]he Federal Reserve is the primary organ responsible for carrying out U.S. monetary policy and, for many, that is its most crucial role."[12] Third, the Federal Reserve's circulation of cash, issued and delivered by the regional Federal Reserve Banks, to meet domestic and foreign demand also generates significant revenues for the U.S. government thanks to the U.S. dollar's status as the global reserve currency.

Conventional Forms of Money in the U.S. Financial System

In the current U.S. financial system, money conventionally manifests in three forms: cash, commercial bank deposits, and central bank accounts, that is accounts held by banks at each of the Federal Reserve Banks through what is called a master account. As described below, the relationship between these three kinds of money is overseen by the Federal Reserve System.

[7] About the Federal Reserve System, Structure of the Federal Reserve System, https://www.federalreserve.gov/aboutthefed/structure-federal-reserve-system.htm.

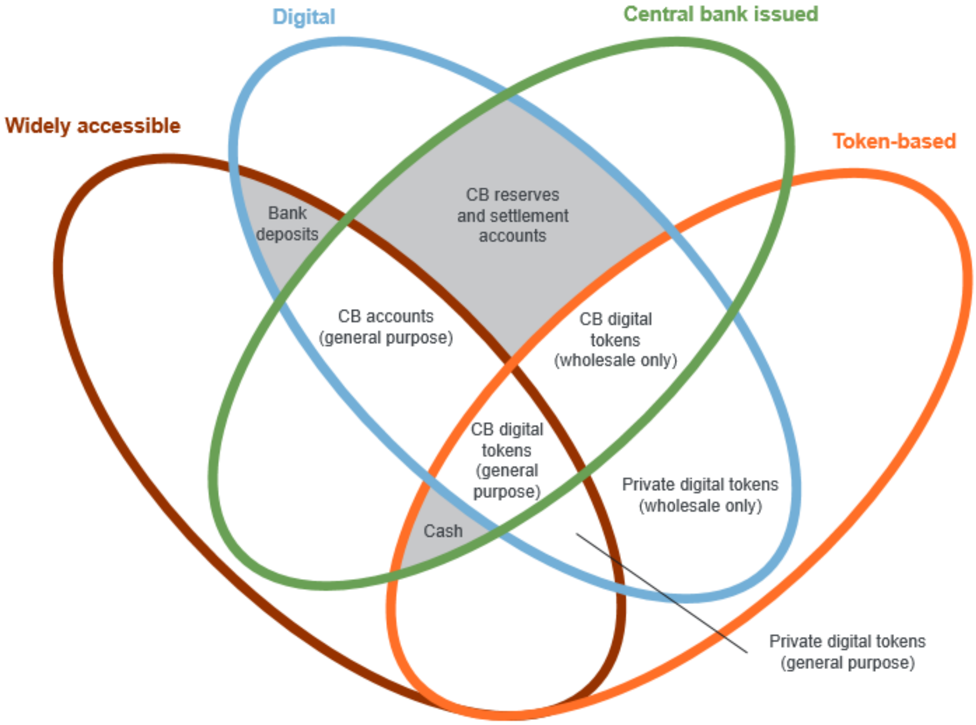
[8] Michael S. Barr, Howell E. Jackson and Margaret E. Tahyar, Financial Regulation: Law and Policy 939 (2d ed. 2018).

[9] *Id.*

[10] *Id.* at 183.

[11] *Id.* at 49.

[12] *Id.* at 939.


Digital
Central bank issued
Widely accessible
Token-based
Bank deposits
CB reserves and settlement accounts
CB accounts (general purpose)
CB digital tokens (wholesale only)
CB digital tokens (general purpose)
Cash
Private digital tokens (wholesale only)
Private digital tokens (general purpose)

Source: Adapted from Bank for International Settlements[13]

Cash consists of both metal coins minted by and paper notes printed by the government. Cash represents a liability of the central bank[14] and is "legal tender for all debts, public charges, taxes, and dues."[15] The Federal Reserve Banks issue and supply cash to commercial banks in their districts, which is then circulated by commercial banks to users based on demand. Generally, anyone can access, store, and use cash. Due to its widely recognized authenticating features (for example, watermarks and holograms on higher value bills), payments involving cash typically do not require a trusted third party to record the transfer or verify the authenticity of the physical notes or coins.[16] Consequently, settling transactions with cash is usually immediate and generally does not come with transaction fees.[17]

Cash also comes with costs attached for both the user, who bears the burden of storage and loss, and the government, which bears the burden of supporting the printing, minting, and initial delivery infrastructure. Although cash is convenient for settling smaller transactions immediately, it is inconvenient for large transactions. Holding and transferring large quantities of cash is both burdensome and unsafe. For these reasons, the proportion of cash in payment values has been declining in many major economies, including in the United States.[18]

[13] Comm. on Paymts. & Mkt. Infrastructures, Markets Comm., *Central bank digital currencies*, BANK FOR INT'L SETTLEMENTS (2018), at 5, https://www.bis.org/cpmi/publ/d174.pdf.

[14] Walter Engert and Ben S.C. Fung, *Central Bank Digital Currency: Motivations and Implications*, BANK OF CAN. (2017), at 1, https://www.bankofcanada.ca/wp-content/uploads/2017/11/sdp2017-16.pdf.

[15] 31 U.S.C. § 5103.

[16] *Id.* at 1.

[17] BARR, *supra* note 8, at 808.

[18] *Id.*

From the government's perspective, cash requires an expensive infrastructure to support its circulation and upkeep.[19] In addition to the logistics of producing, storing, and transporting physical cash to accommodate new demand, the government has to periodically retire and replace unfit coins and notes to maintain existing supply, further consuming resources.[20] Even with these expenses, however, the government's creation of cash generates significant profits for the United States government, due in part to the U.S. dollar's role as a reserve currency, the widespread use of $100 bills as a safe haven asset, or as the currency most valued in illicit transactions.

Money in bank deposit accounts consists of "electronically recorded deposit account liabilities on the ledgers of commercial banks."[21] This form of money is universally available to anyone with a bank account.[22] Money stored in deposit accounts serves as "the main means of payment between ultimate users"[23] and "the main form of money holding of households and businesses."[24] Its supply increases when commercial banks issue loans to borrowers or receive cash deposits and decreases when account holders "make debt repayments or interest payments to the bank."[25] Money in bank deposit accounts, which is a private form of money (i.e., money that is a claim against private banks, rather than the central bank), is the predominant form of money in the U.S. financial system.

Money in central bank accounts is recorded digitally as liabilities on each Federal Reserve Bank's ledger.[26] As discussed earlier, direct access to central bank money is currently restricted to chartered banks and other depository institutions. Nonbank companies and individuals cannot directly access the accounts at a Federal Reserve Bank for payments or storage.[27] Supply of central bank money grows when commercial banks purchase government bonds or deposit funds with their Federal Reserve Banks and contracts when commercial banks borrow on a collateralized basis from their Federal Reserve Banks.[28] Instead of facilitating retail payments, the amounts deposited by commercial banks with the Federal Reserve Banks enable the settlement of wholesale interbank payments.[29]

Taken together, these three conventional forms of money share overlapping features while retaining key distinctions. For instance:

[19] Aleksander Berentsen and Fabian Schär, *The Case for Central Bank Electronic Money and the Non-case for Central Bank Cryptocurrencies*, 100 FED. RES. BK. OF ST. LOUIS REV. 97, 101 (2018), https://doi.org/10.20955/r.2018.97-106; https://research.stlouisfed.org/publications/review/2018/02/13/the-case-for-central-bank-electronic-money-and-the-non-case-for-central-bank-cryptocurrencies.

[20] For reference, there is an average life expectancy of 5.9 years for $1 bills, 4.2 years for $10, 3.7 years for $50, and 15 years for $100. *How Currency Gets into Circulation*, FED. RES. BK. OF N.Y. (July 2013), https://www.newyorkfed.org/aboutthefed/fedpoint/fed01.html.

[21] Ole Bjerg, *Designing New Money–The Policy Trilemma of Central Bank Digital Currency, Working Paper*, COPENHAGEN BUS. SCH. (June 14, 2017), at 15, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2985381.

[22] *Id.* at 14–15. As a practical matter, however, "[m]ore than 9 million U.S. households, including 15.6 million adults and 16.3 million children are unbanked, or lack an account at an insured depository institution." BARR, *supra* note 8, at 826. There are "[a]nother 24.5 million households, comprising 51.1 million adults and 16.3 million children [who] are underbanked, meaning that although they have bank accounts, they also obtain financial services from non-bank, alternative-financial-services providers such as check cashers or payday lenders. Being unbanked or underbanked presents significant challenges for participating in many payment systems." *Id.*

[23] Bk. for Int'l Settlements, *supra* note 4, at 93.

[24] Bjerg, *supra* note 21, at 12.

[25] *Id.* at 15.

[26] *See Id.* at 14.

[27] If the Fintech Charters were granted master accounts, then access would be extended beyond depository institutions. *See* Howell E. Jackson, Margaret Tahyar and Carol Rodriguez, *Fintech Charter Case Study*, HARVARD L. SCH. (Feb. 2020), at 6–7.

[28] *See* Bjerg, *supra* note 21, at 15.

[29] Bk. for Int'l Settlements, *supra* note 4, at 93.

- Cash and commercial bank deposits are, in principle, accessible to anyone, unlike master accounts,[30] which can only be opened by banks.
- Cash and master accounts are liabilities issued by the Federal Reserve Banks, unlike commercial bank deposits.[31]
- Commercial bank deposits and master accounts exist in digital form, unlike cash.[32]

Beyond these abstract comparisons, the three forms of money share an operational infrastructure through the Federal Reserve System's partnership with the banking sector in circulating cash to the public.[33] Specifically, individuals can receive cash by converting digital money stored in their bank deposits into paper notes, most typically by a withdrawal from an ATM machine. These paper notes are purchased by the bank from its regional Federal Reserve Bank through a deduction from the amount held in the bank's master account and a corresponding delivery of physical notes.[34]

[30] Bjerg, *supra* note 21, at 15–16.

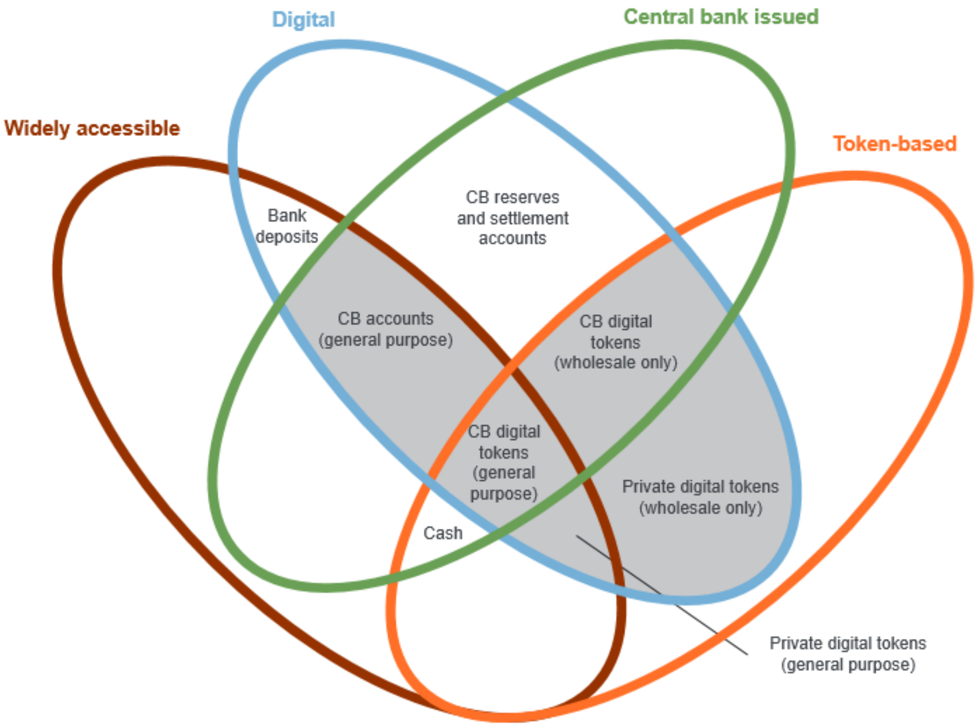
[31] *Id.*

[32] *Id.*

[33] Bk. for Int'l Settlements, supra note 4, at 93 ("[I]n almost all modern-day economies, money is provided through a joint public-private venture between the central bank and private banks, with the central bank at the system's core." This institutional arrangement is not confined to the Federal Reserve System).

[34] J.P. Koning, *Fedcoin: A Central Bank-issued Cryptocurrency*, R3 RESEARCH, (2016), 1t 25, https://www.r3.com/wp-content/uploads/2018/04/Fedcoin_Central_Bank_R3.pdf.

New Forms of Money?


Digital
Central bank issued
Widely accessible
Token-based
Bank deposits
CB reserves and settlement accounts
CB accounts (general purpose)
CB digital tokens (wholesale only)
CB digital tokens (general purpose)
Private digital tokens (wholesale only)
Cash
Private digital tokens (general purpose)

Source: Adapted from Bank for International Settlements[35]

Cryptocurrency

Cryptocurrencies, such as Bitcoin, Ethereum, and Ripple, are a type of digital currency that rely on cryptography to verify and secure transactions, as well as to manage the creation of new units.[36] In contrast to conventional forms of money, and in contrast to other digital currencies (for example, in-game currencies used by certain video game franchises), cryptocurrencies generally are not backed by a trusted institution and typically are not liabilities of any person or institution.[37]

Distributed ledger technology, of which blockchain technology forms a subset, represents the technological engine underpinning many cryptocurrencies, including Bitcoin. Distributed ledger technology "refers to the protocols and supporting infrastructure that allow computers in different locations to propose and validate transactions and update records in a synchronized way across a network."[38] As the term *ledger* implies, distributed ledger technology provides a means of recording account balances or transaction history. In most other contexts, electronic transactions are recorded on a *centralized* ledger. Generally, a trusted intermediary (*e.g.*, the central bank, commercial banks, or

[35] Comm. on Paymts. & Mkt. Infrastructures, *supra* note 13, at 5.

[36] BARR, *supra* note 8, at 835. For information on Bitcoin in particular, *see* Reuben Grinberg, *Bitcoin: An Innovative Alternative Digital Currency*, 4 HASTINGS SCI. & TECH. L.J. 159, 160 (2011).

[37] Lael Brainard, Member, Bd. of Governors of the Fed. Res. Sys., Cryptocurrencies, Digital Currencies, and Distributed Ledger Technologies: What Are We Learning? Speech at the Decoding Digital Currency Conference sponsored by the Federal Reserve Bank of San Francisco (May 15, 2018), https://www.federalreserve.gov/newsevents/speech/brainard20180515a.htm.

[38] Morten Linnemann Bech and Rodney Garratt, *Central Bank Cryptocurrencies*, BK. FOR INT'L SETTLEMENTS Q. REV. (Sept. 2017), at 55, 58, https://www.bis.org/publ/qtrpdf/r_qt1709f.pdf.

PayPal) manages the central ledger to "track account holders' balances and, ultimately, vouch for a transaction's authenticity."[39] However, this is not so with distributed ledger technology. As the name implies, the ledger is *distributed* across computers and other internet-connected devices in separate locations globally, all without the need for a trusted central authority.[40]

For Bitcoin and many other cryptocurrencies, "[t]his ledger is the blockchain."[41] Transactions are recorded in batches, or "blocks," with new blocks being "chained" in order to amend the existing ledger with additional transactions.[42] This process of clearing and settlement happens around the clock—24/7/365—and it all occurs automatically, with minimal human intervention. Parties wishing to transact with blockchain technology must announce their transaction "to the entire network, effectively asking network participants to determine its authenticity."[43] Responsibility for verifying the validity of new blocks is shared by nodes—or computers connected to the network—through a consensus mechanism, whereby the nodes agree to the common state of ledger usually with cryptographic tools and protocol rules.[44] For Bitcoin's proof-of-work consensus mechanism, network participants compete to solve cryptographic puzzles necessary for validating a new block. As an economic incentive, the first to succeed receives newly issued units of bitcoin.[45]

A critical distinction to keep in mind is that Bitcoin is an example of a *permissionless* system, where each node possesses a complete and current copy of the ledger. In principle, anyone can participate in validating transactions in a permissionless system. In contrast, a *permissioned* system only allows trusted nodes—in other words, participants approved by a central entity—to participate in updating the ledger. A permissioned system may involve additional access controls, such as verification of identity.[46]

Many harbor doubts as to whether permissionless cryptocurrencies can function as sound money, much less supplant the use of cash. For instance, Professor David Yermack argued in 2013 that Bitcoin, which remains the most popular cryptocurrency, failed to satisfy the classical criteria of money. Although Bitcoin enjoys some acceptance as a form of payment, "the worldwide commercial use of bitcoin remains miniscule…"[47] He maintained that Bitcoin performs poorly as a unit of account since Bitcoin-based quotes for prices of ordinary goods commonly extend to "four or five decimal places with leading zeros, a practice rarely seen in consumer marketing and likely to confuse both sellers and buyers in the marketplace."[48]

[39] Trevor I. Kiviat, *Beyond Bitcoin: Issues in Regulating Blockchain Transactions*, 65 DUKE L.J. 569, 578 (2015); Bk. For Int'l Settlements, *supra* note 4, at 96.

[40] As such, this system is a "trustless" system.

[41] *Id.*; *see also* Satoshi Nakomoto, *Bitcoin: A Peer-To-Peer Electronic Cash System*, BITCOIN (2009) at 3, https://bitcoin.org/bitcoin.pdf.

[42] Comm. on Paymts. and Mkt. Infra., *Distributed Ledger Technology in Payment, Clearing and Settlement*, BK. FOR INT'L SETTLEMENTS (2017), at 3, https://www.bis.org/cpmi/publ/d157.pdf.

[43] Kiviat, *Beyond Bitcoin*, *supra* note 39, at 578.

[44] Comm. on Paymts. and Mkt. Infra., *supra* note 42, at 3–4.

[45] *Id.* at 4. Bitcoin is programmed to have a finite total outstanding supply. When Bitcoin creation ceases, "the incentive to validate transactions will likely be transaction fees." Kiviat, *Beyond Bitcoin*, *supra* note 39, at 579–580.

[46] Bk. For Int'l Settlements, *supra* note 4, at 96.

[47] David Yermack, *Is Bitcoin a Real Currency? An Economic Appraisal, Working Paper No. 19747*, NAT'L BUR. OF ECON. RES., (rev. Apr. 2014) at 2, https://www.nber.org/papers/w19747.

[48] *Id.* at 2–3. There have been proposals to introduce a millibitcoin (mBTC), then worth $1.85, to better account for pricing of conventional goods, Kai Sedgwick, *It's Time to Change the Way We Measure Bitcoin*, BITCOIN.COM (Dec. 8, 2017), https://news.bitcoin.com/its-time-to-change-the-way-we-measure-bitcoin/.

Even then, his most severe reservation resided with Bitcoin's prospects as a store of value given, among other factors, its high volatility.[49]

Since 2013, use of Bitcoin and other cryptocurrencies as a medium of exchange has increased, especially for those either without access to or wishing to bypass central banks and commercial banks. Yet, adoption remains far from widespread.[50]

Stablecoins

Persisting volatility continues to bely cryptocurrency's function as a stable means for storing value. To many observers, cryptocurrency's extreme fluctuations and growing number of entrants harken ominously back to the era of wildcat banking, when state banks circulated their own currency that too often had dubious worth (see Appendix Item 11).[51] Recently, stablecoins have emerged as an increasingly popular alternative to traditional cryptocurrencies. Stablecoins are digital assets that share the same technical features and infrastructure as traditional cryptocurrencies. However, a critical distinction between stablecoins and traditional cryptocurrencies is that a stablecoin's price is not determined by an open market. Instead, a stablecoin's price is stabilized by linking its value to a reference asset, or pool of assets, such as fiat currency, an exchange traded fund, or other cryptocurrencies. Given the potential increase in value stability, stablecoins may be more usable as a reliable means of storing value than traditional cryptocurrencies.

There are three common methods of stabilizing a stablecoin's value relative to another asset. First, under the depository receipt model, the stablecoin is a direct claim on a single currency.[52] The stablecoin issuer must guarantee the value of the stablecoin by collateralizing all claims and committing to redeem the stablecoins at par value in the currency in which the claims were issued. The Monetary Authority of Singapore successfully implemented a blockchain-based inter-bank payment system using a version of the depository receipt model.[53]

A second, alternative method of reducing stablecoin volatility is to peg a stablecoin's value to a "basket" of assets, commonly referred to as a currency basket. The currency basket can reference a pool of fiat currencies, highly-liquid government securities, cryptocurrencies, or some combination thereof. Notably, the assets in the currency basket are notional, and thus only provide a reference to determine a stablecoin's value. In other words, the holder of a stablecoin backed by a currency basket has no claim on the notional assets within the currency basket. Facebook announced in 2019 that it was participating in the launch of a stablecoin through the Libra Association. The Libra Association's second white paper, released in 2020, proposes a series of single-currency stablecoins as well as a multi-currency stablecoin,

[49] As discussed in footnote 42, Bitcoin's supply is ultimately fixed. Although in theory the consensus mechanism could vote to lift this limit, doing so would be difficult in practice. This effective limit on supply presents a further challenge to Bitcoin's viability as a form of money.

[50] Christian Barontini and Henry Holden, *Proceeding with Caution – A Survey on Central Bank Digital Currency*, BANK FOR INT'L SETTLEMENTS (Jan. 2019), at 14, https://www.bis.org/publ/bppdf/bispap101.pdf.

[51] Robert C. Hockett, *Money's Past Is Fintech's Future: Wildcat Crypto, the Digital Dollar, and Citizen Central Banking* 2 Stanford J. of Blockchain L. & Pol. ___ (June 28, 2019), https://stanford-jblp.pubpub.org/pub/wildcat-crypto-fintech-future, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3299555.

[52] Barontini, *supra* note 50.

[53] Hockett, *supra* note 51.

the Libra Coin, each of which will be fully backed by deposits and short-term government securities held by a network of custodians.[54]

Third and finally, and relevant to the questions at hand, central banks can issue stablecoins in addition to bank notes and overnight deposits. Stablecoins, in this case, would be a central bank liability, similar to traditional cash, and held on the balance sheets of central banks. The Eastern Caribbean Central Bank (ECCB) partnered with Bitt Inc. to initiate a blockchain-based CBDC pilot wherein the ECCB would issue a securely minted, digital Eastern Caribbean (EC) dollar.[55] The EC *digital* dollar will stand 1:1 with the EC *fiat currency* dollar.[56]

Despite the growing utility of stablecoins, the integration of stablecoins within cross-border payment systems has been relatively limited. Private companies such as Facebook are designing payment systems that utilize a stablecoin design.[57] Regulatory reactions to the initial proposal have led to changes.[58] Nevertheless, government regulators are increasingly aware of the advantages of stablecoins and are looking to leverage the design methods discussed above as they explore the feasibility of CBDC. The Group of Seven (G7) stated that "[t]hese stablecoins might be more readily usable as a means of payment and store of value, and they could potentially foster the development of global payment arrangements that are faster, cheaper and more inclusive than present arrangements."[59]

Central Bank Digital Currency

The advent of permissionless cryptocurrencies has catalyzed interest among academics and policymakers in CBDC. In a survey conducted by the Bank for International Settlements (see Appendix Item 7), 70% of the responding central bank participants reported current or imminent engagement with CBDC work.[60] A number of central banks are researching CBDC, including the Bank of England, which released a paper in 2020 that addresses the opportunities and challenges presented by CBDC and sets forth CBDC design principles in order to engage discussion about whether to introduce CBDC in the United Kingdom.[61] In addition, a few central banks have announced plans to implement CBDC in the next decade, most notably China.[62] In 2014, the People's Bank of China (PBOC)—China's central bank—mentioned the possibility of researching the issuance of a digital currency by the PBOC,[63] and has since confirmed its intent to issue a digital currency: the Digital Currency/Electronic Payments (DC/EP). Recently, the PBOC

[54] Libra, *Libra White Paper*, LIBRA , https://libra.org/en-US/white-paper/.

[55] Eastern Caribbean Central Bank, *ECCB to Issue World's First Blockchain-based Digital Currency*, E CARRIB. CEN. BK. (Mar. 9, 2019), https://www.eccb-centralbank.org/news/view/eccb-to-issue-worldas-first-blockchain-based-digital-currency.

[56] *Id.*

[57] Libra, Libra White Paper, LIBRA, https://libra.org/en-US/white-paper/.

[58] *See, e.g.*, Richard Partington, *France to block Facebook's Libra cryptocurrency in Europe*, THE GUARDIAN (Sept. 12, 2019), https://www.theguardian.com/technology/2019/sep/12/france-block-development-facebook-libra-cryptocurrency.

[59] G7 Working Group on Stablecoins, *Investigating the impact of global stablecoins*, BK. FOR INT'L SETTLEMENTS (Oct. 2019), https://www.bis.org/cpmi/publ/d187.pdf.

[60] Barontini, *supra* note 50, at 7.

[61] *Id.* at 12; Bank of England, *Central Bank Digital Currency: Opportunities, challenges, and design* (Mar. 2020), https://www.bankofengland.co.uk/-/media/boe/files/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design.pdf?la=en&hash=DFAD18646A77C00772AF1C5B18E63E71F68E4593.

[62] Barontini, *supra* note 50, at 7.

[63] Mu Changchun, Dep. Dir. of the Paymt and Settlement Dept. of the People's Bk. of China, Design and Architecture of Central Bank's Digital Currency, Keynote speech at the CF40 Yichun Forum (Aug. 10, 2019), http://www.cf40.org.cn/uploads/newsletter/20190803.pdf.

accelerated its efforts to establish the DC/EP, confirming that at least seven financial institutions would receive and transact in the currency when it launches.[64] The DC/EP currency would be compatible with China's existing financial infrastructure and service systems, and China aims to provide DC/EP to the world as a cross-border payment system linked to the RMB.[65]

Despite the growing body of literature, CBDC currently is "not a well-defined term"[66] and standardization has yet to be reached in the form of an agreed taxonomy or lexicon. Because discussions about CBDC have mostly been conceptual, it might be most helpful to define CBDC by way of contrast: CBDC is central bank-issued digital money that is distinct from the existing master accounts at Federal Reserve Banks.[67]

	Conventional forms of money			**New forms of money**	
	Cash	Bank deposits	Master account balances	Privately issued cryptocurrency or stable coins	Central bank digital currency
Digital	×	✓	✓	✓	✓
Central bank-issued	✓	×	✓	×	✓
Universally accessible	✓	✓	×	✓	(✓)
✓ = existing or likely feature, (✓) = possible feature, × = not typical or possible feature					

Source: Adapted from Bank for International Settlements[68]

CBDC is also distinct from privately issued cryptocurrencies: CBDC would be backed by the government in the same way that current forms of fiat currency are backed and may assuage concerns of volatility because supply could be set programmatically (or algorithmically).[69] Some commentators regard a hypothetical CBDC as superior to permissionless cryptocurrencies in two respects. First, CBDC based on stablecoin design principles would be a more reliable and stable store of value.[70] Second, CBDC would likely avoid the "significant waste of resources" required by the consensus mechanisms used by some

[64] Michael del Castillo, *Alibaba, Tencent, Five Others To Receive First Chinese Government Cryptocurrency*, FORBES (Aug. 27, 2019), https://www.forbes.com/sites/michaeldelcastillo/2019/08/27/alibaba-tencent-five-others-to-recieve-first-chinese-government-cryptocurrency/#10624b5a1a51.

[65] Mu, *supra* note 62.

[66] Comm. on Paymts. & Mkt. Infrastructures, *supra* note 13, at 3.

[67] *Id.* at 4.

[68] *Id.* at 6.

[69] Brainard, *supra* note 37.

[70] *Id.*

cryptocurrencies.[71] For these reasons, a few commentators advocate CBDC as a solution for counteracting the migration of users from conventional forms of money to cryptocurrencies.[72]

In recent years, China has taken measures to discourage Bitcoin transactions, specifically banning bank and payment institutions from dealings in Bitcoin in 2013 and, more recently, illegalizing ICOs raising cryptocurrencies such as Bitcoin.[73] Given the tepid acceptance of cryptocurrencies in mainstream payment ecosystems, central banks may turn to CBDC as an alternative method of integrating digital currencies within the monetary system. In a survey released by the Bank for International Settlements, "central banks are undertaking extensive work on [CBDC]. Globally, emerging market economics are moving from conceptual research to intensive practical development, driven by stronger motivations than those of advanced economy central banks. Central banks representing a fifth of the world's population say they are likely to issue the first CBDCs in the next few years."[74] Our own central bank has expressed an interest in analyzing the benefits of CBDC, stating in October 2019 that "at the Federal Reserve, we will continue to analyze the potential benefits and costs of central bank digital currencies and look forward to learning from other central banks."[75] (see Appendix Item 2). That said, Treasury Secretary Mnuchin tempered expectations, stating in December 2019 that he and Federal Reserve Chairman Jerome Powell "see no need for the Fed to issue a digital currency."[76]

Design Choices for Central Bank Digital Currency

Whether to introduce a CBDC and its optimal design features depend on the objectives and motivations of the central bank.[77] Designing a CBDC would need to take into consideration the following features, among others.

Currencies can either be token-based or account-based. If token-based, careful thought should be given to the appropriate degree of anonymity. As with all currencies, CBDC would also require an infrastructure to support its distribution (centralized or decentralized). As a *digital* currency, CBDC must also have in place a validation scheme (centralized or decentralized) to prevent double spending or identity theft. Finally, digital currencies can be subject to caps and/or accrue interest.

[71] Dong He, Karl Habermeier, Ross Leckow, Vikram Haksar, Yasmin Akmeida, Mikari Kashima, Nadim Kyriakos-Saad, Hiroko Oura, Tahsin Saadi Sedik, Natalia Stetenko and Concepcion Verdugo-Yepes, *Virtual Currencies and Beyond: Initial Considerations*, INT'L MON. FUND 20 (Jan. 2016), https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf, ("Mining Bitcoin is costly, requiring computer processing power and associated energy costs. In addition, such systems involve a negative externality that causes overinvestment in computer power.").

[72] Hockett, *supra* note 51. *See also* Itai Agur, *Central Bank Digital Currencies: An Overview of Pros and Cons*, *in* DO WE NEED CENTRAL BANK DIGITAL CURRENCY? 113, 115 (2018) ("[O]ne incentive that central banks may have to develop a retail CBDC is to limit demand for private cryptocurrencies.").

[73] Library of Congress, *Regulation of Cryptocurrency in China*, (July 12, 2018), https://www.loc.gov/law/help/cryptocurrency/china.php#_ftn4.

[74] Codruta Boar, Henry Holden and Amber Wadsworth, *Impending Arrival – A Sequel To The Survey on Central Bank Digital Currency*, BK. FOR INT'L SETTLEMENTS (Jan. 2020, at 3 (2020), https://www.bis.org/publ/bppdf/bispap107.pdf.

[75] Lael Brainard, Member, Bd. of Governors of the Fed. Reserve Sys., Digital Currencies, Stablecoins, and the Evolving Payments Landscape (Oct. 16, 2019), speech At The Future of Money in the Digital Age, sponsored by the Peterson Institute for International Economics and Princeton University's Bendheim Center for Finance, Washington, D.C., https://www.federalreserve.gov/newsevents/speech/brainard20191016a.htm.

[76] Saleha Mohsin, *Mnuchin, Powell See No Need for Fed to Issue Digital FX*, BLOOMBERG (Dec. 5, 2019), https://www.bloomberg.com/news/articles/2019-12-05/mnuchin-powell-see-no-need-for-fed-to-issue-digital-currency.

[77] While the Bank of Canada has undertaken research and experimentation with CBDCs for interbank settlement (wholesale CBDC), ourinterests concern retail payments. To that end, please focus on the features that may be conducive towards a retail or general-purpose CBDC, which may differ from those for a wholesale CBDC.

	Conventional forms of money			New forms of money		
	Cash	Bank deposits	Master account balances	Privately issued cryptocurrency	Token-based CBDC	Account-based CBDC
Tokens or accounts	T	A	A	T	T	A
Anonymity	✓	×	×	✓	(✓)	×
Decentralized distribution	✓	✓	×	✓	(✓)	×
Decentralized validation	✓	✓	×	✓	(✓)	(✓)
Capped	×	×	×	×	(✓)	(✓)
Interest-bearing	×	✓	✓	(✓)	(✓)	(✓)
✓ = existing or likely feature, (✓) = possible feature, × = not typical or possible feature						

Source: Adapted from Bank for International Settlements[78]

Technology: Tokens or Accounts

The technological vehicle for the CBDC could be token-based, involving the transfer of an object of value from one wallet into another, or account-based, involving the transfer of a claim recorded on one account to another.[79] Cash and Bitcoin are examples of token-based money, whereas bank accounts and master accounts are examples of account-based money. One distinction between tokens and accounts turns on the method for verifying an exchange: the focus of verification for token-based money is the object transferred—i.e., the token—and the focus of verification for account-based money is the identities of the account holders.[80]

Transfers involving tokens depend on the payee's ability to "verify the validity of the payment object,"[81] whether in the form of a metal or digital coin. Token-based systems must control for counterfeiting and enable the payee to validate the authenticity of the received token.[82] This implication holds true for both physical and digital coins, as the payer could use a fake token in a transaction. Digital currencies introduce the additional problem of double spending, where the payer uses a *real* digital token for more than one transaction. Thus, policymakers for token-based systems must grapple with designing validation channels (*e.g.*, via a recognizable design as with paper notes or via a decentralized consensus mechanism as with Bitcoin) for limiting counterfeit tokens and duplicate tokens. In contrast, transfers

[78] Comm. on Paymts. & Mkt. Infrastructures, *supra* note 13, at 6.

[79] Tommaso Mancini-Griffoli, Maria Soledad Martinez Peria, Itai Agur, Anil Ari, John Kiff, Adina Popescu and Celine Rochon, *Casting Light on Central Bank Digital Currency*, INT'L MON. FUND, (Nov. 2018), https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2018/11/13/Casting-Light-on-Central-Bank-Digital-Currencies-46233.

[80] Comm. on Paymts. & Mkt. Infrastructures, *supra* note 13, at 4.

[81] *Id.*

[82] *Id.*

involving accounts rely on verifying "the identity of the account holder."[83] Account-based systems must control identity theft and the unauthorized transfer or withdrawal of money held within valid accounts.[84] Consequently, policymakers for account-based systems must seek ways to validate the identity of the transacting parties.[85]

Anonymity

As seen with Bitcoin and metal coins of old, token-based systems rely on verifying the authenticity of the exchanged token, not the identities of the transacting parties. The payer "need reveal nothing to the payee beyond the information associated with the specific coin."[86] As such, a token-based CBDC can "be designed to provide different degrees of anonymity"[87] for its users or traceability for its transactions.[88]

That said, Bitcoin and Ethereum would be more accurately characterized as granting pseudo-anonymity. While "[t]he blockchain does not record real names or physical addresses," the transactions of the ledger are public and would be traceable to the owner should "the owner of the wallet become known."[89] A paper trail may be harder to follow than a digital one.[90] Cash transactions are usually anonymous to third parties (such as banks) and the government.[91] Indeed, the anonymity of cash is an attractive quality for many as a medium for protecting the privacy of their transaction histories. The degree to which a digital token should be—or even could be—designed to be anonymous with respect to (i) the counterparty, (ii) third-party validators, and (iii) the government remains an arena of lively debate.

In contrast, account-based systems generally require some knowledge of the transacting parties' identities, such as the unique account number of the other party.[92] However, even if there was relative counterparty anonymity—for example, where the parties only knew the other's account numbers—third-party anonymity is likely absent. As discussed below, the banks operating the accounts would be "required to have information regarding the individuals' identities for a variety of legal reasons."[93]

Degree of Centralization for Distribution and Validation

The central bank could opt to (i) directly oversee and manage the CBDC or (ii) delegate roles to other actors, such as commercial banks.

[83] *Id.*

[84] *Id.*

[85] *Id.* ("Identification is needed to correctly link payers and payees and to ascertain their respective account histories.")

[86] Charles M. Kahn, Francisco Rivadeneyra and Tsz-Nga Wong, *Should the Central Bank Issue E-Money?, Working Paper 2019-3a*, FED. RES. BANK OF ST. LOUIS (Oct. 2018) at 11, https://research.stlouisfed.org/wp/more/2019-003, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3318871.

[87] Comm. on Paymts. & Mkt. Infrastructures, *supra* note 13, at 4.

[88] Mancini-Griffoli, *supra* note 78, at 4.

[89] Ankit Panda, *Cryptocurrencies and National Security*, COUNC. ON FOR. RELATIONS. (Feb. 28, 2018), https://www.cfr.org/backgrounder/cryptocurrencies-and-national-security.

[90] *See* Agur, *supra* note 71, at 115 ("An essential feature of physical cash is its anonymity.").

[91] This is less often the case with respect to the transacting counterparty, since the cash transactions typically take place in person.

[92] Kahn, *supra* note 85, at 11.

[93] *Id.*

For a token-based CBDC, the Federal Reserve Banks could directly handle the distribution of new digital tokens to consumers and/or directly operate the validation process of digital tokens as a central validating node. Alternatively, the Federal Reserve Banks could collaborate with private entities to accomplish these responsibilities. For distribution, the Federal Reserve Banks could partner with commercial banks to circulate the digital tokens to their consumers based on demand. This decentralized distribution scheme is already used for the circulation of cash. As for validation, the Federal Reserve Banks could rely on a network of nodes outside the Federal Reserve System, be it a permissionless network or a permissioned network, to prevent double spending and preserve the integrity of the ledger.

Although an account-based CBDC would be held by Federal Reserve Banks, the degree to which the Federal Reserve Banks directly administer those accounts would remain a deliberate choice. A more centralized scheme would involve the Federal Reserve Banks designing and operating the account's verification requirements and associated payment and customer services. Alternatively, the Federal Reserve Banks could delegate the day-to-day responsibilities of administering the digital accounts to private sector firms, such as commercial banks.[94]

Quantitative Limits

The Federal Reserve Board and the Federal Reserve Banks could impose quantitative limits on transaction or storage sizes for CBDC "as a way of controlling potentially undesirable implications or to steer usage in a certain direction."[95] For instance, a cap could be imposed on the amount of CBDC that can be stored in a wallet or account. Alternatively, there could be a cap in the amount of CBDC a user can transact in for a single transaction. Finally, softer limits could be imposed, where the user would be permitted to hold or transact in an amount of CBDC beyond the limit—but with reduced anonymity.

Interest-bearing

Unlike cash, digital tokens and accounts could be designed to pay interest (positive or negative).[96] Indeed, existing forms of account-based money, such as master accounts and commercial bank accounts, are already interest-bearing. Importing this characteristic to digital tokens is also technically feasible. Positive CBDC interest rates would encourage storing CBDC and converting holdings of other currencies into CBDC; negative CBDC interest rates would encourage spending and converting holdings of CBDC into other currencies.[97]

Legal and Policy Considerations

The particular bundle of features that define a CBDC will pose important legal and policy implications for the central bank. Provided below are a few to consider.

[94] *See* Ben Dyson and Graham Hodgson, *Digital Cash: Why Central Banks Should Start Issuing Electronic Money*, Positive Money (2016), at 16–19, https://positivemoney.org/wp-content/uploads/2016/01/Digital_Cash_WebPrintReady_20160113.pdf.

[95] Comm. on Paymts. & Mkt. Infrastructures, *supra* note 13, at 4.

[96] A negative interest rate means that the user pays the central bank to store its CBDC.

[97] Comm. on Paymts. & Mkt. Infrastructures, *supra* note 13, at 6.

Concerns Related to Anti-Money Laundering, Know Your Customer, and Counter-Terrorism Financing

The Federal Reserve Board would need to consider concerns and policies relating to laws on anti-money laundering (AML) and counter-terrorism financing (CFT). Banks are subject to various laws that restrict them from providing financial services that would assist with criminal activity. Such laws also require banks to maintain customer due diligence programs for bank accounts and monitor suspicious activity, including cash transaction amounts exceeding $10,000.[98] AML and know-your-customer laws (KYC) also apply to the Federal Reserve Banks but current compliance is easy in practice, as only banks have direct access to master accounts with Federal Reserve Banks.

CBDC that grants broad anonymity to users and limits traceability of transactions could become a favored medium for illicit activities, thereby potentially raising legal and reputational concerns for the Federal Reserve System. Cryptocurrencies have been criticized by some as a preferred medium of payment for facilitating illegal activities.[99] A recent Europol report found that cryptocurrencies "remain the primary payment mechanism for the payment of criminal services…"[100] For example, the Islamic State of Iraq and al-Sham (ISIS), a militant terrorist organization, solicited donations in Zcash and Bitcoin in order to finance their propaganda efforts.[101] Cryptocurrencies also figure prominently in so-called Darknet markets, which are online marketplaces for illicit commodities and services, especially drugs.[102] A recent paper concluded that "illegal activity accounts for a substantial proportion of the users and trading activity of bitcoin.[103] Such concerns caution against issuing opaque digital tokens, at least not without a key in the government's hands to unlock encrypted transaction information.

On the other hand, there may be legitimate demands for anonymity to safeguard privacy. Transacting parties might seek to avoid the unwelcome nuisance of directed advertising or weightier dangers of identity theft or personal harm.[104] Purchase history could also reveal health-related conditions and shopping habits, which, while not unlawful, could cause embarrassment. After all, "knowledge by a third party of the payee, amount, and time of payment for every transaction made by an individual can

[98] 31 C.F.R. § 1010.311 ("Each financial institution…shall file a report of each deposit, withdrawal, exchange of currency or other payment or transfer, by, through, or to such financial institution which involves a transaction in currency of more than $10,000….").

[99] Large-denominated paper notes—which grant almost complete anonymity—are also widely used for transactions related to criminal activities, including transactions abroad, *see* Kenneth S. Rogoff, *Response to Jeffrey Rogers Hummel's Review of 'The Curse of Cash'*, 14 ECON. J. WATCH (May 2017), at 164, 168 ("[W]hile there are many reasonable uses of the $100 bill abroad, it is indisputably popular with Russian oligarchs, Mexican drug lords, illegal arms dealers, Latin American rebels, corrupt officials, human traffickers, etc., and of course North Korean counterfeiters."), https://econjwatch.org/articles/response-to-jeffrey-rogers-hummel-s-review-of-the-curse-of-cash.

[100] EUROPOL, *Internet Organised Crime Threat Assessment (IOCTA) 2018*, EUROPOL (2019), at 58 (2018), https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018.

[101] *Id.* at 53 ("Cryptocurrencies represent a source of opportunity for terrorist groups, allowing them to move funds across borders while avoiding the regular banking scrutiny…[By] the end of 2017…[Islamic State] sympathisers triggered mass cryptocurrency (Bitcoin and the more anonymous Zcash) donation campaigns in [Islamic State] affiliated websites as well as in chat environments (e.g. Telegram) to support their cause.").

[102] *Id.* at 47. (In 2014, the FBI and DEA shut down Silk Road, perhaps the most infamous Darknet market).

[103] Sean Foley, Jonathan R. Karlsen and Tālis J. Putniņš, *Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies?*, OXFORD L.: OXFORD BUS. L. BLOG (Feb. 19, 2018), https://www.law.ox.ac.uk/business-law-blog/blog/2018/02/sex-drugs-and-bitcoin-how-much-illegal-activity-financed-through ("For example, approximately one-quarter of all users (25%) and close to one-half of bitcoin transactions (44%) are associated with illegal activity. The estimated 24 million bitcoin market participants that use bitcoin primarily for illegal purposes (as at April 2017) annually conduct around 36 million transactions, with a value of around $72 billion, and collectively hold around $8 billion worth of bitcoin. To give these numbers some context, the total market for illegal drugs in the US and Europe is estimated to be around $100 billion and €24 billion annually.").

[104] Bech and Garratt, *supra* note 38, at 64.

reveal a great deal about the individual's whereabouts, associations and lifestyle."[105] The trends towards privacy around consumer data means that users are increasingly worried about what happens to their information after its collection, since data could be shared, sold, or lost. Indeed, the anonymity of cash remains an attractive quality for many as a medium for protecting the privacy of their transaction histories. Even if the government or company collecting the data fully aligned with the user's interests, others—such as foreign states or rogue hackers—could also be trying to get ahold of that information.

Monetary Policy

Provocatively, CBDC could expand the Federal Reserve's arsenal for controlling monetary policy in two respects. For the purposes of this briefing, please consider how CBDC's implications for monetary policy relate to discussions on whether consumers' usage of currency should fall outside or within the control of the central bank.[106] Negative interest rates are highly controversial and viewed by many as a confiscation of private property. Since a direct deduction would be made from the account, negative interest rates are quite different from the erosion of inflation. Negative interest rates, as used in Europe, and as recently suggested by President Trump, have been limited to the wholesale accounts of commercial banks with the central bank. They have not been imposed upon consumers. This analysis should include how the controversial nature of these policies may impact the political economy.

First, replacing cash with an interest-bearing digital currency could grant the Federal Reserve a powerful new instrument for effectuating negative interest rates[107]—which means that the user pays the central bank to store its currency—a policy theorized to discourage users from hoarding money and stimulate spending in the economy. Because cash has no interest rate, a central bank's ability to cut interest rates becomes constrained when it approaches negative interest rate territory as people can convert their holdings in the banking system into cash. However, if cash were to be supplanted by an interest-bearing CBDC, the Federal Reserve could be able to overcome this effective lower bound.[108]

Second, account-based CBDCs would enable the Federal Reserve to proactively airdrop funds into the accounts of consumers as another way of encouraging spending.[109] Some argue that such "helicopter drops" would operate more directly and precisely than reliance on quantitative easing, interest rate adjustments or commercial bank lending.[110] Furthermore, helicopter drops can be performed universally on all accounts or on a selective basis, depending on the relevant situation.[111] The operational difficulties

[105] David Chaum, *Blind Signatures for Untraceable Payments*, in Advances in Cryptology: Proceedings of Crypto 82, 199 (David Chaum, Ronald L. Rivest and Alan T. Shermanm eds. 1983).

[106] An economic policy division is handling the precise implications on monetary policy, so no need for you to closely parse the economic technicalities or the merits of deploying the following policies for the purposes of our briefing.

[107] *See* Kenneth Rogoff, *Dealing with Monetary Paralysis at the Zero Bound*, 31 J. OF ECON. PERSPS. 47, 57-58, (Summer 2017), https://scholar.harvard.edu/files/rogoff/files/dealing_with_monetary_paralysis_at_the_zero_bound.pdf.

[108] See *Id.*

[109] Some suggest that helicopter drops could also be performed by token-based CBDC, *see, e.g.*, Mike Bird, *HSBC Says the Blockchain Could Be Used for "HelicopterMoney,"* BUS. INSIDER (Nov. 9, 2015), https://www.businessinsider.com/hsbc-says-the-blockchain-could-be-used-for-radical-central-bank-helicopter-money-policies-2015-11?r=UK&IR=T, but this mechanism would likely be less straightforward; *see* Dyson and Hodgson, *supra* note 93, at 22 ("[I]t would be extremely easy for the Bank of England to make small and regular 'helicopter drops' to every citizen, as a tool of monetary policies.").

[110] Dyson, *supra* note 93, at 2, 8.

[111] For example, the government could selectively use helicopter drops for lower-income households to stimulate spending and "cushion[] their purchasing power from the effects of the downturn as well as from the temporarily negative level of the CBDC interest rate," Michael D. Bordo

of getting stimulus and unemployment checks to taxpayers during the COVID 19 pandemic has illustrated the need for a better system of distribution then mailing checks or cards.

These options would come at severe political cost, which you should account for in your briefing preparations. First, the imposition of negative interest rates assumes a feasible path towards eliminating cash. As a matter of practical reality, the abolition of cash and the threat of negative interest rates would confirm the suspicions held by broad demographic swaths of the country about the Federal Reserve's ambitions for repressing financial autonomy (see Appendix Item 13 and Appendix Item 18). Second, helicopter drops overtly tread into controversial decisions about redistribution—for example, decisions about how much money should be delivered and to whom. [112] Both actions could provoke public backlash and reignite critiques of the democratic legitimacy and institutional independence of the Federal Reserve. [113]

Seigniorage

Seigniorage, the profit made by the central bank from its issuance of currency (a function of the currency's face value *minus* production and distribution costs),[114] forms a vital source of revenue for the Federal Reserve System and the U.S. Treasury (that is, the American taxpayer).[115] Because of its status as the leading international reserve currency, the U.S. dollar generates substantial seigniorage revenues compared to other national currencies.[116] Seigniorage is particularly pronounced for high-denomination bills (namely $100 bills), which account for nearly 80% of the total value of U.S. dollars in supply[117] and which also enjoy high demand outside the United States. [118] The Federal Reserve System does not rely on congressional appropriations, [119] which could fluctuate based on political pressures. The independent

and Andrew T. Levin, *Central Bank Digital Currency and the Future of Monetary Policy, Econ. Working Paper 1714* 3 n. 10, HOOVER INSTITUTION (Aug. 2017), https://www.hoover.org/sites/default/files/research/docs/17104-bordo-levin_updated.pdf; *see also* Dyson, *supra* note 93, at 8; Mancini-Griffoli, *supra* note 78, at 16 n. 22 ("[Helicopter drops] would not necessarily reach all citizens.").

[112] Mancini-Griffoli, *supra* note 78, at 16 n.22 ("[T]he issue of legitimacy remains: how does the central bank decide how much to transfer to each household given the notable and very explicit redistributional consequences? Finally, helicopter drops would continue to be viewed as a form of monetary financing, thus undermining central bank independence.").

[113] *See* BARR, *supra* note 8, at 49 ("The Federal Reserve Board's power, however, remains controversial, and many critics want the Federal Reserve Board weakened or abolished. Critics allege that the Federal Reserve Board is secretive and undemocratic…."); *see also* PAUL TUCKER, UNELECTED POWER: THE QUEST FOR LEGITIMACY IN CENTRAL BANKING AND THE REGULATORY STATE (2018).

[114] Engert, *supra* note 14, at 3.

[115] *See*, Bd. Of Governors, *Who Owns the Federal Reserve?*, *FAQs*, FED. RES. SYS, https://www.federalreserve.gov/faqs/about_14986.htm ("[T]he Federal Reserve Banks are required by law to transfer net earnings to the U.S. Treasury, after providing for all necessary expenses of the Federal Reserve Banks, legally required dividend payments, and maintaining a limited balance in a surplus fund.").

[116] To illustrate, the Federal Reserve Banks transferred to the U.S. Treasury $97.7 billion, $91.5 billion, $80.2 billion, and $62.2 billion (estimated) in earnings remittances in 2015, 2016, 2017, and 2018, respectively, Bd of Governors, *Press Release: Federal Reserve Board announces Federal Reserve Bank income and expense data and transfers to the Treasury for 2018*, FED. RES. SYS. (Jan. 10, 2019), https://www.federalreserve.gov/newsevents/pressreleases/other20190110a.htm.

[117] Kenneth S. Rogoff, The Curse of Cash: How Large-Denomination Bills Aid Crime and Tax Evasion and Constrain Monetary Policy, 3, 51 (2016).

[118] *See* Ruth Judson, *Big Note, Small Note: Central Bank Digital Currency and Cash*, *in* DO WE NEED CENTRAL BANK DIGITAL CURRENCY? 33, 35 (2018) ("[T]he estimates in Judson (2016) indicate that about 70% of $100s could be held abroad, with the rest held at home."); ROGOFF, *supra* note 116, at 39 ("[F]oreign holdings…might explain as much as 50% of US dollar holdings.").

[119] Bd. Of Governors, *What Does It Mean that the Federal Reserve Is "Independent Within the Government?"*, *FAQs*, FED. RES. SYS. (Mar. 1, 2017) https://www.federalreserve.gov/faqs/about_12799.htm ("The Federal Reserve does not receive funding through the congressional budgetary process."); Bd. Of Governors, *Who Owns the Federal Reserve?*, *FAQs*, FED. RES. SYS., https://www.federalreserve.gov/faqs/about_14986.htm.

funding of the Federal Reserve provides an additional safeguard for its institutional autonomy and independent policymaking.[120]

Seigniorage revenues would decline if demand for U.S. currency decreases. Cash's share in payment amounts has dropped considerably over recent years. Its decline could continue if users begin to favor cryptocurrencies or foreign currencies over U.S. currency, whether that be paper notes or digital notes. Although for now these concerns remain far from compelling, further developments in stablecoins—currently mostly experimental[121]—and non-U.S. CBDCs—currently mostly conceptual[122]—could provide an appealing alternative to the U.S. dollar. On the other hand, some have argued that developing a U.S. CBDC could recover leakage of or even exceed the seigniorage from U.S. cash.[123] This, of course, hinges on the perhaps overoptimistic assumption that future demand for a U.S. CBDC would match or exceed the existing demand for U.S. cash. Indeed, replacing cash with a CBDC that fails to appeal to users could inadvertently hasten the decline of seigniorage.

Financial Stability

Some academics worry that a retail CBDC that resembles bank deposits could raise the costs of deposit-taking for commercial banks, thereby reducing their ability to perform productive lending. Because a CBDC would be backed by the U.S. government, it would pose a safer alternative to bank deposits, which would be guaranteed only up to the deposit insurance limit of $250,000 per depositor.[124] There is a policy question whether it is sensible for the U.S. government to provide what would be, in effect, unlimited insurance of deposit funds. In times of crisis, the qualities of a CBDC having the "safety of physical cash but convenience of bank deposit accounts"[125] could induce depositors to flee from depository institutions towards the central bank, thereby weakening financial stability.[126] Indeed, the traditional bank run has been caused by depositors converting bank deposits into cash. A conversion of bank deposits into CBDC would have a similar impact on bank balance sheets and stability. Unlike a traditional bank run, the speed and scale would likely be unprecedented since a digital run could be triggered at the click of a button.[127]

Others, however, are less worried about financial stability. Some, including Professor Morgan Ricks, embrace the perceived structural implications of expanding the central bank's role and causing

[120] Christopher J. Waller, *Independence + Accountability: Why the Fed Is a Well-Designed Central Bank*, FED. RES. BANK OF ST. LOUIS *REV.* 293, 298 (2011) ("[A] common method for politicians to entice government agencies is to threaten to cut the agencies' budgets…To counteract this possibility, Congress gave the Federal Reserve budget autonomy when it created the Fed in 1913. The Fed was given the power to earn its own income and spend it without government interference.").

[121] Stablecoins seek to overcome the volatility endemic among cryptocurrencies. Specifically, they are a type of crypto-asset for which the value is pegged to the value of another asset, such as the U.S. dollar, gold, or algorithmic pricing based on circulation supply. Santiago Fernández de Lis, *Central Bank Digital Currencies: Features, Options, Pros and Cons*, *in* DO WE NEED CENTRAL BANK DIGITAL CURRENCY? 46, 54 (2018).

[122] Barontini, *supra* note 50, at 1 ("The survey shows that, although a majority of central banks are researching CBDCs, this work is primarily conceptual and only a few intend to issue a CBDC in the short to medium term.").

[123] *See* Dyson, *supra* note 93, at 11–12; *see also* Morgan Ricks, John Crawford and Lev Menand, Digital Dollars, (Vanderbilt Univ. Law Sch., Research Paper No. 18-33, also Univ. Cal. Hastings Research Paper No. 287) (rev. Feb. 10, 2020), at 16–17, https://ssrn.com/abstract=3192162.

[124] *But see* Mancini-Griffoli, *supra* note 78, at 25 (commenting that while deposit insurance does not immunize banks from runs, it significantly mitigates the risk).

[125] Dyson, *supra* note 93, at 27.

[126] Comm. on Paymts. & Mkt. Infrastructures, *supra* note 13, at 16.

[127] *Id.*

"large-scale migration from bank deposits" to the central bank (see Appendix Item 14).[128] These proponents take the view that radical disintermediation of the private banking sector from deposit-taking would generate *more* financial stability, not less.

Cybersecurity

While offering convenience and efficiencies, digitization also carries risks of cyberthreats, including malware and fraud.[129] Cybersecurity is a significant operational risk and central banks are not immune to hacks.[130] In fact, instituting a CBDC could elevate the profile of the central bank as a target for cyberattacks.[131] The likelihood and severity of cyberattacks would be further exacerbated for a CBDC that enjoys reserve currency status and is universally accessible, which would open the platform to "many participants and points of attack."[132]

Options for a U.S. Central Bank Digital Currency

The two proposed CBDCs aim to improve the convenience and lessen the costs of payment systems, and enhance implementation of monetary policy. With this background in mind, please consider the three options discussed below. Both proposed CBDCs would be issued by Federal Reserve Banks, would be denominated in the U.S. dollar, and would also be convertible with other forms of money; similar to cash, both CBDCs would be deemed to be legal tender. As a third option, consider whether it would be more prudent to adopt a wait-and-see approach, and stick with the existing system.

Option 1: Fedcoin

Fedcoin is a digital token built on a permissioned blockchain (Fedchain)[133] and issued by the Federal Reserve Banks. Unlike permissionless cryptocurrency, like Bitcoin, the production of Fedcoin is managed and controlled by the Federal Reserve Banks, which also serve as the only trusted parties in the network. Federal Reserve Banks would possess the ability to create and destroy Fedcoin in order to preserve a 1:1 conversion ratio between Fedcoin and the dollar. Although Federal Reserve Banks would maintain Fedcoin's value, approved nodes would maintain the ledger's verification, validating new transactions and screening out counterfeiting and double spending. These nodes would be operated by a select group of large commercial banks approved by the Federal Reserve Banks.

[128] Ricks, *supra* note 122. (While Professor Ricks and his coauthors would prefer "more traditional nomenclature," *Id.* at 25–26, his FedAccount proposal is an example of a universally accessible, accounts-based CBDC.).

[129] Comm. on Paymts. & Mkt. Infrastructures, *supra* note 13, at 10.

[130] Other Federal institutions have demonstrated vulnerability to cyberattacks. *See, e.g.*, Jim Sciutto, *OPM Government Data Breach Impacted 21.5 Million*, CNN (July 10, 2015), https://www.cnn.com/2015/07/09/politics/office-of-personnel-management-data-breach-20-million/index.html ("Government investigators now believe that the data theft from the Office of Personnel Management computer systems compromised sensitive personal information, including Social Security numbers, of roughly 21.5 million people from both inside and outside the government, the government announced Thursday.").

[131] Brainard, *supra* note 37.

[132] Comm. on Paymts. & Mkt. Infrastructures, *supra* note 13, at 10.

[133] Among other things, Fedchain would overcome Bitcoin's technological constraints of scalability.

Users cannot directly access Fedcoin through an account at a Federal Reserve Bank but must withdraw Fedcoin from their commercial bank accounts. Once withdrawn, the Fedcoin becomes anonymous to the bank. Subsequently, Fedcoin may be stored in digital wallets provided by various private sector firms (*e.g.*, banks or fintech companies) that are certified by a Federal Reserve Bank. Anyone who purchases and installs the requisite wallet software into a smartphone or personal computer is able to store and pay with Fedcoin. A user can set up as many addresses for the wallet as he or she wishes. Once the wallet is set up, a user can engage in transactions in a similar way as Bitcoin.

As mentioned before, the nodes are operated by large commercial banks approved by the Federal Reserve Banks and validate Fedcoin transactions between users. These entities also use Fedcoin for their own payments. As an incentive for operating these nodes, those responsible for validation will be able to collect transaction fees. If consensus is reached by these nodes, the approved Fedcoin transaction is recorded on the Fedchain. Although Fedchain is a public ledger, only transaction amounts and party addresses are viewable.

Option 2: Fedcount

Fedcount offers a new account-based money created and held by the Federal Reserve Banks. Unlike master accounts, Fedcounts would be generally accessible to the nonbank public for holding electronic money. Fedcounts would hold electronic money for all users who register with their Federal Reserve Bank. To prevent fraud and enable instantaneous verification, registration with a Federal Reserve Bank and login to Fedcount require fingerprint and/or facial recognition, which is already technologically feasible with smartphones. After successful login, users can review the account balance and transaction history of the Fedcount but nothing else. The development of expanded interfaces for payments and other functions would have to be provided by private sector firms, such as commercial banks. Such institutions would administer the relevant services to make Fedcount suitable for a user's needs in exchange for fees. Integral functions to develop include the interfaces to initiate payments and to review more detailed transaction summaries. Other functions would include internet coverage, periodic statements, and customer support.

Although a commercial bank might administer Fedcounts, Fedcounts would be distinct from a deposit account at a private bank because Fedcounts would be directly held at a Federal Reserve Bank and belong to the account holder (*i.e.*, the user). The relevant Fedcount administrator would only be responsible for offering services associated with the Fedcount. Therefore, unlike conventional bank accounts, commercial banks providing Fedcounts would not be able to conduct lending with money housed within Fedcounts. Moreover, money stored in Fedcount represents a liability of the relevant Federal Reserve Bank, not of the Fedcount administrator. Thus, according to the analysts, even if the bank administering services to the Fedcount were to fail, the Fedcount would remain safe with the Federal Reserve Bank.

Option 3: Neither

For the purposes of practicably advancing payment efficiencies and monetary policy implementation, neither Fedcoin nor Fedcount would be superior to maintaining the existing infrastructure supporting cash. It is therefore prudent to continue with the current system for the foreseeable future.

Briefing Questions

Having examined the proposals, please review the materials included in the attached Appendix and prepare to brief the Director. In particular, the Director is eager to know your thoughts as to the following:

1. What are the comparative strengths and weaknesses of Fedcoin and Fedcount? In what ways can these proposals be improved?
2. What would be the likely reaction from financial sector stakeholders to these proposals? Consider the following four examples:
   - Ames Bank is a depository institution located in Cambridge, Massachusetts. Its business primarily consists of making loans to businesses, for which much of the funding is done through deposit-taking.
   - BitBank is a cryptocurrency company that supports and develops wallets for Bitcoin and Bitcoin-derived currencies. Its wallets do not have compatibility with other types of cryptocurrencies.
   - The Zcash Company supports and develops Zcash, which is a privacy-protecting digital currency. Zcash features zero-knowledge proofs that allow the payee to prove the validity of a transaction without revealing information about the transaction itself. This allows transactions to be fully shielded from being traced within the public blockchain, thereby completely protecting the users' privacy.
   - Libra is a blockchain-based digital currency, proposed by Facebook, and administered by the Libra Association. The currency and network are still in development.
3. Consider the following proposals made by our IT specialists:
   - For Fedcoin – IT specialists claim that Fedchain's cybersecurity capabilities could be enhanced by moving from a permissioned network of nodes to a permissionless network of nodes. They argue that a permissionless network would offer more robust operational resilience as the consensus mechanism could continue operating should any node become unavailable or compromised. What are the benefits and concerns?
   - For Fedcount – IT specialists insist that Fedcount has the technological capability of providing more comprehensive services and greater financial inclusion for users if the Federal Reserve assumed control over administering Fedcount's payment and customer services. What are the benefits and concerns?
4. Although cash is deemed legal tender, Federal law does not obligate a private business to accept cash payments. Businesses retain discretion to accept payment in whatever form they prefer. Take for example, bus lines that refuse pennies or convenience stores that refuse high-

denomination bills.[134] Other countries such as China and France take a different approach, making it generally unlawful for payees to refuse notes and coins with the status of legal tender. What are the benefits and drawbacks of these two approaches as applied to CBDC? How likely is the U.S. approach to change to this alternative approach? How should society weigh the payer's right to choose between payment methods with that of the payee's?

5. As the readings suggest, many closely associate anonymity with privacy. Yet, the two are distinct. Information can be private but not anonymous, such as transaction logs with personally identifying information safeguarded by a bank; likewise, information could be anonymous but not private, such as the sharing or disclosure of spending patterns aggregated across large numbers of users. Is this a meaningful distinction? If so, how does it pertain to the conversation about CBDC?
6. How does CBDC, whether by its nature or by design choice, compare with the attributes of cash?
7. Circulation and usage of U.S. notes extends beyond U.S. citizenship and territoriality. On the other hand, eligibility for master accounts with Federal Reserve Banks is limited to U.S. entities with a few exceptions. What legal and policy considerations would be implicated if CBDC access is granted internationally or restricted nationally? If the latter, should any controls be in place?
8. How would you rank the three options for purposes of payment efficiencies and monetary policy implementation?
    - Would your conclusion change if the motivation for developing CBDC was instead to advance (i) financial stability or (ii) financial inclusion (see footnote 22)? Is either financial stability or financial inclusion a pressing objective for the Federal Reserve System?

[134] Treas. Dept., Legal Tender Status, U.S. Dep't of Treasury (Jan. 4, 2011), https://www.treasury.gov/resource-center/faqs/currency/pages/legal-tender.aspx.

Appendices

Speech by Governors of the Federal Reserve Board

1. Remarks by Gov. Lael Brainard, Bd. of Governors of the Fed. Reserve Sys., Cryptocurrencies, Digital Currencies, and Distributed Ledger Technologies: What Are We Learning? (May 15, 2018), https://www.federalreserve.gov/newsevents/speech/brainard20180515a.htm.
2. Remarks by Gov. Lael Brainard, Bd. of Governors of the Fed. Reserve Sys., Digital Currencies, Stablecoins, and the Evolving Payments Landscape (October 16, 2019), https://www.federalreserve.gov/newsevents/speech/brainard20191016a.htm.

Congressional Hearing

3. The Future of Money: Digital Currency, Hearing Before the Subcommittee on Monetary Policy and Trade of the Committee on Financial Services, U.S. House of Representatives (July 18, 2018).
4. Transcript Excerpts of the Prepared Statement of Eswar S. Prasad

Casebook

5. Excerpts of Chapters 1.2 and 9.1, Michael S. Barr, Howell E. Jackson and Margaret E. Tahyar, Financial Regulation: Law and Policy (2d ed. 2018).

IMF Publications

6. Christine Lagarde, Managing Director, IMF, Winds of Change: The Case for New Digital Currency (Nov. 14, 2018).
7. TOMMASO MANCINI-GRIFFOLI ET AL., IMF, CASTING LIGHT ON CENTRAL BANK DIGITAL CURRENCY, IMF STAFF DISCUSSION NOTE (Nov. 2018).

BIS Report

8. BANK FOR INT'L SETTLEMENTS, CENTRAL BANK DIGITAL CURRENCIES (2018), https://www.bis.org/cpmi/publ/d174.pdf.
9. CHRISTIAN BARONTINI AND HENRY HOLDEN, BANK FOR INT'L SETTLEMENTS, PROCEEDING WITH CAUTION – A SURVEY ON CENTRAL BANK DIGITAL CURRENCY (2019), https://www.bis.org/publ/bppdf/bispap101.pdf.

Academic Articles

10. Itai Agur, *Central Bank Digital Currencies: An Overview of Pros and Cons*, *in* DO WE NEED CENTRAL BANK DIGITAL CURRENCY? (2018).
11. Aleksander Berentsen and Fabian Schär, *The Case for Central Bank Electronic Money and the Non-case for Central Bank Cryptocurrencies*, 100 FED. RES. BANK OF ST. LOUIS *REV.* 97 (2018).

12. Charles M. Kahn, Francisco Rivadeneyra and Tsz-Nga Wong, Should the Central Bank Issue E-Money? (Oct. 2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3271654.
13. Robert C. Hockett, Money's Past Is Fintech's Future: Wildcat Crypto, the Digital Dollar, and Citizen Central Banking (Dec. 11, 2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3299555.
14. Kenneth Rogoff, *Dealing with Monetary Paralysis at the Zero Bound*, 31 J. of Econ. Persps., Summer 2017, at 47 (2017).
15. Jeffrey Rogers Hummel, *The War on Cash: A Review of Kenneth Rogoff's* The Curse of Cash, 14 Econ. J. Watch, May 2017, at 138.
16. Morgan Ricks, John Crawford and Lev Menand, *A Public Option for Bank Accounts (or Central Banking for All)* (Vanderbilt Univ. Law Sch., Research Paper No. 18-33, 2018), https://ssrn.com/abstract=3192162.

News Articles

17. Izabella Kaminska, *When the State Takes on the Digital Float, the State Takes on the Risk*, Fin. Times (Jan. 10, 2019), https://ftalphaville.ft.com/2019/01/10/1547096400000/When-the-state-takes-on-the-digital-float--the-state-takes-on-the-risk/.
18. Nouriel Roubini, *Central Bank Digital Currencies Will Destroy Cryptocurrencies*, ING Think (Nov. 19, 2018), https://www.project-syndicate.org/commentary/central-banks-take-over-digital-payments-no-cryptocurrencies-by-nouriel-roubini-2018-11.
19. Simon Scorer, *Central Bank Digital Currency: DLT, or not DLT? That Is the Question*, Bank Underground (June 5, 2017), https://bankunderground.co.uk/2017/06/05/central-bank-digital-currency-dlt-or-not-dlt-that-is-the-question/.
20. James Grant, *Hostage to a Bull Market*, Wall St. J. (Sept. 9, 2016), https://www.wsj.com/articles/hostage-to-a-bull-market-1473456611.

International Reports

21. Center for the Fourth Industrial Revolution, *Central Bank Digital Currency Policy-Maker Toolkit*, World Economic Forum (Jan. 2020), http://www3.weforum.org/docs/WEF_CBDC_Policymaker_Toolkit.pdf.

PART V

PRIVACY & THE REGULATION OF INFORMATION

HARVARD LAW SCHOOL | The Case Studies

CSP059
JUNE 2020

Regulating Consumer Permissioned Access to Financial Data

CONNOR TWEARDY AND NAFISA ABUBAKAR ADAMA

Memorandum

DATE: June 1, 2020
TO: Junior.Attorney@joebiden.com
FROM: Senior.Attorney@joebiden.com
RE: Consumer Permissioned Access to Financial Data

Welcome to the Biden for President Policy Team! We've got a live topic that needs your immediate attention, so I hope you're ready to get started. A few groups that support our campaign are at loggerheads over an issue in the Fintech space and we need you to prepare a platform on the topic and recommend a series of steps for us to implement if and when we take the White House.

The debate is between Fintech startups and privacy advocates and focuses on how the Consumer Financial Protection Bureau ("CFPB") should regulate access to consumer financial data. To give you some general background, the United States ("U.S.") federal government is lagging behind many other bodies in regulating consumer data. The European Union ("E.U.") in particular set the new global standard with their General Data Protection Regulation ("GDPR"). That provision implemented consumer rights to access, rectify, and delete their data, the right to data portability, and a number of other novel and innovative consumer protections.[1] The regulation also reaches extraterritorially and applies to any US companies storing or processing personal data of E.U. residents.[2]

In the US, Title V of the Gramm-Leach-Bliley Act ("GLBA") provides some very limited protections for consumer *financial* data (as compared to data regulations of general application). It gives consumers nationwide a right to disclosure of privacy practices by some financial institutions and the right to prevent

[1] GDPR, Art. 1-20.

[2] *See* GDPR, Art. 3.

Written by Nafisa Abubakar Adama, HLS LLM 2020, and Connor Tweardy, HLS JD 2020, under the supervision of Professor Howell E. Jackson, James S. Reid, Jr., Professor of Law, Harvard Law School. Case development at Harvard Law School is partially funded by a grant from Dechert LLP. Cases are developed solely as the basis for class discussion. They are not intended to serve as endorsements, sources of primary data, legal advice, or illustrations of effective or ineffective management.

Copyright © 2020 President and Fellows of Harvard University. No part of this publication may be reproduced, stored in a retrieval system, used in a spreadsheet, or transmitted in any form or by any means—electronic, mechanical, photocopying, recording, or otherwise—without permission. To order copies or permissions to reproduce materials please visit our website at casestudies.law.harvard.edu or contact us by phone at 617-496-1316, by mail at Harvard Law School Case Studies Program, 1545 Massachusetts Avenue – Areeda 507, Cambridge, MA 02138, or by email at HLSCaseStudies@law.harvard.edu.

those institutions from sharing their data with non-affiliated parties. Even these narrow rights are subject to exemptions.[3]

At the state level, California enacted a general data protection measure similar to GDPR in the California Consumer Privacy Act ("CCPA"). Similar to GDPR, the CCPA does not restrict its application to any industry in particular but rather applies to all companies that collect the personal information of Californians provided the company is a for-profit, carries on business activities in California, and qualifies as a "business" per the definition in the CCPA.[4] Many national financial institutions are thus subject to these rules.

This patchwork regulatory approach has produced outcries from different groups for different reasons. US financial institutions bemoan the patchwork approach as subjecting them to duplicative regulation. Fintechs and large banks alike fear that other states might follow California's lead and enact local privacy regulations in the absence of a federal approach.[5] Privacy advocates meanwhile argue that too many banks are under regulated at the moment. GBLA provides only narrow rights while CCPA and GDPR are both bounded geographically, leaving many small financial institutions and those that segment their operations into under regulated regional entities.[6] For these reasons, actors on both sides are calling for federal action on data privacy protection, but with different views as to the content of appropriate measures.

One specific issue has come to the forefront of this debate in the financial sector: consumer-permissioned access to financial data. To be clear, this issue goes beyond the rights of consumers themselves to *directly* access their data held by financial institutions. That right is relatively uncontroversial. The debate here is about consumer-*permissioned* access to financial data.[7] An industry has sprung up in recent years with data aggregators and Fintech startups using consumer consent to gather data from traditional financial institutions.[8] These data flows have been integral to the Fintech boom and have produced innovative services and greater competition in the financial sector. In fact, some estimate that increasing access to data in consumer finance could add between $210 to $280 billion a year to global GDP, with up to 50 percent of this total flowing to consumers through enhanced price transparency and tailored product offerings.[9]

At the same time, transfer of sensitive financial data from well-regulated entities to unregulated startups carries inherent risks to consumer privacy and data security and these practices have been opposed by many banks and consumer advocates. Consent, if not fully informed, may allow private data

[3] 15 U.S.C. § 6802; 12 C.F.R. § 1016.10(a).

[4] CAL CIV. CODE § 1798.140(c)(1).

[5] *See* Lauren Davis, *The Impact of the California Consumer Privacy Act on Financial Institutions Across the Nation*, 24 N.C. BANKING INST. 499 (2020), available at https://scholarship.law.unc.edu/ncbi/vol24/iss1/22.

[6] *America Should Borrow from Europe's Data-Privacy Law*, The Economist, April 5, 2018, available at https://www.economist.com/leaders/2018/04/05/america-should-borrow-from-europes-data-privacy-law.

[7] *See* Brian Knight, *Statement Regarding CFPB Dodd-Frank Section 1033 Symposium* (Feb. 26, 2020), available at https://files.consumerfinance.gov/f/documents/cfpb_knight-statement_symposium-consumer-access-financial-records.pdfhttps://files.consumerfinance.gov/f/documents/cfpb_knight-statement_symposium-consumer-access-financial-records.pdf.

[8] U.S. Dep't of Treasury, A Financial System that Creates Economic Opportunity: Nonbank Financials, Fintech, and Innovation 22 (2018) (hereinafter "Treasury Fintech Report").

[9] Manyika et al., *Open Data: Unlocking Innovation and Performance with Liquid Information*, Mckinsey Global Institute 91-101, available at https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/open-data-unlocking-innovation-and-performance-with-liquid-information.

to be shared in ways that a consumer would likely not approve. A consumer might think they are sharing only a small part of their data for a limited purpose only to find that a Fintech or other third party is receiving income data or other sensitive information they did not intend to share, holding that data indefinitely, and even reselling it on to other groups.[10] Startups and other small Fintech players also make attractive targets for hackers, creating even more unintended spreading of a consumer's data.[11]

Our objective is to find a policy platform that addresses these concerns and makes the sharing of consumer financial data both freer and safer. We have two basic sets of levers to pull in reaching that goal. First, we can direct the CFPB to use the authority granted to it under Section 1033 of the Dodd-Frank Act ("Section 1033 of the DFA") to issue a new rule clarifying the right of consumers to grant permissioned access to their data. Second, we can have the CFPB issue guidance regarding how existing regulations apply to these new business models.

Senior staff would like you to prepare a briefing in which you propose a regulatory direction for our administration and propose concrete steps that should be taken.[12] Please consider the reactions we should expect from Fintech firms, established financial institutions (both large and small), and privacy advocates, including a discussion of how we might structure our approach to be responsive to their legitimate interests.

Included is a memo we obtained from the CFPB to help get you started. It was prepared in advance of a symposium that was held on this topic earlier this year and lays out several of the key regulatory questions at issue.

Here's a list of specific questions to address during the briefing:

Section 1033 of the DFA

1. Does Section 1033 of the DFA include a right to consumer-permissioned access to data?
2. Assuming a consumer's consent is informed, should their ability to grant permissioned access to their data be unlimited?
3. Should financial service providers be able to decline transfers to certain parties despite customer consent (e.g. if they find that a company has insufficient security protocols in place to protect the transferred data)? If so, who should determine the criteria for disqualification?
4. Does the text of DFA 1033 specify whether consumers may access observed and/or inferred data under their financial service provider's control? If the text is ambiguous, what stance should the CFPB take?
5. Should the CFPB take any steps to encourage API adoption and discourage the use of screen-scraping?

[10] National Consumer Law Center (on behalf of its low income clients), *Written Statement for CFPB's Symposium on Consumer Access to Financial Records, Section 1033 of the Dodd-Frank Act* (Feb. 12, 2020), accessible at https://files.consumerfinance.gov/f/documents/cfpb_wu-statement_symposium-consumer-access-financial-records.pdf (hereinafter "NCLC Symposium Statement").

[11] American Bankers Association, Request for Information Regarding Consumer Access to Financial Records Docket No.: CFPB-2016-0048 9-10 (Feb. 21, 2017), available at https://www.regulations.gov/document?D=CFPB-2016-0048-0041 (hereinafter "ABA RFI Response").

[12] Please also assume that our administration will have sufficient authority and influence to guide the direction of the CFPB on this issue, setting aside their status as an independent agency.

FAIR CREDIT REPORTING ACT ("FCRA")

6. Are data aggregators consumer reporting agencies under FCRA?
7. Is a financial institution a data furnisher if it provides an API through which aggregators access data?

ELECTRONIC FUNDS TRANSFER ACT ("EFTA")

8. As a legal matter, do banks remain liable under Reg E for unauthorized charges made in their systems that result from a consumer data breach at a Fintech company?
9. As a policy matter, how should liability be apportioned between Fintechs and traditional financial institutions in such cases?

Note that we also have a second policy team addressing the broader question of whether our administration should adopt a general privacy regulation (in the same vein as GDPR or CCPA). Their recommendation will likely have implications for your research and we may ask you both to coordinate your work, and possibly even present at a joint meeting. I'm attaching an academic memorandum that they are using as a reference point.

Thank you for your help and we look forward to your presentation.

Best,
Policy Team Lead

Memorandum

DATE: February 20, 2020

TO: Kathy Kraninger, Director, CFPB

Tom Pahl, Policy Associate Director for Policy, Research and Regulations

FROM: Office of Susan Bernard, Assistant Director for Regulations

RE: Primer for the Upcoming Symposium on Consumer Access to Financial Data

Thank you both for your help in organizing the upcoming Symposium on Consumer Access to Financial Records. This internal memorandum is meant to serve as a primer to help prepare you and your teams for the debates that we expect to take place at the event, specifically focusing on the regulation of data aggregation and consumer-permissioned access to financial data. It first looks at the basic policy concerns underlying this debate and then turns to a general description and brief history of the market for consumer financial data. It ends with a discussion of ongoing regulatory debates that could require CFPB actions including potential rulemaking under Section 1033 of the Dodd-Frank Act ("Section 1033 of the DFA") and the need for guidance on the applicability of other existing regulations to data aggregation and Fintech.

General Policy Considerations

Regulation of the modern information economy has increasingly focused on giving consumers greater control over their own data. This emphasis on consumer autonomy has led several countries to recognize new consumer rights relating to their personal data, such as rights to access, correction and deletion. One less-discussed right in this toolkit is the right to data portability. The right to data portability allows individuals to obtain and reuse their personal data and can require data controllers to transfer the data to other service providers upon a consumer's request.[13] The right to permissioned access to consumer data is a variation of this concept.

Policy debates regarding the desirability of the right to data portability, and the appropriate limitations that should apply to it, focus on balancing four policy considerations:

Consumer Autonomy.[14] The datafication of the information economy has led to a general loss in power of consumers relative to businesses. Consumers have little ability to negotiate privacy terms in contracts as a result of insufficient expertise, asymmetric information, and a collective action problem. This leaves them without many options to exercise choice and control over their personal information (apart from declining to participate all together in certain industries). Regulation can address this power imbalance, restoring consumer choice and meaningful consumer control over their data.

[13] *See* GDPR Art. 20.

[14] *See generally* Michiel Rhoen, *Beyond consent: improving data protection through consumer protection law*, 5 *Internet Policy Review* (Mar.31, 2016), accessible at https://policyreview.info/articles/analysis/beyond-consent-improving-data-protection-through-consumer-protection-law.

Competition.[15] Access to data is a driving competitive dynamic in many modern industries. A company with more data on a consumer is often better able to serve that consumer. For instance, Amazon's ability to recommend books based on your shopping history gives it an advantage over Barnes & Noble. Allowing consumers to move their data between service providers makes it easier for new entrants to compete in the market or to provide new and innovative services that make use of that data.

Privacy.[16] Sharing consumer data between providers inherently reduces a consumer's privacy. Consent arguably mitigates this concern, but regulators and privacy advocates worry that consent alone does not provide sufficient protection. Consumers may not understand the types of data that are being shared, whom they might be shared with, and how they might be used. Absent regulation, the private sector arguably has little incentive to ensure that consent is fully informed and effective, worsening consumer privacy.

Security.[17] Data breaches and other illegal activities create costs for both consumers and businesses. Increasing data sharing between service providers introduces vulnerabilities that can increase the likelihood of breaches. For example, fraudsters may entice consumers to give them permission to access their data. Startups and other smaller companies may have weaker security relative to larger market players, making them attractive targets for hackers.

In the United States, the current regulatory debate surrounding the implementation of a right to permissioned access to consumer financial data involves the interaction of these considerations with the current state of the market for consumer financial data and, specifically, the emergence of modern financial data aggregators.

The Market for Financial Data Aggregation

Data Aggregation as a Business

Data aggregation is the process by which information from one or more sources is gathered and standardized.[18] In finance, the basic form of this market involves four groups of players:

- **Consumers** are individuals who use financial services. Their interactions with financial service firms create consumer financial data. They also decide which consumer Fintech applications they would like to use, and provide their consent to facilitate the flow of data from financial service firms to data aggregators and those consumer Fintech applications.
- **Financial services firms** are those that gather consumer financial data from users in the first instance, usually through direct commercial interactions with consumers. These are the banks, insurance companies, wealth management firms, and other financial institutions that one might associate with traditional consumer finance. The companies are the source of consumer financial account and transaction data.

[15] *See* Michael Barr et al, Consumer Autonomy and Pathways to Portability in Banking and Financial Services, University of Michigan Centeron Finance, Law and Policy 1-2 (November 3, 2019), available at http://financelawpolicy.umich.edu/files/umich-cflp-working-paper-consumer-autonomy-and-data-portability-pathways-Nov-3.pdf.

[16] *See* NCLC Symposium Statement, *supra* note 10, at 4-5.

[17] *See* ABA RFI Response, *supra* note 11, at 9-10.

[18] Treasury Fintech Report, *supra* note 8, at 23.

- **Data aggregators** access, aggregate, standardize, store, and disseminate consumer financial account and transaction data from a variety of financial services firms. They act as intermediaries between financial service firms as suppliers and consumer Fintech applications as clients. They may, but generally do not, have a direct commercial relationship with consumers. Instead they commonly function as back-end tools enabling Fintech applications.
- **Consumer Fintech applications** use consumer financial data to provide value-added services to consumers that may either complement or substitute services provided by traditional financial institutions. They obtain the data needed to provide their service either directly from financial services firms or from a data aggregator.[19]

A single entity may play multiple roles in this system. For example, a Fintech startup using a machine learning algorithm to make loans may at once use consumer financial data to make a lending decision, then gather new data as the loan is paid down.

Financial data aggregation is a technically demanding task, involving the large upfront cost of connecting to thousands of different financial institutions.[20] Connecting to banks can be particularly difficult. Banks are incentivized to impose switching costs on their depositors, giving them little reason to invest in easy data portability.[21] As a result, a handful of data aggregators who have sunk time and effort into making these connections serve as the backbone of the modern Fintech ecosystem.[22] A company like Plaid provides a single interface through which a startup can interact with the data from thousands of financial services firms.

Data Aggregation Methods

In practice, data aggregators generally access consumer financial data through one of two methods: screen-scraping or application programming interfaces (“APIs”).[23]

Screen-scraping is a method by which a data aggregator can retrieve consumer data from a financial services provider that does *not* have the technology to allow other companies to access their data directly.[24] Under this method, a consumer will give a Fintech application their login credentials for each financial service provider at which they have an account. For example, a consumer might want to use the application Mint to view their total cash balance across the multiple banks at which they have open accounts. The consumer would then give Mint their login credentials for, say, Bank of America and JP Morgan Chase. Mint would then, either directly or through a tool like Plaid, use those credentials to automatically login to the consumer’s online account at each of those banks and “scrape” their account

[19] *Id.* at 23-4.

[20] *Id.* at 25-7.

[21] Thomas P. Brown, *Section 1033 of Dodd-Frank—A Decade of Waiting for the Green Flag to Drop*, available at https://files.consumerfinance.gov/f/documents/cfpb_brown-statement_symposium-consumer-access-financial-records.pdf.

[22] *See* MX Technologies Inc., A List of Financial Data Aggregators in the United States, blog post (Mar. 5, 2018), available at: https://www.mx.com/moneysummit/a-list-of-financial-data-aggregators-in-the-united-states. (listing eight major consumer financial data aggregators in the United States).

[23] Treasury Fintech Report, *supra* note 8, at 26-8.

[24] *See Id.*

balances off of the screens made available through the banks' web portals. With this information, Mint could display the aggregate consumer's aggregate bank account balance.

Screen scraping is an effective method for data aggregators to access data from banks that may not have the resources to build an API, improving the comprehensiveness, and thus the usefulness, of Fintech applications. But it has drawbacks as well and is generally considered a suboptimal solution.[25] Most notably, it requires users to trust small Fintech startups with their login credentials to all of their financial accounts. These startups are then attractive targets for hackers and new sources of vulnerabilities for banks. It can also impose costs on banks as the repeated requests to their web portals needed to refresh the data in these apps will quickly increase their web volume and costs. It's even suboptimal for data aggregators as they need to track any changes that banks make to their web interfaces.

APIs, by contrast, are software packages that allow a data source or other system to interact with or be used by other software.[26] This can be thought of as a direct feed that allows data aggregators and Fintech applications to interact with a financial service firm's data without requiring the consumer to store their login credentials with the new service. APIs allow banks and other data providers to specify with granularity which data fields they are comfortable sharing. They also allow for more robust security features and make related information technology costs easier to predict. Their primary drawback is that they cost money to develop, potentially placing an excessive burden on small financial institutions and creating barriers to entry.[27] By definition, they also require data providers to allow data under their control to be shared, making it easier for banks to shut off access and otherwise exert control over smaller companies that rely on the data provided therein.[28]

Increasing Demands for Regulation

As is often true when regulating financial technology, a bit of history can help explain the stakeholder battle taking place today. Data aggregators have been using screen scraping to accumulate financial data for the past twenty years at least.[29] But, data aggregation and the Fintech ecosystem built on it have begun to grow exponentially in the last decade. By 2015, the industry had grown large enough to draw the ire of the traditional financial institutions it was disrupting.[30] That year, a few large banks tried to shut the industry down and turned off aggregators' access to consumer financial account information.[31] Banks justified this decision by pointing to the security issues created by these applications and the operational costs incurred on their servers from the constant stream of aggregator data

[25] *Id.*

[26] *Id.*

[27] *See* Independent Community Bankers of America, *Docket No. CFPB-2016-0048, Request for Information Regarding Consumer Access to Financial Records*, 6 (Feb. 21, 2017), accessible at https://www.regulations.gov/document?D=CFPB-2016-0048-0035 (hereinafter "ICBA RFI Response").

[28] *See* Plaid Technologies, Written Statement for the Symposium on Consumer Access to Financial Records (Feb. 19, 2020), available at https://files.consumerfinance.gov/f/documents/cfpb_pitts-statement_symposium-consumer-access-financial-records.pdf (hereinafter "Plaid Symposium Statement").

[29] Treasury Fintech Report, *supra* note 8, at n.46.

[30] Brian Hurh et al, *Consumer Financial Data Aggregation & the Potential for Regulatory Intervention*, Davis Wright Tremaine LLP (June 2010), available at https://www.dwt.com/files/paymentlawadvisor/2017/06/Blog_Article_-_Consumer_Financial_Data_Aggregation.pdf.

[31] *See* Robin Sidel, *Big Banks Lock Horns with Personal-Finance Web Portals*, Wall Street Journal (November 4, 2015), available at https://www.wsj.com/articles/big-banks-lock-horns-with-personal-finance-web-portals-1446683450.

requests.[32] But consumer outcry forced banks to reverse course within days, allowing data aggregators to access their data even as the banks sought new ways to limit these requests.[33]

The CFPB entered the scene soon after, expressing concern with the banks' actions. CFPB Director Richard Cordray chastised financial institutions for "looking for ways to limit, or even shut off, access to financial data rather than exploring ways to make sure that such access, once granted, is safe and secure."[34] The CFPB subsequently issued a Request for Information ("RFI") to: (1) help the industry develop best practices to deliver benefits to consumers and address potential consumer harms; and (2) evaluate whether any guidance or future rulemaking is needed.[35] The Bureau followed the RFI with a document maintaining that Section 1033 of the DFA granted consumers the right to give permission to third parties to access their data, but stating that right should be qualified.[36]

Despite these actions, uncertainty persists over fundamental questions and furor for new regulation has grown on all sides. Today, data aggregators and Fintech applications ask the CFPB to use its rulemaking authority under Section 1033 of the DFA to confirm the right to the permissioned access to consumer financial data.[37] Banks ask regulators to subject these new players to the same regulatory scrutiny under which they operate, and to clarify uncertainty over who bears liability for breaches.[38] Commentators on both sides criticize the CFPB's lack of action, arguing that the lack of decisive regulatory action is distorting the market's development.[39] These forces convinced the CFPB to convene the upcoming Symposium on this topic.

Potential Areas for CFPB Action

The various stakeholders at the Symposium have divergent interests and all lay out different paths that the CFPB might take. The regulatory questions the CFPB is facing fall into two main groups: first, whether and how to implement Section 1033 of the DFA; and second, how to apply other preexisting regulations to data aggregation and the new economy for consumer financial data. These two courses of action are not mutually exclusive and either would help increase certainty in this space. The CFPB should assess the merits of all of the options on the table as well as their interrelationships to set a policy platform that expands access to consumer financial data while still protecting consumer privacy and security.

[32] *See* Patrick Dehan, *Banking, Consumer Groups Battle Over Mint.com*, Associations Now (Nov. 16, 2015), available at http://associationsnow.com/2015/11/banking-consumer-groups-battle-mint-com.

[33] Hurh et al, *supra* note 30 at 2.

[34] Prepared Remarks of CFPB Director Richard Cordray at Money 20/20, October 23, 2016, available at https://www.consumerfinance.gov/about-us/newsroom/prepared-remarks-cfpb-director-richard-cordray-money-2020/.

[35] Request for Information Regarding Consumer Access to Financial Records, 81 Fed. Reg. 83606 (Nov. 22, 2016).

[36] CFPB, *Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation* (Oct. 18, 2017), available at https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf.

[37] *See, e.g.*, Plaid Symposium Statement, *supra* note 28.

[38] *See, e.g.*, Statement of PNC Bank, Symposium on Consumer Access to Financial Records, https://files.consumerfinance.gov/f/documents/cfpb_talpas-statement_symposium-consumer-access-financial-records.pdf.

[39] *See* Knight, *supra* note 7, at 3.

New Regulation Pursuant to Section 1033 of the DFA

The ongoing debate regarding a potential rulemaking under Section 1033 of the DFA has coalesced around five issues:

Issue One: Does Section 1033 of the DFA include a right to consumer-permissioned access to data?

An ongoing debate questions whether Section 1033 of the DFA includes a right to consumer-*permissioned* access to financial data, or only a right to *direct* consumer access to financial data. Direct consumer access would only require financial institutions to share data with the consumers directly. Consumer-permissioned access, by contrast, would also force them to share data with other companies designated by the consumer, potentially including their competitors.

Section 1033 of the DFA specifies that "a covered person shall make available *to a consumer*, upon request" (emphasis added), certain data regarding that consumer that the covered person either possesses or controls.[40] Such right is also "subject to rules prescribed by the Bureau." Notably, the definition of "consumer" in Title X of Dodd-Frank includes not only an individual, but "an agent, trustee, or representative acting on behalf of an individual."[41] Notably, one of the drafters of the provision, Professor Michael Barr, has noted that the scope of the provision was "intended to be broad – providing a framework for customer access that would encourage competition and innovation, including through the use of third-party providers and aggregators."[42]

Fintechs believe themselves to be covered by the broad definition of "consumer," obligating covered persons to share permissioned data with them. Traditional financial institutions, on the other hand, note that the plain language of Section 1033 itself only mentions consumers, that the broad language in the definition's section does not appear to contemplate forcing companies to give valuable data to their competitors, and that Congress could very easily have expanded the provision to create this right.[43]

Following the 2017 RFI, the CFPB issued the Consumer Protection Principles, which touch on this question. That document states that consumers are "able to authorize trusted third parties to obtain such information…to use on behalf of consumers."[44] Still, the debate persists. In a recent case, PNC used the arguments outlined above to deny Venmo access to consumer data despite consumer requests that the data be transferred.[45] Commentators have thus argued that the CFPB should create a rule to resolve the issue and clarify the rights of third parties to consumer-permissioned access to financial data.[46] Such a

[40] 12 U.S.C. §5533 (2010).

[41] 12 U.S.C. §5481(4) (2010).

[42] Michael Barr et al, Consumer Autonomy and Pathways to Portability in Banking and Financial Services, University of Michigan Center on Finance, Law and Policy 4 (November 3, 2019), available at http://financelawpolicy.umich.edu/files/umich-cflp-working-paper-consumer-autonomy-and-data-portability-pathways-Nov-3.pdf.

[43] *See, e.g.*, ICBA RFI Response, *supra* note 27.

[44] Consumer Protection Principles, *supra* note 36, at 3.

[45] Kate Rooney, *PNC's fight with Venmo highlights bigger issue over who owns your banking data,* CNBC (Dec. 16, 2019), available at https://www.cnbc.com/2019/12/16/venmo-and-pncs-fight-over-sharing-consumer-financial-data.html.

[46] *See* Knight, *supra* note 1, at 3.

rule would also be an opportunity for the CFPB to regulate the means of obtaining consent, the limits of consented sharing of information, and other open policy debates.[47]

- Should the CFPB engage in a rulemaking process to clarify the existence of a right to consumer-permissioned access to data in Section 1033 of the DFA?
- Does the CFPB face legal risk in passing a rule that specifies a right for consumer-permissioned access to data? Could such a rule be struck down for exceeding the CFPB's statutory mandate?

Issue Two: Should the CFPB limit the power of consumers to grant third parties permissioned access to their financial data?

Assuming that consumers have a right to the permissioned sharing of their data, various stakeholders disagree over the appropriate limitations that the CFPB should impose on that right.

Fintechs argue that consumer autonomy is best supported by a broad consumer right to consent to the sharing of data, subject to disclosure requirements and the right to revoke consent.[48] Requiring consumers to jump through added hoops to share their data is an inherent limit on consumer choice and autonomy. Further, empirical evidence shows that consumers appear to value convenience and a smooth user experience in most transactions over added privacy protections.[49] Consumers are then better served by full disclosure and a continuing ability to revoke their consent, such an option encourages transparency and gives those who are privacy-conscious the ability to exercise choice.

Privacy advocates, on the other hand, argue that the ability to consent should be subject to inherent limits.[50] Proposed limits include a mandatory period after which consent expires requiring it be granted again, and limits on the number of data fields or data uses that may be consented to at once.[51] Their argument comes out of two concerns. First, consent may be insufficient to safeguard consumer privacy.[52] Even if the disclosure is provided, Fintechs and data aggregators potentially have an incentive to obfuscate them. As such, consumers are unlikely to fully appreciate what data they are sharing, with whom it is shared, and how that data may be used. Access may also last longer than expected by a consumer who only intended it for a one-time transaction.[53] Second, consumer consent may only represent a limited act of autonomy. Structural power imbalances between data subjects and data controllers mean that consumer consent does not always mean consumer choice.[54] Consent provisions are included as non-negotiable terms in contracts of adhesion, in which the average consumer does not have the capacity or the competency to change. If general consent is an option, it will then become the

[47] Another ongoing debate concerns whether or not Section 1033 of the DFA is self-executing. If it is self-executing, then consumers already enjoy the rights mentioned in the statute, even absent a CFPB rulemaking. If not, then financial institutions do not have enforceable obligations under this section absent CFPB action. This question is relevant if a new administration wants to enforce this right before rulemaking is complete. Notably, the CFPB announced that Section 1071 of the DFA, which has some similar language to Section 1033, is not self-executing.

[48] *See, e.g.*, Plaid Technologies, *Plaid response to CFPB regarding Consumer Access to Financial Records Docket No. CFPB-2016-0048*, 1-2 (Feb. 21, 2017), accessible at https://www.regulations.gov/document?D=CFPB-2016-0048-0058.

[49] *See* Alessandro Acquisti and Jens Grossklags, *Privacy and Rationality in Decision Making*, 3(1) IEEE, Security and Privacy Magazine 26-33 (Jan. 2005), accessible at https://www.heinz.cmu.edu/~acquisti/papers/acquisti.pdf.

[50] *See, e.g.*, NCLC Symposium Statement, *supra* note 10, at 4-5.

[51] *Id.*

[52] *See generally* Daniel Solove, *Privacy Self-Management and the Consent Dilemma*, 126 Harvard Law Review 1880 (2013), accessible at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2171018.

[53] NCLC Symposium Statement, *supra* note 10, at 4-5.

[54] *See* Rhoen, *supra* note 15.

norm. The mandated parsing of consumer consent, whether by time, data field, etc., gives consumers more effective opportunities to exercise choice.

- Should the CFPB impose limits on the power of consumers to grant permissioned access to their data?
- If yes, what forms of limitations would be appropriate?
  - **Time bounds**. Should permissioned access be time limited, requiring periodic renewal for continued access? Should consent be self-expiring, requiring Fintechs to renew consent or delete a consumer's permissioned data after a set period?
  - **Use.** Should consumers be able to provide access to data for general use or without specifying a use?
  - **Permissioned data fields**. Should consumers be able to grant a Fintech permission to access all of their data held by another entity? Or should consumers need to consent to the sharing of individual data elements? What if the data transfer involves transferring a relationship to a new service provider (e.g. switching banks)?
  - Other?

Issue Three: Can banks deny an entity's access to financial data in spite of a proper consumer request?

Returning to the text of Section 1033 of DFA, the CFPB will also need to grapple with the limits of which third parties properly qualify as an "agent, trustee, or representative acting on behalf of an individual." Most parties agree that the ability of a consumer to grant permission to a third party is not unlimited. Financial institutions should have some latitude to ensure that their clients' data is not transferred to untrustworthy providers. For example, it seems logical that they should be able to condition access on adequate security measures being in place. In their previous statements on this topic, the CFPB alluded to this limitation and specified that permissioned access should occur "in a safe manner."[55]

At the same time, Fintech startups and data aggregators complain that financial institutions are likely to abuse this kind of discretion.[56] As a result of their size, financial institutions often enjoy a bargaining advantage relative to small Fintech startups. These kinds of discretionary rights to revoke access exacerbate that issue and give financial institutions leverage in any negotiations. Some financial institutions also use this kind of logic as a shield to deny properly permissioned access to Fintech applications and evade the spirit of Section 1033.[57] Determining the shape of any such discretionary right will have a major impact on any potential rule.

- Should financial service providers be able to decline transfers to certain parties despite customer consent (e.g. if they find that a company has insufficient security protocols in place to protect the transferred data)? If so, who gets to determine the criteria for disqualification:
  - Individual financial institutions?
  - A self-regulatory organization or other industry-level group?

[55] Consumer Protection Principles, *supra* note 36, at 3.

[56] *See, e.g.*, Plaid Symposium Statement, *supra* note 28.

[57] *See, e.g.,* PNC's fight with Venmo, *supra* note 40.

- The CFPB (through rulemaking, guidance, etc.)?
- A hybrid approach?

Issue Four: What type of data must be shared?

Section 1033 of the DFA states that covered persons must provide access to "information in the control or possession of the covered person concerning the consumer financial product or service that the consumer obtained from such covered person, including information relating to any transaction, series of transactions, or to the account including costs, charges and usage data."[58] The scope of the data that must be provided is further limited by several exceptions, including one that provides that covered persons need not share "any confidential commercial information, including an algorithm used to derive credit scores or other risk scores or predictors."[59]

Regulators in other countries have conceptualized consumer data as falling into three categories: volunteered, observed, and inferred.[60] Volunteered data includes information that is readily and knowingly provided by the consumer to the service provider, e.g. one might share their social security number when setting up an account. Observed data includes data that is passively collected by the service provider over the course of a relationship, such as a lender tracking whether you prefer to pay your monthly bill through their website or mobile application. Finally, inferred or derived data covers any information generated about you using those other data points, such as a credit score.[61]

The plain language of the statute appears to leave ambiguous whether or not all three of these types of data must be shared upon request. Volunteered, observed, or inferred data may all "concern" the product or service that a bank provides to a customer. The exception for confidential commercial information also notably mentions the algorithms used to generate risk scores, but not the risk scores themselves. The National Consumer Law Center ("NCLC") in particular has argued that the CFPB should interpret this language to allow consumers access to any credit score data that a financial institution may have in its possession.[62]

Such a measure would almost certainly be opposed by financial institutions. They are likely to consider inferred information to be proprietary, even if it does not rise to the same level of confidentiality as the algorithm used to determine a credit score. Such data also seems at odds with the volunteered data listed in the first paragraph of Section 1033 of the DFA ("costs, charges, and usage data"). In foreign contexts, academics have also questioned whether such a right to inferred information is a privacy-oriented overreach that limits innovation and competitiveness objectives of data access rules.[63] The CFPB will need to provide clarity on the scope of the data fields that a consumer may request.

[58] 12 U.S.C. §5533 (2010).

[59] *Id.*

[60] *See* Article 29 Data Prot. Working Party, Guidelines on the Right to Data Portability, 16/EN WP242 at 10 (April 5, 2017) available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233.

[61] *Id.*

[62] National Consumer Law Center, *Comments in Response to Requests for Information: Consumer Access to Financial Records, Docket No. CFPB-2016-0048*, 7 (Feb. 21, 2017), accessible at https://www.regulations.gov/document?D=CFPB-2016-0048-0072 (hereinafter "NCLC RFI Response).

[63] Paul De Hert, Vagelis Papakonstantinou, Gianclaudio Malgieri, Laurent Beslay & Ignacio Sanchez, *The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services*, COMPUTER L. & SECURITY REV. 193 (2018).

- Does the statutory text of Section 1033 of the DFA indicate whether consumers may access observed and/or inferred data regarding the consumer under their financial service provider's control?
- Specifically regarding inferred data, if the text is ambiguous, what stance should the CFPB take?
    - Should the CFPB prescribe a regulatory right to access some or all kinds of inferred data?
    - Should the CFPB explicitly exclude some or all kinds of inferred data from the scope of Section 1033 of the DFA?
    - Should the CFPB remain silent on this issue for the time being?

Issue Five: To what extent should the CFPB regulate the method of transfer and try to move the industry away from screen-scraping?

As discussed above, there is near-universal acknowledgement among industry stakeholders that screen-scraping is a risky and suboptimal practice, and that APIs are a safer, more reliable method that also allow consumers more control over how their data is shared.[64] Recognizing these arguments, a number of foreign jurisdictions have taken affirmative steps to promote the use of APIs for the transmission of consumer financial data.[65] With its open banking initiative, the United Kingdom mandated that the largest banks in the country had to establish APIs and provided an opt in regime for smaller banks to join the program. The European Union adopted the Revised Payment Service Directive, requiring banks to give licensed parties access to account data. It did not mandate the use of APIs, but encouraged their use and provided standards to make APIs more interoperable where implemented. Singapore has also issued guidance encouraging the use of bank APIs but has not made any regulatory mandate on the subject.[66]

Industry efforts in the US to move toward greater API use have had little success outside of the largest financial institutions.[67] Part of this reflects a general reluctance on the part of financial institutions to make it easier for consumers to shift their business to other companies. At the same time, there has been concerted opposition from small and mid-sized banks who do not want to take on the added burdens of implementing this technology.[68] Any mandate to adopt the technology would need to account for their needs and take affirmative steps to prevent this requirement from becoming a barrier to entry for new banks.

The CFPB has rulemaking authority under Section 1033 of the DFA to "prescribe standards applicable to covered persons to promote the development and use of standardized formats for information…"[69] The CFPB should explore whether or not it should use this authority to follow the lead of other countries to resolve the industry logjam in this area.

[64] Treasury Fintech Report, *supra* note 8, at 34-5.

[65] *Id.*

[66] *Id.*

[67] Fidelity Investments, *Request for Information Regarding Consumer Access to Financial Records; Docket No. CFPB-2016-0048*, 6-8 (Feb. 21, 2017), available at https://www.regulations.gov/document?D=CFPB-2016-0048-0053.

[68] ICBA RFI Response, *supra* note 27, at 7.

[69] 12 U.S.C. §5533 (2010).

- Should the CFPB take any steps to encourage API adoption and discourage the use of screen-scraping?
    - Should the CFPB provide any regulatory mandate for the use of APIs (e.g. through rulemaking)? If so, should it be targeted at only large banks and should there be any relief to help smaller banks adopt the technology?
    - Should the CFPB provide regulatory guidance to encourage and standardize API implementation?
    - Should the CFPB take a more conservative approach and wait to see how other changes impact the direction of the industry on this point?

Applying Existing Regulations to Data Aggregation

The above issues relate to Section 1033 of the DFA and how the CFPB should implement it. Regardless of the approach taken on that topic, regulators will need to also grapple with how to apply existing regulations to data aggregators, Fintech startups, and other new participants in the financial sector. In general, these new players have resisted the application of existing financial regulatory regimes. Financial institutions, meanwhile, claim that the underenforcement of existing regulation is allowing Fintechs to practice a form of regulatory arbitrage and that they should be brought under the same regulatory umbrella.[70]

Fair Credit Reporting Act ("FCRA")

The FCRA is one of the other pieces of the patchwork of privacy regulations that apply to the US financial sector.[71] Among other things, the FCRA gives consumers access to the data in their consumer reports, gives them the opportunity to restrict the use of those reports, and requires financial institutions to conduct reasonable investigations if a consumer disputes the accuracy of the information therein.[72]

Crucially, the FCRA is the primary tool that provides American consumers with a right to rectify incorrect data that is being used to judge their creditworthiness.[73] This right is arguably even more important in the context of Fintech applications. Screen scraping and other suspect data gathering techniques make alternative data more likely to be inaccurate than traditional data.[74] The CFPB's post-RFI statements also stressed the importance of accuracy as one of their key principles in protecting consumers in the new data sharing economy, stating that consumers should have a reasonable expectation that the data regarding them is accurate and that they'll have a meaningful opportunity to dispute inaccuracies.[75]

[70] *See, e.g.*, ABA RFI Response, *supra* note 11.

[71] For a general summary of the rights contained within this statute, see the Federal Trade Commission's *A Summary of Your Rights Under the Fair Credit Reporting Act*, accessible at https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.

[72] *See* Regulation V, 12 C.F.R. § 1022 https://www.consumerfinance.gov/policy-compliance/rulemaking/regulations/1022/1/ (hereinafter "Reg V").

[73] Carlo Kostka and Sam Adriance, *The Effects of GDPR on U.S. Financial Institutions*, Covington and Burling (blog post), available at https://www.cov.com/-/media/files/corporate/publications/2018/08/the_effects_of_gdpr_on_us_financial_institutions.pdf.

[74] NCLC Symposium Statement, *supra* note 10.

[75] Consumer Protection Principles, *supra* note 36.

As a legal matter, there has been an ongoing debate over whether or not data aggregators fall under the FCRA's regulatory boundaries.[76] The FCRA's primary obligations are imposed on "consumer reporting agencies." A consumer reporting agency is any person that regularly assembles or evaluates consumer credit information for the purposes of providing consumer reports. A consumer report is defined as any information that relates to an individual's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, and mode of living, or that is otherwise collected to be used in assessing someone's eligibility for credit.[77] By these terms, a consumer report encompasses broad categories of information that are not limited to credit-based data. Consumer advocacy groups point to the apparent breadth of this language and the important policy goals advanced by the statute to argue that it should apply to Plaid and other data aggregators in the new financial ecosystem.[78]

However, many data aggregators continue to argue that they should not be subject to the FCRA's requirements.[79] One of their main arguments rests on the requirement that a consumer reporting agency "regularly engage[]… in the practice of *assembling or evaluating* [consumer reports] (emphasis added)."[80] The Federal Trade Commission, which had regulatory authority over this statute before the establishment of the CFPB, has interpreted this language relatively narrowly. It defined "assembling" to mean "gathering, collecting, or bringing together consumer information such as data obtained from CRAs or other third parties, or items provided by the consumer in an application."[81] On the other hand, "evaluating" means "appraising, assessing, determining or making a judgment on such information."[82]

Some data aggregators, including Plaid, have argued that they do neither and merely function as a "pipe" for data.[83] In this telling, the aggregator is merely a piece of software that serves as a data conduit, allowing Fintechs themselves to assemble and evaluate data from financial institutions. The Ninth Circuit found a similar argument persuasive in *Zabriskie v. Federal National Mortgage Association*, holding that Fannie Mae was not a consumer reporting agency because it merely provided a software tool that allowed mortgage lenders to assemble or evaluate consumer information themselves.[84] On the other hand, a few aggregators, including Finicity, feel that their activities constitute more than functioning as a conduit and have already registered as consumer reporting agencies.[85] Consumer groups argue that most, if not all, aggregators fall into this latter category and differences in the business models of Plaid and Finicity do not justify different treatment.[86] Resolution of this debate will significantly impact the coverage of the rights in the FCRA.

[76] NCLC Symposium Statement, *supra* note 10.

[77] Reg V, *supra* note 71, at § 1022.130(c)-(d).

[78] NCLC Symposium Statement, *supra* note 10, at 6-9.

[79] *See, e.g.*, John Pitts, *Statement before the Senate Committee on Banking, Housing and Urban Affairs* (Mar. 15, 2019), accessible at https://www.banking.senate.gov/imo/media/doc/Data%20Submission_Plaid1.pdf.

[80] Federal Trade Commission, *40 Years of Experience with the Fair Credit Reporting Act: An FTC Staff Report with Summary of Interpretations* 29, July 2011, https://www.ftc.gov/sites/default/files/documents/reports/40-years-experience-fair-credit-reporting- act-ftc-staff-report-summary-interpretations/110720fcrareport.pdf.

[81] *Id.*

[82] *Id.*

[83] *See* NCLC Symposium Statement, *supra* note 10, at 8.

[84] 912 F.3d 1192 (9th Cir. 2019).

[85] *See* Finicity, *Consumer Reporting Agency*, accessible at https://www.finicity.com/consumer-reporting-agency/.

[86] *See* NCLC Symposium Statement, *supra* note 10, at 8.

If data aggregators are determined to be consumer reporting agencies, a secondary debate asks whether or not all of their sources of data then become data furnishers under the FCRA. A data furnisher is an entity that furnishes information relating to consumers to one or more consumer reporting agencies for provision in a consumer report.[87] The FCRA imposes various obligations on these entities including avoiding the transmission of data it suspects may be incorrect. Again, consumer advocates point to the apparent breadth of the language and need for consumer protections to argue for a broad application of this language.[88] However, other groups have argued that the term furnish requires an "affirmative undertaking to provide information."[89] If data is collected from a financial institution via screen scraping, that financial institution arguably does not "furnish" the data to the aggregator. On a more hotly contested point, some financial institutions argue that providing an API is a passive activity that does not constitute furnishing. An API is merely a piece of software that allows external systems to interact with a group's software in clearly defined ways. It defines calls and requests that external users can make to a company's systems and may be available on an open or permissioned basis. Under such a system, the data recipient simply inputs a command which is automatically fulfilled by the data source. In the case of public APIs, a consumer reporting agency may draw data from a source without directly contacting employees. Whether or not this constitutes "furnishing" will also significantly impact the scope of the FCRA going forward.

- Are data aggregators consumer reporting agencies under FCRA?
- Is a financial institution a data furnisher if it provides an API through which aggregators access data?

Electronic Funds Transfer Act ("EFTA")

Screen-scraping has created a string of liability disputes between financial services companies and new Fintech startups. Data aggregators and downstream Fintech applications may both store consumer account credentials in order to gather consumer financial data absent an API. If those providers experience a data breach, the hackers may then use those credentials to log into the impacted consumer's financial accounts and conduct fraudulent transactions.[90] There is an ongoing legal dispute regarding whether the EFTA and Reg E obligate the financial institution, the Fintech, or neither, as responsible to repay the consumer for the unauthorized transaction under these circumstances.

Banks strongly maintain that they are not liable under Reg E for any losses that result in this manner.[91] Under Reg E, an "unauthorized transfer" does not include transactions performed by a person furnished with an "access device" by the consumer.[92] Under the banks' reading, a consumer furnishes an access device to a data aggregator when they provide them with account credentials and thus the

[87] Reg V, *supra* note 71, at § 1022.41(c).

[88] *See* NCLC Symposium Statement, *supra* note 10, at 8.

[89] Kwamina Williford and Brian Goodrich, Why Data Sources Aren't Furnishers Under Credit Report Regs, HK Law (blog post Sep. 25, 2019), available at https://www.hklaw.com/-/media/files/insights/publications/2019/09/whydatasourcesarentfurnishersundercreditreportregs.pdf?la=en.

[90] Treasury Fintech Report, *supra* note 8, at 35-6.

[91] *See, e.g.*, ABA RFI Response, *supra* note 11.

[92] Regulation E, 12 C.F.R. § 1005, available at https://www.consumerfinance.gov/policy-compliance/rulemaking/regulations/1005/14/#14-b-Interp-1.

transaction is not an unauthorized transaction at all.[93] Banks thus have no liability and if a data aggregator is unable or unwilling to compensate the consumer, the consumer suffers the loss.[94] Several banks have started including disclosures to this effect in their terms of service, partially as a method to dissuade their users from giving their credentials to Fintech applications.[95]

Consumer groups, on the other hand, strongly contest this argument. They argue that even if the account credentials constitute an access device, the consumer does not furnish it to the party that makes the transaction.[96] Even if the consumer furnishes this information to a data aggregator and that data aggregator then experiences a breach, one could not reasonably claim that the consumer furnished the access device to the hacker. They further argue that, as a policy matter, it's difficult to trace the origins of unauthorized charges and it will often be difficult to establish fault under these circumstances.

These arguments are compelling but, as a policy matter, there is also force to the banks' claim. It appears unfair to force them to share consumer account data with third parties, then be penalized if that data is breached if those same parties underinvest in security. Reducing the use of screen-scraping, increasing the data security obligations of Fintechs, or providing for some liability sharing could all help resolve this issue. The CFPB should clarify this ongoing legal dispute and provide policy guidance to ensure that all parties are properly incentivized to protect consumer financial data and that consumers have adequate means to seek relief if and when unauthorized transactions occur.[97]

- As a legal matter, do banks remain liable under the Reg E for unauthorized charges made in their systems that result from a consumer data breach at a Fintech company?
- As a policy matter, how should liability be apportioned between Fintechs and traditional financial institutions in such cases?
    - Should the two parties be jointly liable?
    - Should the apportionment depend on the respective fault of the parties?
    - If the Fintech alone should be liable, should the consumer still be able to bring a claim for reimbursement through their bank? Would the bank be liable to pay the claim in the first instance with a right to recover against the Fintech or should the bank not be forced to pay at all?

[93] ABA RFI Response, *supra* note 11, at 9.

[94] *Id.*

[95] NCLC RFI Response, *supra* note 62.

[96] *Id.*

[97] *Id.*

Research Note on Financial Data Protection and Consumer Privacy in the United States[*]

NAFISA ADAMA

The United States (U.S.) does not have a single overarching data protection law. Instead, separate sector-specific data protection laws have been enacted to regulate the use of data and consumer information in limited contexts. This memorandum provides background to the primary data protection laws applicable in the U.S. financial services industry and draws a distinction with comparable legislation in other jurisdictions, such as the General Data Protection Regulation (GDPR) in the European Union and the European Economic Area. It also discusses the key features of the recently enacted California Consumer Protection Act and the ensuing deliberations on the adequacy of the existing U.S. financial data protection and consumer privacy legal framework.

The Gramm-Leach-Bliley Act

At the federal statutory level, the main legislation that protects consumers' personal financial data, albeit in a limited fashion, is the Gramm-Leach-Bliley Act (GLBA), also known as the Financial Services Modernization Act, enacted in 1999. A crucial aspect of the GLBA is the Title V which makes provisions for financial privacy protection. The safeguards provided under the GLBA can be broken down into the following:

- Safe storage and sharing of consumer confidential information with affiliated third parties;
- Provision of privacy notices to consumers; and
- Securing consumer confidential information from unauthorized third-party access.

The GLBA imposes several obligations on financial institutions—companies that offer consumers financial products or services like loans, financial or investment advice, or insurance—regarding the handling or storing of what it terms "consumer nonpublic personal information."[98] This subjects all information personal to the consumer such as their names, home addresses, social security numbers, or any additional information that a financial institution requires to provide financial services or sell a product to the data sharing restrictions of the GLBA. The GLBA places limited obligations on affiliated third parties that have received nonpublic personal information from GLBA regulated financial institutions. In the absence of an applicable exception, financial institutions are prohibited from sharing nonpublic personal information with non-affiliated parties unless consumers are first issued a notice containing the privacy policy of the financial institution with an opportunity to "opt-out."[99] The notice is issued only when an individual first becomes a customer of the bank and then annually thereafter. Each opt-out notice to a consumer must be clear, conspicuous, and provide a reasonable means to exercise the opt-out right, such as through designated check boxes or providing a toll-free telephone number that

[*] Optional reading. Prepared by Nafisa Adama, HLS LLM 2020, June 3, 2020.

[98] A "consumer" under the GLBA is an "individual who obtains, from a financial institution, financial products or services which are to be used primarily for personal, family, or household purposes" or "the legal representative of such an individual." 15 U.S.C. § 6809(9). 70. "Nonpublic personal information" is defined as "personally identifiable financial information — provided by a consumer to a financial institution; resulting from any transaction with the consumer or any service performed for the consumer; or otherwise obtained by the financial institution."

[99] § 6802; 12 C.F.R. § 1016.10(a).

consumers may call to opt-out.[100] Even though the GLBA specifies the type of information to be contained in the privacy notices,[101] the exact language of the notice is left to be determined by the financial institution thereby giving them some leeway to decide on the complexity and transparency of language in a manner that best serves their interests. It is no wonder why most privacy policies are considered convoluted, technical, and difficult to understand, further diminishing the power of the consumer to effectively control how their information is shared. Notably, the GLBA takes away from the consumer the power to control the sharing of their information among affiliate companies of the financial institutions. As such, the opt-out right is inapplicable in affiliate information sharing scenarios and this presents the risk of information being collected by an indeterminable number of affiliated companies who may even be non-financial institutions.

Even though the opt-out strategy gives the consumer the opportunity to permit or object to the sharing of their information with unauthorized parties, financial institutions will not be bound by the requirements for notification and the consumer's exercise of opt-out rights where they disclose nonpublic personal information:

- to nonaffiliated third-party service providers, such as promoters of the financial institution's own products, provided that such nonaffiliated third parties are contractually bound to maintain the confidentiality of the consumer's information.[102]
- to service or process transactions requested by the consumer.[103]
    - to protect the confidentiality or security of their records on the consumer, service, product, or transaction; (ii) to protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability; (iii) for required institutional risk control or for resolving consumer disputes or inquiries; (iv) to persons holding a legal or beneficial interest relating to the consumer; or (v) to persons acting in a fiduciary or representative capacity on behalf of the consumer.[104]
- to provide information to applicable rating agencies, the institution's attorney's accountants, auditors, and other organizations assessing the financial institution's compliance with industry standards.[105]
- to law enforcement agencies, self-regulatory organizations, or in connection with an investigation on a matter of public safety.[106]
- to a consumer reporting agency in accordance with the Fair Credit Reporting Act (FCRA) or from a consumer report by a consumer reporting agency.[107]

[100] 12 C.F.R. § 1016.7(a)).

[101] The notices must include, among other things, the categories of information collected and disclosed, the categories of third parties with which the financial institution shares information, and policies and practices with respect to protecting the confidentiality and security of the information. *Id. § 1016.6(a)).*

[102] 15 U.S.C. § 6802(b)(2); 12 C.F.R. § 1016.13.

[103] 15 U.S.C. § 6802(e); 12 C.F.R. § 1016.14.

[104] 15 U.S.C. § 6802(e)(3)(A); 12 C.F.R. § 1016.15(a)(2)).

[105] 15 U.S.C. § 6802(4); 12 C.F.R. § 1016.15(a)(3)).

[106] 15 U.S.C. § 6802(5); 12 C.F.R. § 1016.15(a)(4)).

[107] 15 U.S.C. § 6802(6)(A) - (B); 12 C.F.R. § 1016.15(a)(5)(i)-(ii)).

- in connection with the sale, transfer, or merger of all or a portion of the institution's business or operating unit, where the disclosure relates solely to the nonpublic personal information of consumers of that business or unit.[108]
- to comply with all legal requirements including federal state and local laws, subpoenas, summons, judicial processes or government regulatory authorities having jurisdiction over them.[109]

Part of the enforcement framework of the GLBA is the Safeguards Rule 110 issued by the Federal Trade Commission (FTC). Together, the GLBA and the Safeguards Rule require all financial institutions under FTC jurisdiction to ensure the security and confidentiality of customers'[111] (as opposed to consumers as with the disclosure requirements) information. In implementing this provision, the law requires that the financial institutions put in place "administrative, technical, and physical safeguards" to secure the customers' information against "any anticipated threats or hazards" or "unauthorized access" to such information.[112] In this regard, the law anticipates the development and implementation of an "information security program" that contains safeguards that are suitable to the "size and complexity, the nature and scope" of the company's activities as well as the "sensitivity of the customer information".[113] Finally, the companies must, in maintaining the information security system, among other things, designate an information security program coordinator, put in place a risk assessment process, and regularly monitor the effectiveness of the safeguards procedure.[114] Regulatory authorities such as the Securities and Exchange Commission as well as the federal banking agencies impose other supervisory standards with respect to cybersecurity safeguards at regulated firms, which provides additional protections for consumer data.[115]

The California Consumer Privacy Act

Effective January 2020, the California Consumer Privacy Act (CCPA), compared to title V of the GLBA, provides a much more extensive and comprehensive framework for the protection of consumer's personal information, despite being state law. The CCPA does not restrict its application to any industry in particular but rather applies to all companies that collect the personal information of Californians – provided the company is a for-profit, carries on business activities in California, and qualifies as a CCPA covered business., e.g., any company with more than $25 million in annual gross revenues, or that engages in the buying, selling, or receipt of the personal information of 50,000 or more California residents, or that

[108] 15 U.S.C. § 6802(7); 12 C.F.R. § 1016.15(a)(6)).

[109] 15 U.S.C. § 6802(8); 12 C.F.R. § 1016.15(a)(7)).

[110] *See*, e.g., Financial Institutions and Customer Information: Complying with the Safeguards Rule, Federal Trade Commission (Apr. 2006), available at https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying.

[111] Customer is defined as someone who has a continuing relationship with the financial institution, such as someone who has obtained a loan or who has opened a credit or investment account. 16 C.F.R. § 313.3(h)–(i); see also 12 C.F.R. § 1016.3 (i)–(j)).

[112] 15 U.S.C. § 6801(a) – (b)).

[113] 16 C.F.R. § 314.3.

[114] 16 C.F.R. § 314.4.

[115] *See* Brian Neil Hoffman, Romaine Marshall And Matt Sorensen, Federal and State Cybersecurity Regulation of Financial Services Firms, Law Journal Newsletters, June 2017, available at http://www.lawjournalnewsletters.com/sites/lawjournalnewsletters/2017/06/01/federal-and-state-cybersecurity-regulation-of-financial-services-firms/. *Also see* Cybersecurity regulation and best practice in the U.S. and UK, Lexis Nexis, available at https://www.lw.com/thoughtLeadership/Cybersecurity-regulation-and-best-practice.

derives more than 50% of its annual revenues from the sale of California residents' personal information.[116] Accordingly, the CCPA may be enforced against all companies (including affiliates and subsidiaries) that fit these criteria, irrespective of the industry or location. It has been suggested that these thresholds have been set in such a way that it is easily fulfilled by even small to medium businesses, who merely collect personal data (IP addresses, cookie IDs, etc.) through a website accessible by California residents.[117] It is instructive to note that even though the CCPA provides a partial carve-out for financial institutions concerning information collected pursuant to the GLBA,[118] financial institutions whose activities go beyond the scope of the GLBA and fit within the business threshold will still need to comply with the provisions of the CCPA as it relates to data collection activities not governed by the GLBA.[119] Therefore, all personal information not covered by the GLBA and collected by financial institutions that qualify as a business will now be subject to the CCPA. This is also enabled by the fact that the GLBA does not exempt regulated entities from complying with data and privacy issues not covered under the GLBA.[120]

The CCPA defines "personal information" just as broadly as it defines businesses. Unlike the GLBA, which implies specific personal identifiers, the CCPA broadly construes personal information to include, with the exception of publicly available information[121] and "de-identified" or "aggregate consumer information,"[122] all information of California residents that "identifies, relates to, describes, or is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household".[123] This applies regardless of how the collection is done or the type of industry in which the business operates. In fact, the CCPA illustrates further that personal information can include "electronic network activity such as browsing or search history, and information regarding a consumer's interaction with an internet website, application, or advertisement" and "inferences drawn from any of" this information.[124]

The CCPA regime affords California consumers three primary "rights" with respect to the disclosure of their personal information.

The Right to Know/Disclosure of Personal Information. As the name implies, the California based consumer has the right to know all information collected, stored, and/or shared about them. Accordingly, the CCPA requires that a business must, in advance of collecting a consumer's personal information, inform the consumer (via mail or electronically) the categories of personal information to be collected and purposes for which such information will be used.[125] This is similar to the privacy notice under the

[116] CAL CIV. CODE § 1798.140(c)(1)).

[117] *See,* Christopher A. Ott, Q&A: Privacy and Security Partner Christopher Ott on the California Consumer Privacy Act of 2018, Davis Wright Tremaine LLP Privacy & Security Law Blog, August 6, 2018, available at https://www.dwt.com/blogs/privacy--security-law-blog/2018/08/qa-privacy-and-security-partner-christopher-ott-on.

[118] CAL CIV. CODE § 1798.145(e)).

[119] *See,* Mathews, Fleisher & Foester, Financial Institutions and the CCPA: What Remains After the Law's Exceptions, Bloomberg Law, Available at https://media2.mofo.com/documents/191025-financial-institutions-ccpa.pdf.

[120] 15 U.S.C. § 6807.

[121] CAL CIV. CODE § 1798.140(o)(2)).

[122] *Id. Also see,* CAL CIV. CODE § 1798.145(a)(5)).

[123] CAL CIV. CODE § 1798.140(O)(1)).

[124] *Id.* § 1798.140(O)(1)(A)–(K)).

[125] CAL CIV. CODE § 1798.100.

GLBA regime, except the latter does not burden financial institutions with the responsibility of disclosing the specific usages for collected information. This presumably gives the CCPA an edge over the GLBA, especially in terms of transparency of privacy policies. Predictably, GLBA regulated financial institutions will need to change their privacy policies and data protection mechanisms in order to fulfill the more stringent compliance requirements of the CCPA.

The Right to Opt-Out of Sale of Personal Information. Under the CCPA, the consumer shall have the power to restrict the sale of their information by expressly exercising the right to opt out of such sale by the business. In this regard, the CCPA mandates the business to inform consumers of their right to opt-out, after which the business shall be barred from selling such consumer's information until such a time when the consumer provides express authorization for sale.[126] This provision of the CCPA supplements the GLBA, as it allows the consumer to retroactively direct the business on the sale of its information or otherwise and, in this regard, the law requires the business to act promptly. This strengthens the consumer's ability to retain control over the use of their information to a considerable extent.

Right to Request Deletion of Personal Information. Lastly, under the CCPA, the consumer enjoys the right to have previously collected information deleted or forgotten by the business and the latter must, at the time of collection, disclose this right to the consumer.[127] Once a consumer makes such a request, the business and its service providers are obligated to proceed and delete such information. The GLBA does not accord the consumer the right to request the deletion of their information. Any opt-out directives or request to delete the information by the consumer will not be complied with when the disclosure of the information is necessary to detect illegal activity, to comply with legal obligations, or to perform contracts between the business and the consumer. This is reflective of the exceptions under the GLBA where financial institutions may disclose consumer information without prior authorization. Also worthy of note is the fact that the CCPA makes provision for additional anti-discrimination safeguards of consumers' data which goes beyond the scope of the GLBA. Accordingly, businesses handling consumer data shall not discriminate against consumers based on rights exercised within the confines of the CCPA.[128] Therefore, all consumers of CCPA covered businesses must be treated fairly in a manner that does not indict the good-faith practices of the businesses.[129]

The CCPA is enforced by the Attorney General of California who also has the power to impose non-compliance fines. In addition, and unlike the GLBA, the CCPA provides consumers with a private right of action concerning data breaches such as unauthorized access, theft, and/or disclosure of certain types of personal information including the right to seek statutory damages.[130] Although the CCPA goes well beyond the requirements of the GLBA, the GLBA, as amended, explicitly provides that states may provide greater privacy protections.[131]

[126] CAL CIV. CODE § 1798.120.

[127] CAL CIV. CODE § 1798.105.

[128] CAL CIV. CODE § 1798.125.

[129] *See,* Cynthia J. Larose, Analysis of Modified Attorney General Regulations to CCPA – Part 5: Discriminatory Practices and Financial Incentives, February 21, 2020, available at https://www.natlawreview.com/article/analysis-modified-attorney-general-regulations-to-ccpa-part-5-discriminatory.

[130] Cal. Civ. Code § 1798.150(a) (as amended by Assembly Bill 1355 effective October 11, 2019)).

[131] *See* 15 U.S.C. § 6807:

Since the passage of CCPA, some analysts have questioned whether a federal privacy law should be enacted and include new preemption provisions with respect to state privacy.[132] Calls have been made in Congress and both Republicans and Democrats have explored a comprehensive federal data privacy law that would not only serve as a national-wide privacy law in the U.S., but also would preempt to a considerable extent the application of inconsistent provisions of state privacy laws. These efforts have, however, remained stalled as there is a divergence of opinion with respect to state preemption, amongst other issues. On the one hand, it is argued that without the preemption of state laws, businesses and consumers will suffer due to the patchwork of regulations with which they will need to comply. On the other hand, there are those who believe that federal legislation should do no more than lay the foundation for states to build on as preemption will stifle state innovation in this area.[133] The California Attorney General, Xavier Becerra, has specifically argued that a federal law should not undermine state protections urging that Congress "favor legislation that sets a federal privacy–protection floor rather than a ceiling" so as to allow states provide protections tailored to their residents.[134] The debate over federal preemption in this area remains unresolved.[135]

The European General Data Protection Regulation (GDPR)

The CCPA is arguably the U.S. version of the GDPR, because of their similarities in terms of their broad scope of application. Just like the GLBA and the CCPA, the purpose of the GDPR is to regulate how personal data is processed by regulating those persons that collect and process that data, while ensuring that it moves freely throughout the E.U..[136] Any personal data or information relating to an identified or identifiable person such as their name, address, employment history, income, IP address, etc., subject to any applicable exception,[137] cannot be collected, recorded, organized, structured, stored, used, transferred, adapted, altered, or otherwise processed unless such processing is in compliance with the

(a) In general: This subchapter and the amendments made by this subchapter shall not be construed as superseding, altering, or affecting any statute, regulation, order, or interpretation in effect in any State, except to the extent that such statute, regulation, order, or interpretation is inconsistent with the provisions of this subchapter, and then only to the extent of the inconsistency.

(b) Greater protection under State law: For purposes of this section, a State statute, regulation, order, or interpretation is not inconsistent with the provisions of this subchapter if the protection such statute, regulation, order, or interpretation affords any person is greater than the protection provided under this subchapter and the amendments made by this subchapter, as determined by the Bureau of Consumer Financial Protection, after consultation with the agency or authority with jurisdiction under section 6805(a) of this title of either the person that initiated the complaint or that is the subject of the complaint, on its own motion or upon the petition of any interested party.

[132] The GLBA preempts provisions of state statute, regulation, order or interpretation that areinconsistentare inconsistent with its provisions and such preemption is only to the extent of the inconsistency. State statutes, regulations, orders or interpretations will not be considered inconsistent if they provide greater consumer privacy protection as compared to the GLBA. Therefore, the GLBA does not preempt the enforcement of the CCPA for providing stricter consumer privacy safeguards.

[133] *See* Robert E. Slavkin, Is A Federal Privacy Law In the Cards for 2020?, December 12, 2019, available at https://www.healthlawrx.com/2019/12/is-a-federal-privacy-law-in-the-cards-for-2020/.

[134] *See* Sara Merken, California Attorney General Asks Congress to Shield Privacy Laws, Bloomberg Law, February 25, 2020, available at https://news.bloomberglaw.com/privacy-and-data-security/california-attorney-general-asks-congress-to-shield-privacy-laws.

[135] *See* Alysa Zeltzer Hutnik, Michael Lynch, Paul A. Rosenthal & Jewel Tewiah, Potential Constitutional Challenges to the CCPA, AD Law Access, December 12, 2019, available at https://www.adlawaccess.com/2019/12/articles/potential-constitutional-challenges-to-the-ccpa/.

[136] GDPR, Art. 1.

[137] The GDPR does not apply to the processing of personal data: (1) in the course of an activity that "falls outside the scope of E.U. law"; (2) by E.U. nations carrying out certain -E.U.-wide foreign policy and national security objectives; (3) by an individual in the course of a purely personal or household activity; and (4) by competent authorities conducting criminal investigations and prosecutions, including safeguarding against preventing threats to public security - GDPR Art. 2(2).

GDPR.[138] The CCPA's conceptualization of personal information is slightly broader as it considers information traceable, directly or indirectly, to a household and not just an individual. The GDPR categorizes holders of personal data into the controller and processor such that a controller determines the purposes and means of processing personal data,[139] and a processor is responsible for processing data on behalf of a controller.[140] Similar to the CCPA, the GDPR is extraterritorial in its application and offers a comprehensive data protection framework that applies throughout the European Union and in other jurisdictions that process personal data of persons resident in the E.U..[141] Therefore, U.S. companies, acting as either controllers or processors, that have an "establishment"[142] in the E.U. and/or (a) process personal data in the E.U.; (b) are established outside the E.U., but are offering goods and services in the E.U.; or (c) monitor behavior of individuals in the E.U. will be required to comply with the data protection requirements of the GDPR.

The key rights provisions of data subjects under the GDPR can be summarized under six headings, some of which are also provided for under both the CCPA and the GLBA:

Right to be informed. Individuals have a right to be informed about the collection and use of their personal data[143] and controllers have a corresponding right to provide them with privacy notices clearly stating the purposes for processing, retention periods, and with whom the data will be shared.[144] This transparency is also seen with the CCPA.

Right of access. Individuals have the right to access and obtain copies of their personal data and controllers must respond to a request for access within one month.[145] This provides certainty of obligation to the controllers and manages the expectations of the data subject.

Right to rectification. Individuals have the right to require personal data controllers to correct inaccurate information or complete incomplete data.[146]

Right to erasure. (also known as the "right to be forgotten") This provision is largely similar to the consumer's right to have their personal information deleted under the CCPA, save that the CCPA broadly guarantees this right subject to the applicability of certain exceptions. Under the GDPR, controllers are only obliged to comply with an erasure request without undue delay when, among others: (1) the data is no longer necessary for the purposes for which it was collected; (2) the controller relied on consent as its legal basis for processing and such consent has subsequently been withdrawn; or (3) the controller relied on the "legitimate interests"[147] basis for processing, the individual objected to processing, and there was

[138] GDPR Art. 4(2)).

[139] *Id.* Art 4(7)).

[140] *Id.* Art 4(2)).

[141] GDPR, Art. 3.

[142] The GDPR does not define "establishment," but states that it "implies the effective and real exercise of activity through stable arrangements." – GDPR recital 22.

[143] GDPR Art 12 – 14.

[144] *Id.*

[145] *Id.* Arts. 12(3), 15.

[146] *Id.* Art 16.

[147] Legitimate interests for data processing include, among other things, processing for direct marketing purposes, transmission within a group of affiliated entities for internal administrative purposes, ensuring network and information security, and reporting of possible criminal acts or threats to public security. GDPR, recitals 47–50.

no overriding legitimate interest.[148] In the absence of an applicable exception, the individual's right to be forgotten also applies when: (1) the controller is processing personal data for direct marketing purposes and the individual objects to the processing; (2) the data was processed unlawfully; (3) E.U. law or the law of an E.U. member nation requires the data to be erased; or (4) the data was collected in connection with the offering of internet services to a child.

Right to restrict processing. Individuals may exercise the right to restrict data processing in certain circumstances, within a limited period of time. In this regard, the right to restrict the data processing activities of the controller will apply when: (1) the accuracy of personal data is contested and the controller is in the process of verifying whether the data is accurate; (2) the processing is unlawful, but the data subject prefers restriction instead of erasure; (3) the controller no longer needs the personal data, but the data subject requires the data to be maintained in relation to its legal claims; or (4) the controller is considering whether the data subject's objection to processing overrides the legitimate interests in the processing while the controller evaluates a broader objection to its data processing activities.[149]

Right to data portability. This right allows data subjects to obtain their personal data that they provided to a controller in a commonly used, automated form that can be transmitted to another controller without affecting the data's usability.[150] This allows data to be transferred between controllers irrespective of the controller that originally collected or compiled the data. The portability of such data shall be based on the express consent of the data subject, or in fulfillment of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract.[151]

The rights conferred by the GDPR and the CCPA, particularly the rights to data portability and the right to request the deletion of information, respectively constitute some of the most prominent distinguishing features from the standard protections provided under the GLBA. Financial institutions have had to grapple with making the necessary infrastructural adjustments to their data collection and preservation practices[152] to ensure maximum compliance with the requirements of all three legislations. No matter the data security measures employed, the nature and scope of its security must be appropriate to the severity of the risks of infringement on individual rights if data security were to be violated.[153] This is particularly important given the rise of new industry players, such as Fintech firms and data aggregators, whose business activities are wholly automated with attendant risks of cyber intrusions and data theft, which may sometimes go undetected due to under regulation.

Although both the CCPA and the GDPR have the extra-territorial effect, the GDPR appears to have farther applicability as its data protection provisions extend to protect the personal data of consumers temporarily in the E.U. In reality, many financial institutions in the U.S. are able to comply with both the

[148] *Id*. Art. 17.

[149] *Id.* Art. 18(1).

[150] GDPR Art. 20(1)(a) – (b)).

[151] *Id.*

[152] *See* Lauren Davis, *The Impact of the California Consumer Privacy Act on Financial Institutions Across the Nation*, 24 N.C. BANKING INST. 499 (2020), available at https://scholarship.law.unc.edu/ncbi/vol24/iss1/22.

[153] GDPR Art 32(1)).

CCPA and the GDPR due to the scope and size of their operations transcending geographical boundaries. E-commerce businesses, firms providing Fintech solutions such as Apple Pay, PayPal etc., also carry similar burdens to ensure compliance with the CCPA, GDPR, and the GLBA because of the large amount of personal data processed as part of their routine business activities.

Who truly owns/controls consumer financial data and how should it be used?

The GLBA makes an effort to protect consumer financial data by giving them the power to control how their financial information is collected and shared with third parties. However, the broad list of excepted circumstances where financial institutions may act without notifying or obtaining the consumer's consent demonstrates in practical terms that consumers do not have real control over their financial data and any resulting third party disclosures or onward transfers. A recent report by the Federal Reserve of San Francisco (SF Fed) advocates for the reframing of the construct of consumer 'data ownership' to a more realistic notion of consumers having 'active data rights '.[154] The argument here is that this shift does not diminish the proprietary relationship between consumers and their data but rather "provides a broader framing that…acknowledges the inherent complexity of data as an intangible resource that is shared between individuals, businesses and the broader society."[155] This is understandable as, today's interconnected data economy makes it increasingly difficult for consumers to track who has access to their data and how it is being used. Therefore, consumers are limited in their capacity to actively take steps to protect collected data in the traditional sense of exercising ownership. This issue is further aggravated in instances where consumers authorize financial institutions to share their data with named third parties. Such authorized data sharing arrangements provide very limited means for the consumer to determine with certainty how often their data are being accessed, how long their data are being retained, with whom their data are being shared, and the risks associated with sharing their data and account credentials.[156]

It is also difficult to ensure that such third party's access is limited to the express purpose for which the consumer authorized access to their data. Discussions around the attendant privacy risks stemming from such authorized access have been on the rise owing to the proliferation of the financial market by new industry players, such as Fintech startups. They can access consumer information from financial institutions based on consents obtained from consumers directly or through alternative means, including the consumer's use of services provided by Fintech applications to track spending, set monthly budgets, apply for loans, or manage investments. Financial institutions and consumer privacy advocates are particularly concerned that the ease of portability of such sensitive data to largely unregulated industry actors will not only pose privacy risks for the consumers but also expose their data system safeguards to risks of cybersecurity breaches that could ultimately lead to unintended and unauthorized access to consumer's financial data. In essence, stakeholders are concerned about how informed

[154] Kaitlin Asrow, The Role of Individuals in the Data Ecosystem: Current debates and considerations for data protection and date rights in the United States, Fintech Edge Special Report, Federal Reserve Bank of San Francisco (June 3, 2020), available at https://www.frbsf.org/banking/files/The-Role-of-Individuals-in-the-Data-Ecosystem-Full-Report.pdf, Pages 17 – 22.

[155] *Id*. page 18

[156] *See* Michael S. Barr, Abigail Dehart and Andrew Kang, Consumer Autonomy & Pathways to Portability in Banking and Financial Services, Centre of Finance and Policy, University of Michigan, available at https://www.cio.com/article/3379036/the-united-states-needs-a-federal-privacy-law.html, Page 8.

consumers really are when providing such authorized access and whether financial institutions should out rightly honor them or exercise some discretion.

The CFPB attempted to address some of these issues and also assuage concerns around data security in its non-binding Consumer Protection Principles for Consumer-Authorized Financial Data Sharing and Aggregation, without creating new rules. The principles deal with the pressing issues of informed consumer consent, data scope, and usability, noting that third parties' authorized to access consumer's financial information should ensure that the authorization obtained addresses access frequency, data scope, and retention period so as to limit the third parties' access to the extent of the consent provided. Essentially, third parties with authorized access should only access the data necessary to provide the specific services for which access was granted and only maintain such data for as long as it is necessary.[157] Notwithstanding, these issues remain contentious and campaigns for a more substantive regulation on the matter persist.[158]

Should the U.S. Implement a Federal GDPR-styled privacy law?

Another question that has arisen since the coming into effect of the CCPA is whether the U.S. should adopt an overarching data protection and privacy law as opposed to leaving the field open for states to create their respective privacy laws. The wide reach and stringent conditions of the CCPA raise concerns about other states following suit. The federal government's approach to privacy and data protection has been industry-focused with its provisions limited to specific industry participants and certain types of data leading to duplicity of regulations and in some instances, contradictions. Consequently, financial institutions in the U.S. have the burden of complying with both the CCPA and the GLBA, while adjusting their procedures to ensure full compliance in circumstances where the laws diverge. This fragmented regulatory framework places undue burdens on business as they strive to avoid penalties for breaches or non-compliance.

Stakeholders in the financial industry have canvassed for Congress to consider creating protections in a federal law similar in spirit to the GDPR (and the CCPA) as it puts consumers in charge of their personal data.[159] Accordingly, several Senate Committee hearings to examine proposals for an overarching consumer privacy legislation have been held over the last 18 months. Participants at these hearings, which range from internet service providers to consumer privacy organizations, have made proposals to the Senate for a comprehensive federal privacy legislation highlighting the benefits that would come from such a law especially in today's highly digitally integrated world. Should Congress consider a comprehensive national data protection law, its legislative proposals would involve numerous legal considerations including, amongst others, the scope of application and nature of the information to be protected, enforcement agency/authority, issues of statutory overlap, and preemption of state laws.

[157] CFPB, Consumer Protection Principles: Consumer Authorized Financial Data Sharing and Aggregation (Oct. 18, 2017), http://files.consumerfinance.gov/f/documents/cfpb_cons umer-protection-principles_data-aggregation.pdf.

[158] Brian Knight, *Statement Regarding CFPB Dodd-Frank Section 1033 Symposium* (Feb. 26, 2020), available at https://files.consumerfinance.gov/f/documents/cfpb_knight-statement_symposium-consumer-access-financial-records.pdf.

[159] America Should Borrow from Europe's Data-Privacy Law, The Economist, April 5, 2018, available at https://www.economist.com/leaders/2018/04/05/america-should-borrow-from-europes-data-privacy-law.

Appendices – CFPB Memo

1. U.S. Dep't of Treasury, *A Financial System that Creates Economic Opportunity: Nonbank Financials, Fintech, and Innovation* 22-44 (2018) (hereinafter "Treasury Fintech Report"), https://home.treasury.gov/sites/default/files/2018-08/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financials-Fintech-and-Innovation.pdf.
2. Michael Barr et al, *Consumer Autonomy and Pathways to Portability in Banking and Financial Services*, University of Michigan Center on Finance, Law and Policy 1-2 (November 3, 2019), available at http://financelawpolicy.umich.edu/files/umich-cflp-working-paper-consumer-autonomy-and-data-portability-pathways-Nov-3.pdf.
3. Plaid Technologies, *Plaid response to CFPB regarding Consumer Access to Financial Records Docket No. CFPB-2016-0048* (Feb. 21, 2017), accessible at https://www.regulations.gov/document?D=CFPB-2016-0048-0058.

DODD FRANK S. 1033

General

4. 12 U.S.C. §5533 (2010) (Dodd Frank Act, Title X generally and Section 1033 specifically), accessible at https://legcounsel.house.gov/Comps/Dodd-Frank%20Wall%20Street%20Reform%20and%20Consumer%20Protection%20Act.pdf
5. CFPB, *Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation* (Oct. 18, 2017), available at: https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf.
6. CFPB, *Stakeholder Insights that Inform the Consumer Protection Principles* (October 18, 2017), available at https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation_stakeholder-insights.pdf.

Issue 1

7. Brian Knight, *Statement Regarding CFPB Dodd-Frank Section 1033 Symposium* 3-5 (Feb. 26, 2020), available at https://files.consumerfinance.gov/f/documents/cfpb_knight-statement_symposium-consumer-access-financial-records.pdf.
8. American Bankers Association, *Request for Information Regarding Consumer Access to Financial Records Docket No.: CFPB-2016-0048, 13*-14 (Feb. 21, 2017) available at https://www.regulations.gov/document?D=CFPB-2016-0048-0041.

9. Plaid Technologies, *Written Statement for the Symposium on Consumer Access to Financial Records* (Feb. 19, 2020), available at https://files.consumerfinance.gov/f/documents/cfpb_pitts-statement_symposium-consumer-access-financial-records.pdf.

Issue 2

10. National Consumer Law Center (on behalf of its low income clients), *Written Statement for CFPB's Symposium on Consumer Access to Financial Records, Section 1033 of the Dodd-Frank Act* (Feb. 12, 2020), accessible at https://files.consumerfinance.gov/f/documents/cfpb_wu-statement_symposium-consumer-access-financial-records.pdf.
11. Alessandro Acquisti and Jens Grossklags, *Privacy and Rationality in Decision Making*, 3(1) IEEE, Security and Privacy Magazine 26-33 (Jan. 2005), accessible at https://www.heinz.cmu.edu/~acquisti/papers/acquisti.pdf.
12. Daniel Solove, *Privacy Self-Management and the Consent Dilemma*, 126 Harvard Law Review 1880 (2013), accessible at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2171018.

Issue 3

13. ABA RFI Response, see appendix 8.
14. Kate Rooney, *PNC's fight with Venmo highlights bigger issue over who owns your banking data,* CNBC (Dec. 16, 2019), available at https://www.cnbc.com/2019/12/16/venmo-and-pncs-fight-over-sharing-consumer-financial-data.html.

Issue 4

15. Article 29 Data Prot. Working Party, Guidelines on the Right to Data Portability, 16/EN WP242 at 10 (April 5, 2017) available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233.
16. National Consumer Law Center, *Comments in Response to Requests for Information: Consumer Access to Financial Records, Docket No. CFPB-2016-0048*, 7 (Feb. 21, 2017), accessible at https://www.regulations.gov/document?D=CFPB-2016-0048-0072.
17. Paul De Hert, Vagelis Papakonstantinou, Gianclaudio Malgieri, Laurent Beslay & Ignacio Sanchez, *The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services*, COMPUTER L. & SECURITY REV. 193 (2018), accessible at https://www.sciencedirect.com/science/article/pii/S0267364917303333.

Issue 5

18. Treasury Fintech Report (see appendix 1)
19. Written Statement of Petal Card, Inc., Symposium on Consumer Access to Financial Records, Section 1033 of the Dodd-Frank Act (Feb. 12, 2020), available at https://files.consumerfinance.gov/f/documents/cfpb_gross-statement_symposium-consumer-access-financial-records.pdf.
20. Independent Community Bankers of America, *Docket No. CFPB-2016-0048, Request for Information Regarding Consumer Access to Financial Records*, 6 (Feb. 21, 2017), accessible at https://www.regulations.gov/document?D=CFPB-2016-0048-0035.

21. Fidelity Investments, *Request for Information Regarding Consumer Access to Financial Records; Docket No. CFPB-2016-0048*, 6-8 (Feb. 21, 2017), available at https://www.regulations.gov/document?D=CFPB-2016-0048-0053.

FCRA

22. Regulation V, 12 C.F.R. § 1022 https://www.consumerfinance.gov/policy-compliance/rulemaking/regulations/1022/1/.
23. Kwamina Williford and Brian Goodrich, *Why Data Sources Aren't Furnishers Under Credit Report Regs*, HK Law (blog post), available at https://www.hklaw.com/-/media/files/insights/publications/2019/09/whydatasourcesarentfurnishersundercreditreportregs.pdf?la=en.
24. NCLC Symposium Statement, 6-9 (see appendix 10)
25. Plaid RFI Response, 11-14 (see appendix 3).
26. Federal Trade Commission, *40 Years of Experience with the Fair Credit Reporting Act: An FTC Staff Report with Summary of Interpretations* 29, July 2011, https://www.ftc.gov/sites/default/files/documents/reports/40-years-experience-fair-credit-reporting- act-ftc-staff-report-summary-interpretations/110720fcrareport.pdf.

EFTA

27. Regulation E, 12 C.F.R. § 1005, available at https://www.consumerfinance.gov/policy-compliance/rulemaking/regulations/1005/14/#14-b-Interp-1.
28. NCLC RFI Response (see appendix 16)
29. ABA RFI Response (see appendix 8)

Appendices - Privacy

1. Juliana De Groot, What is GLBA Compliance? Understanding the Data Protection Requirements of the Gramm-Leach-Biley Act in 2019, Digital Guardian's Blog (July 15, 2019) https://digitalguardian.com/blog/what-glba-compliance-understanding-data-protection-requirements-gramm-leach-bliley-act
2. Debevoise & Plimpton, The California Consumer Privacy Act: Compliance Strategies for Financial Institutions, Debevoise Update, (May 2, 2019) https://www.debevoise.com/insights/publications/2019/04/the-california-consumer-privacy-act
3. Juliana De Groot, What is the General Data Protection Regulations? Understanding and Complying with the GDPR Requirements in 2019, Digital Guardian's Blog (December 2, 2019) https://digitalguardian.com/blog/what-gdpr-general-data-protection-regulation-understanding-and-complying-gdpr-data-protection
4. Helen Goff Foster, Exempt or Not Exempt? California Consumer Privacy Act and the Gramm-Leach-Biley Act, Davis Wright Tremaine LLP, Privacy & Security Law Blog (April 15, 2019) https://www.dwt.com/blogs/privacy--security-law-blog/2019/04/exempt-or-not-exempt
5. Ropes & Gray, GDPR vs CCPA (2019) https://www.ropesgray.com/-/media/Files/Prax-Pages/CCPA/GDPR-vs-CCPA.pdf?la=en&hash=8C02199DFCD96E702D76B8880DD70EF7FFB7B744
6. Davis Wright Tremaine LLP, Q&A: Privacy and Security Partner Christopher Ott on the California Consumer Privacy Act of 2018, , Privacy & Security Law Blog, (August 6, 2018) https://www.dwt.com/blogs/privacy--security-law-blog/2018/08/qa-privacy-and-security-partner-christopher-ott-on
7. Mayer Brown LLP, Whose Data is it: CFPB Releases Consumer protection Principles for Consumer Authorized Financial Data Sharing and Aggregation (November 2, 2017) https://www.mayerbrown.com/-/media/files/perspectives-events/publications/2017/11/whose-data-is-it-cfpb-releases-consumer-protection/files/updatecfpbprinciplesforfinancialdatasharingandaggr/fileattachment/updatecfpbprinciplesforfinancialdatasharingandaggr.pdf
8. Kaitlin Asrow, The Role of Individuals in the Data Ecosystem: Current debates and considerations for data protection and date rights in the United States, Fintech Edge Special Report, Federal Reserve Bank of San Francisco (June 3, 2020), https://www.frbsf.org/banking/files/The-Role-of-Individuals-in-the-Data-Ecosystem-Full-Report.pdf
9. Lauren Davis, The Impact of the California Consumer Privacy Act on Financial Institutions Across the Nation, 24 N.C. BANKING INST. 499 (2020), https://scholarship.law.unc.edu/ncbi/vol24/iss1/22
10. Kristen Mathews, Adam Fleisher, Morrison & Foester, Financial Institutions and the CCPA: What remains after the Law's Exceptions?, Bloomberg Law, (October 2019) https://media2.mofo.com/documents/191025-financial-institutions-ccpa.pdf

11. America should borrow from Europe's data-privacy law, The Economist, (April 5, 2018), https://www.economist.com/leaders/2018/04/05/america-should-borrow-from-europes-data-privacy-law
12. David MacCabe, Congress & Trump Agreed they want a National Privacy Law. It is Nowhere in Sight, The New York Times, (October 2019) https://www.nytimes.com/2019/10/01/technology/national-privacy-law.html
13. Fara Soubouti, Data Privacy and the Financial Services Industry: A Federal Approach to Consumer Protection, 24 N.C. BANKING INST. 527 (2020) https://scholarship.law.unc.edu/ncbi/vol24/iss1/23
14. Information Technology & Innovation Foundation, Debate: Should the U.S. Copy the E.U.s New Privacy Law, (September 18, 2018), https://itif.org/events/2018/09/25/debate-should-us-copy-eu-privacy-law
15. Carl Schonander, The United States needs a federal privacy law, CIO, (March 22, 2019), https://www.cio.com/article/3379036/the-united-states-needs-a-federal-privacy-law.html
16. Derek Hawkins, The Cybersecurity 202: Why a privacy law like GDPR would be a tough sell in the U.S., The Washington Post, May 25, 2018, https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/05/25/the-cybersecurity-202-why-a-privacy-law-like-gdpr-would-be-a-tough-sell-in-the-u-s/5b07038b1b326b492dd07e83/
17. Council on Foreign Relations, Reforming the U.S. Approach to Data Protection and Privacy, January 30, 2018, https://www.cfr.org/report/reforming-us-approach-data-protection

HARVARD LAW SCHOOL | The Case Studies

CSP023
MAY 2020

Anti-Money Laundering and Blockchain Technology

CHUNG-CHIA HUANG AND ASHER TRANGLE

Memorandum

DATE:	January 26, 2020
TO:	Junior FinCEN Lawyer
FROM:	Director of FinCEN
RE:	Recommendations Regarding Reforming BSA/AML Compliance

Welcome to your new position as a junior attorney at FinCEN. FinCEN plays a critical role in monitoring and enforcing financial crimes involving banks and other financial institutions. The organization takes this role very seriously, and we are proactively seeking more effective ways of detecting illegal activity and fighting financial crime. Over the past year, I have been monitoring articles and suggestions regarding how to improve or reform anti-money laundering laws. As new technologies develop, a number of startups are using blockchain technology with the goal of helping financial institutions comply with U.S. anti-money laundering (AML) laws. Financial institutions are eager to test whether blockchain technology products can simultaneously improve or increase their compliance with AML laws while reducing the enormous costs associated with the current AML framework.

I want you to look into what types of reforms, if any, FinCEN should seriously consider adopting. In particular, please research the viability of new technologies, such as blockchain and/or machine learning, for changing our regulatory approach and make a recommendation as to whether FinCEN should support the adoption of such technologies for AML compliance.

Please note that there may be other data sharing systems or technologies (e.g. permissioned ledgers) that have also been mentioned with respect to increasing the efficiency of AML compliance. Include the pros and cons of adopting your recommendations. I am certain that you understand the importance of FinCEN's role in the enforcement community; we are on the front lines of fighting financial crimes and cutting off funding for terrorist organizations and terrorist attacks. Adopting new technology to help combat these crimes may be very helpful—if not imperative—in the future. However, FinCEN

Written by Chung-Chia Huang and Asher Trangle under the supervision of Professor Howell E. Jackson, James S. Reid, Jr., Professor of Law, Harvard Law School. Case development at Harvard Law School is partially funded by a grant from Dechert LLP. Cases are developed solely as the basis for class discussion. They are not intended to serve as endorsements, sources of primary data, legal advice, or illustrations of effective or ineffective management.

Copyright © 2020 President and Fellows of Harvard University. No part of this publication may be reproduced, stored in a retrieval system, used in a spreadsheet, or transmitted in any form or by any means—electronic, mechanical, photocopying, recording, or otherwise—without permission. To order copies or permissions to reproduce materials please visit our website at casestudies.law.harvard.edu or contact us by phone at 617-496-1316, by mail at Harvard Law School Case Studies Program, 1545 Massachusetts Avenue – Areeda 507, Cambridge, MA 02138, or by email at HLSCaseStudies@law.harvard.edu.

cannot support the use of new technology by financial institutions if it means less-effective monitoring or enforcement.

I would like your recommendation on my desk as soon as possible. I have had our analysts compile the following primer to help bring you up to speed on these issues.

Origins of the Bank Secrecy Act and Subsequent Legislation

FinCEN is a bureau of the U.S. Department of the Treasury and is tasked with safeguarding the financial system from illicit use and combating domestic and international financial crimes, including money laundering and terrorist financing.[1] As a feature of its enforcement powers, FinCEN is the designated administrator of the Bank Secrecy Act of 1970 (BSA) and the subsequent laws enhancing and amending the BSA.[2]

The goal of the BSA compliance scheme is to encourage financial institutions to help identify the source, volume, and movement of currency flowing through those financial institutions.[3] As initially conceived, the BSA was implemented as a way to fight the drug trade in the 1970s, as drug dealers were using the financial system to divert profits from illegal operations to legitimate sources.[4] To combat this money laundering, authorities sought to "follow the money" and establish a paper trail of all customer transactions in an effort to make it far more difficult for drug dealers to launder profits.[5] To accomplish this, the BSA established recordkeeping and reporting requirements like the Consumer Transaction Report (CTR) for all deposits, withdrawals, exchanges, or transfer of funds over $5,000 (since increased to $10,000).[6]

Since 1970, numerous other laws have been enacted by Congress enhancing and amending the BSA to provide FinCEN and other regulatory agencies with the most effective tools to detect and prevent money laundering and other financial crimes.[7] The Money Laundering Control Act of 1986 (MLCA) directed financial institutions to establish and maintain procedures designed to reasonably monitor and ensure compliance with the reporting and recordkeeping requirements of the BSA while imposing sanctions on financial institutions that assisted customers in laundering money.[8] Later, the Annunzio-Wylie Anti-Money Laundering Act of 1992 expanded the concept of the CTR and required financial institutions to file reports

[1] *Mission*, FINCEN, www.fincen.gov/about/mission [perma.cc/LJX2-ARFE] (last visited Oct. 30, 2016).

[2] FinCen, *History of Anti-Money Laundering Laws*, FINCEN, www.fincen.gov/history-anti-money-laundering-laws [perma.cc/Q9QL-R9FB] (last visited Oct. 30, 2016).

[3] FFIEC, *Bank Secrecy Act Anti-Money Laundering Examination Manual: Introduction*, FED. FIN. INSTITUTIONS EXAMINATIONS COUNCIL, www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_002.htm [perma.cc/D99L-QUQE] (last visited Oct. 30, 2016); [hereinafter Fed. Fin. Institutions Examinations Council will be referred to as FFIEC).

[4] Stavros Gadinis and Colby Mangels, *Collaborative Gatekeepers*, 73 WASH. & LEE L. REV. 797, 859 (2016) (citing Peter E. Meltzer, *Keeping Drug Money From Reaching the Wash Cycle: A Guide to the Bank Secrecy Act*, 108 BANKING L.J. 230, 231 (1991)).

[5] *Id.*

[6] *See* FFIEC, *supra* note 3; Gadinis & Mangels, *supra* note 4, at 859-60.

[7] FinCEN, *supra* note 2.

[8] *See* Money Laundering Control Act, Pub. L. No. 99-570, 100 Stat. 3207, § 1359; FFIEC, *supra* note 4; Gadinis & Mangels, *supra* note 4, at 861.

whenever they detected suspicious activity.[9] The Annunzio-Wylie Act also granted the U.S. Treasury broad authority to create AML regulations and demand reports for any violation of law or regulation.[10]

In the wake of the September 11, 2001 terrorist attacks, Congress passed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (Patriot Act), which imposed striking new requirements on financial institutions as part of the broader goal to combat terrorism.[11] The Patriot Act included provisions to expand AML requirements to all financial institutions subject to U.S. regulatory jurisdiction, provide the Secretary of Treasury with the authority to impose "special measures" on financial institutions that are of "primary money-laundering concern," augment the existing BSA framework by strengthening customer identification procedures, impose a 120 hour period in which financial institutions must respond to regulatory requests for information, and improve information-sharing between financial institutions and the U.S. government.[12]

Aside from FinCEN, other federal agencies also shoulder responsibility for enforcing aspects of overall U.S. AML policy. For example, the Department of Justice (DOJ), focuses on the criminal aspect of the AML laws, investigates and brings charges against those laundering money. The DOJ not only targets natural persons who commit crimes, but also has power to investigate and prosecute financial institutions and their officers, directors, and employees.[13] Their investigations mostly lead to non-prosecution agreements or deferred-prosecution agreements. Bank regulators are also a crucial component of AML compliance schemes. Bank regulators execute examinations, whether on-site or off-site, to ensure the regulated banks are in compliance with prudential standards. On top of that, examinations would also include some AML aspects, such as whether the bank follows certain process or standards.[14]

The Current AML Compliance Regime

The current AML compliance regime has several important requirements that impose obligations on financial institutions. The key features of AML compliance include requirements that financial institutions file currency reports with the U.S. Department of the Treasury,[15] report suspicious transactions through Suspicious Activity Reports (SAR),[16] properly identify persons conducting transactions and opening bank accounts through customer identification programs (CIP—this compliance technique is commonly referred to as "know your customer" or "KYC"),[17] and maintain a paper trail by

[9] 31 U.S.C. § 5318(g) (2012) (the Annuzio-Wiley Act's "Reporting of Suspicious Transactions" provision); Gadinis & Mangels, *supra* note 4, at 869-70.

[10] Gadinis, *supra* note 4, at 869-70.

[11] USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001), www.sec.gov/about/offices/ocie/aml/patriotact2001.pdf [perma.cc/XQR4-FYLV]; FFIEC, *supra* note 4.

[12] FFIEC, *supra* note 3.

[13] https://www.justice.gov/jm/jm-9-105000-money-laundering

[14] A job post of OCC hiring BSA examiner. https://careers.occ.gov/careers/explore/bank-supervision/bsa-aml/index-bsa-aml-supervision.html

[15] 31 C.F.R. §§ 1010.311 (requirements for financial institutions to report currency transactions in excess of $10,000); 1010.340 (requirements for filing a Report of International Transportation of Currency or Monetary Instruments (CMIR)); 1010.350 (requirements of reporting foreign financial accounts for each entity having a financial interest in a foreign account).

[16] *Id.* at §§ 1010.320 (SAR requirement for banks); 1025.320 (SAR requirement for insurance companies).

[17] *Id.* at §§ 1010.312 (requirement that financial institutions verify the identity of persons conducting currency transactions in excess of $10,000); 1020.320 (requirement for financial institutions to have a written Customer Identification Program).

keeping appropriate records of financial transactions.[18] These features are designed to enable law enforcement and regulatory agencies to pursue investigations of criminal, tax, and regulatory violations, if warranted, and provide evidence useful in prosecuting money laundering and other financial crimes.[19]

Two of the most robust compliance mechanisms are SARs requirements (banks must detect and report any suspicious activity) and KYC requirements (banks must obtain and verify detailed information about customers when processing transactions and opening new accounts). According to Treasury regulations, the range of suspicious activities that a bank must report is broad. It first encompasses transactions involving funds that come from illegal activities or that are designed to mask illegal activities. In addition, it includes transactions that are designed to evade the BSA and its reporting requirements (such as the $10,000 CTR threshold). Finally, any other unusual activity or transactions which have no business or lawful purpose must also be reported.[20] This scheme imposes on a bank a duty to both use its judgment when it comes to detecting suspicious activity and also to explain its suspicions to the government in the SAR it files.[21]

KYC programs require that a bank verify "the identity of individuals and businesses that are account holders" and the bank must also "be familiar enough with their banking practices so that transactions that are outside the norm can be readily identified."[22] Thus, a bank must have a system installed to collect relevant information about a client's background, business purposes, and anticipated activities to make such a determination.[23]

In many ways, the AML scheme imposes greater burdens on financial institutions than the compliance regimes of other financial laws. Outside of the AML context, many other financial regulatory schemes, such as the U.S. securities laws, require financial institutions to identify problematic clients or transactions, yet only impose heavy liability if the financial institution *knowingly* or *negligently* allowed such transactions to occur.[24] Conversely, when it comes to AML, financial institutions must report customers and activities based merely on *suspicions* of misconduct.[25] Thus, financial institutions cannot be "willfully blind" when it comes to their customers or the transactions that they process.[26]

The BSA also places a heavy emphasis on the requirement that financial institutions create internal mechanisms to comply with these regimes. U.S. law sets out the "four pillars" of a BSA program that financial institutions must establish for its anti-money laundering programs, which must at a minimum include 1) development of internal policies, procedures, and controls, 2) a designated

[18] *Id.* at §§ 1010.306 (requirements that financial institutions maintain records relating to purchases of monetary instruments with currency in amounts between $3,000 and $10,000); 1010.415; 1010.420; 1010.430; 1020.410; *see also* FFIEC, *supra* note 4.

[19] FFIEC, *supra* note 3.

[20] *See* 12 C.F.R. § 21.11(c); 31 C.F.R. § 1010.311; Gadinis, *supra* note 4, at 870-71; *see also* U.S. Gov't Accountability Office, GAO-95-156, Report to the Ranking Minority Member Permanent Subcommittee on Investigations, Committee on Governmental Affairs, U.S. Senate 12 (1995), gao.gov/assets/160/155076.pdf [perma.cc/K4VN-YPLL] (listing other suspicious transactions such as customers changing the dollar amount of or cancelling transactions when informed of reporting requirements, unusually large purchases of money orders or cashier's checks, unusually large deposits, and international wire transfers).

[21] *See* Gadinis & Mangels, *supra* note 4, at 871.

[22] U.S. Gov't Accountability Office, *supra* note 18, at 12.

[23] *See* Bank Secrecy Act Anti-Money Laundering Examination Manual: Appendix F: Money Laundering and Terrorist Financing "Red Flags", FFIEC, www.ffiec.gov/bsa_aml_infobase/pages_manual/olm_106.htm [perma.cc/TUR6-PJVT] (last visited Oct. 30, 2016); Gadinis & Mangels, *supra* note 4, at 871 (citing 31 U.S.C. § 5318 (2012)).

[24] Gadinis & Mangels, *supra* note 4, at 801-02.

[25] *Id.* at 802.

[26] *See U.S. v. St. Michael's Credit Union*, 880 F.2d 579, 584-86 (1st Cir. 1989); *see* Gadninis & Mangels, *supra* note 35, at 873.

compliance officer, 3) ongoing employee training, and 4) an independent audit function to test programs.[27] A "fifth pillar" was added by the Treasury Department in May 2016 requiring banks to identify beneficial owners of legal entities which have accounts at the bank and to add risk-based customer due diligence procedures to its monitoring program.[28] Due to regulators' reliance on banks to discover and report problematic customers and transactions, any failure to comply with the AML regime results in harsh sanctions being imposed on financial institutions, with both civil and criminal penalties available to enforcement agencies.[29] In fact, a number of financial institutions have faced stiff fines not for processing suspicious transactions but because their compliance scheme or detection mechanisms were deemed insufficient.[30]

Beyond the mandatory compliance programs, there are a number of non-compulsory steps that financial institutions are encouraged to take to help the government reach its AML objectives. FinCEN has stressed to banks the importance of sharing information not only internally (within components or departments of the same institution) but also with entirely distinct financial institutions.[31] This inter-bank sharing mechanism was established by a Patriot Act safe-harbor provision contained in Section 314(b) that allows for financial institutions to voluntarily share information with each other to better identify and report potential money laundering or terrorist activities.[32] Voluntarily engaging in information exchange under Section 314(b) to help identify AML violations is strongly encouraged by FinCEN.[33]

Relevant Government Players

As noted above, given the iterative development of a comprehensive BSA / AML scheme over time, different federal entities have been entrusted responsibility for differing components of the overall system. Established in 1990, FinCEN has, in recent years, come to focus heavily on BSA/ AML from a lens centered on national security and antiterrorism.[34] Its stated mission is to "follow the money" and partner with law enforcement to support "the nation's foreign policy and national security objectives."[35] FinCEN could be seen as an "information conduit between financial institutions and government agencies" by collecting and storing troves of financial information provided by financial institutions for access by law enforcement agencies.[36] Given FinCEN's heavy focus on antiterrorism, it could be argued that FinCEN could be more reticent to develop or accept reformist arguments aimed at curbing compliance costs if it would result in decreased efficacy of BSA / AML outcomes. As noted later, other financial regulators

[27] *See* 31 U.S.C. § 5318(h) (2012).

[28] *See* 81 Fed. Reg. 29397 (May 11, 2016) (codified at 31 C.F.R. §§ 1010, 1020, 1023, 1024, 1026 (2016)) (established in the wake of the 2016 "Panama Papers" scandal).

[29] *See* 31 U.S.C. §§ 5321-22 (2012).

[30] *See* Samee Zafar, *Can Blockchain Prevent Money Laundering?*, Edgar, Dunn & Co. Mgmt. Consultants (Sept. 30, 2016), edgardunn.com/2016/09/can-blockchain-prevent-money-laundering [perma.cc/ZC4Q-WMJC] (noting the case of Standard Chartered Bank where the bank was fined $300 million because the bank had below-par AML systems and controls).

[31] FINCEN, FIN-2014-A007, ADVISORY TO U.S. FINANCIAL INSTITUTIONS ON CREATING A CULTURE OF COMPLIANCE 3, note 2 (2014), www.fincen.gov/sites/default/files/shared/FIN-2014-A007.pdf [perma.cc/EFG8-CAY6].

[32] USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 307 § 314(b) (2001); 31 C.F.R. § 1010.540.

[33] FinCEN, INFORMATION SHARING BETWEEN FINANCIAL INSTITUTIONS: SECTION 314(b) FACT SHEET (2013), www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf [perma.cc/32MD-8SL2].

[34] https://www.fincen.gov/what-we-do/

[35] *Id.*

[36] Jeffrey R. Boles, Financial Sector Executives As Targets for Money Laundering Liability, 52 AM. BUS. L.J. 365, 382 (2015)

(perhaps foreign analogues or other domestic entities charged with other aspects of AML / BSA) may be more attuned to potential inefficiencies in the overall scheme. Direct enforcement arising out of the information collected by FinCEN would likely be carried out by federal prosecuting agencies such as the Department of Justice. These actors may utilize the FinCEN in the course of developing their investigations or prosecuting bad actors who have violated the substance of AML laws (rather than simply being noncompliant). These actors may be less likely to interface with financial institutions or have a close working relationship such that they understand the staggering nature of compliance costs incurred under BSA / AML requirements.

Modern AML Outcomes: Mixed Results

As for the overall efficacy of AML, a 2015 article found that the current and comprehensive set of AML compliance requirements *were* effective in detecting and preventing money laundering operations and illegal financial activity.[37] Furthermore, according to Daniel Benjamin, the former National Security Council Director for Transnational Threats, some argue that the effort to disrupt terrorists' access to financial resources has been "the most successful part" of the fight against terrorism since 9/11.[38] However, some critics argue that insufficient empirical data has been collected and that no tests have been conducted to adequately examine the effectiveness of the current scheme. Therefore, the current system may not actually be the most effective.[39]

AML enforcement has become especially robust in the wake of the financial crisis. Four out of the eight largest fines against financial institutions since the Great Recession have involved AML violations.[40] Many of the most prominent global banks have faced AML sanctions since the financial crisis, including J.P. Morgan Chase, BNP Paribas, HSBC, TD Bank, Credit Suisse, and UBS.[41] Goldman Sachs is currently being investigated for allegedly aiding a fraud committed on Malaysia's 1MDB development fund and whether the investment bank violated U.S. AML laws.[42] Marking a dramatic increase in AML enforcement since 2009, financial institutions have been assessed over $12 billion in fines, penalties, and forfeitures for failure to report suspicious transactions as required by the AML regime.[43] From 2011-2015 the number of AML enforcement actions has risen 75%, and the dollar amount of penalties has increased by 431%.[44] In short, the U.S. AML regime has become a critical detection and enforcement mechanism that regulators use to hold banks accountable and to combat financial crimes.[45] However, critics of the current system

[37] *See* Jimmy Yicheng Huang, *Effectiveness of US anti-money laundering regulations and HSBC case study*, 18 J. Money Laundering Control 525, 532 (2015) (using HSBC as a case study).

[38] *See* Anne L. Clunan, *The Fight against Terrorist Financing*, 121 POL. SCI. Q. 569, 569 (2006).

[39] See generally Lanier Saperstein, Geoffrey Sant & Michelle Ng, The Failure of Anti–Money Laundering Regulation: Where Is The Cost-Benefit Analysis?, 91 NOTRE DAME L. REV. 1 (2015); see also Zafar, supra note 28.

[40] Stephen Grocer, *A List of the Biggest Bank Settlements*, Moneybeat (Blog), Wall St. J. (June 23, 2014), blogs.wsj.com/moneybeat/2014/06/23/a-list-of-the-biggest-bank-settlements/s.wsj.com/moneybeat/2014/06/23/a-list-of-the-biggest- bank-settlements/; *see* Gadinis, *supra* note4, at 801.

[41] *See* Grocer, *supra* note 35; Gadinis, *supra* note 4, 801.

[42] Justin Baer, Tom Wright & Bradley Hope, *Goldman Probed Over Malaysia Fund 1MDB*, WALL ST. J. (June 7, 2016).

[43] U.S. Gov't Accountability Office, GAO-16-297, Financial Institutions: Fines, Penalties, and Forfeitures for Violations of Financial Crimes and Sanctions Requirements 11 (2016), gao.gov/assets/680/675987.pdf [perma.cc/36U3-GKYJ].

[44] Stephen Heifetz & Evan Abrams, *Dramatic Rise in FinCEN Enforcement*, STEPTOE INTERNATIONAL COMPLIANCE (BLOG), STEPTOE & JOHNSON LLP (Oct. 11, 2016), www.steptoeinternationalcomplianceblog.com/2016/10/dramatic-rise-in-fincen-enforcement [perma.cc/3EVT-UM7U].

[45] *See* Gadinis, *supra* note 4, at 801.

posit that “regulators have been punishing the banks not because of any actual money laundering, but rather because the banks did not meet the regulators’ own subjective vision of the ideal anti–money laundering or counter–terrorist financing program.”[46]

The Growing Costs of AML Compliance

As noted above, the current U.S. AML regime enlists private financial institutions as gatekeepers and places monitoring and reporting requirements on banks.[47] Beyond the $12 billion fines levied on financial institutions for AML violations over the past decade, banks are facing increasing costs to meet AML compliance requirements. Banks have increased spending to adopt complex compliance systems that attempt to integrate new technologies while also dedicating entire staff members purely to compliance work.[48] For example, J.P. Morgan CEO Jamie Dimon revealed in his 2014 annual letter to shareholders that the bank had hired 8,000 new employees in 2013 to focus primarily on AML compliance and that J.P. Morgan employees had undergone 800,000 hours of compliance training.[49]

According to FinCEN’s outreach report, a single large financial institution could have over 80 lines of business where each product employs its own AML compliance officer.[50] Because of this complexity, certain banks have faced added compliance costs totaling more than $4 billion annually as compared to pre-financial crisis levels.[51] These developments have led to concomitant increase in SAR reports from approximately 50,000 in 1996 to roughly 1,800,000 in 2015.[52] It is estimated that the total spending on AML compliance alone has grown from $3.6 billion in 2008 to an estimated $10 billion annually in recent years.[53] Factoring in sanctions, financial institutions pay nearly $18 billion in AML costs annually.[54] Thus, banks are constantly looking for innovative ways to lower compliance costs without increasing their liability. However, executives are aware that regulators remain focused on compliance and any cutbacks or lapses in compliance procedures would likely be met with disapproval.[55] Beyond fines, banking executives have expressed concerns over being placed into a regulatory “penalty box” whereby *other* business activities must be curtailed or the business’s ability to expand is explicitly constrained. As part of

[46] Saperstein, *supra* note 34, at 1.

[47] *See generally* Gadinis, *supra* note 4.

[48] *See* Gadinis, *supra* note 4, at 874-75.

[49] Jamie Dimon, *Dear Fellow Shareholders*, J.P. Morgan Chase 21, 23 (Apr. 8, 2015), www.jpmorganchase.com/corporate/investor-relations/document/JPMC-AR2014-LetterToShareholders.pdf [perma.cc/BR6T-7Y83]; Anthony Effinger, *The Rise of the Compliance Guru—and Banker Ire*, Bloomberg (June 25, 2015), www.bloomberg.com/news/features/2015-06-25/compliance-is-now-calling-the-shots-and-bankers-are-bristling [perma.cc/D8RC-6GLM]; *see also* Monica Langley & Dan Fitzpatrick, *Embattled J.P. Morgan Bulks Up Oversight*, Wall St. J., (Sep. 12, 2013).

[50] FinCEN, Financial Institutions Outreach Initiative: Report on Outreach to Large Depository Institutions 5 (2009), www.fincen.gov/sites/default/files/shared/Bank_Report.pdf [perma.cc/L3M6-KVJE]; *see also* Gadinis, *supra* note 4, at 883.

[51] Laura Noonan, *Banks Face Pushback Over Surging Compliance and Regulatory Costs*, Fin. Times (May 28, 2015), www.ft.com/content/e1323e18-0478-11e5-95ad-00144feabdc0.

[52] *See* FinCEN, The SAR Activity Review: By The Numbers 1 (2004), www.fincen.gov/news_room/rp/files/sar_by_numb_03.pdf; [https://perma.cc/S2QL-F6HG] ; *Suspicious Activity Report Statistics*, FinCEN https://www.fincen.gov/reports/sar-stats; [https://perma.cc/GA39-48M5]; (last visited Oct. 30, 2016) (evaluating 2015 statistics).

[53] WealthInsight, 2020 Foresight: The Impact of Anti-Money Laundering Regulations on Wealth Management 6 (2013), www.marketresearch.com/product/sample-7717318.pdf; [https://perma.cc/4MDV-9J83]; Goldman Sachs, Profiles in Innovation: Blockchain 71 (2016), www.the-blockchain.com/docs/Goldman-Sachs-report-Blockchain-Putting-Theory-into-Practice.pdf [perma.cc/YZ8U-2AKP].

[54] Goldman Sachs, *supra* note 49, at 71.

[55] *See* Noonan, *supra* note 47.

the consequences imposed on Wells Fargo for their recent fraudulent account scandal, the Fed imposed just such growth restrictions.[56] These growth restrictions could be a much greater source of concern or worry for financial institutions than the imposition of financial penalties for AML compliance breakdowns.

Sanctions Violations Penalties

In addition to AML obligations, banking entities face a number of regulatory and compliance burdens stemming from U.S. governmental sanctions imposed on foreign entities. The Treasury Department's Office of Foreign Asset control (OFAC) holds primary responsibility for implementing U.S. sanction policies. As some scholars note, "OFAC has become one of the most feared regulators of the global financial sector."[57] Recent sanctions against large multinational banks have accounted for some of the largest fines these entities have suffered.[58] In 2014, BNP Paribas paid $963 million as part of a settlement agreement with OFAC for alleged violations of U.S. sanctions laws.[59] In addition, OFAC has fined ING $619 million, HSBC $375 million and Credit Suisse nearly $500 million for sanctions violations.[60] Pressure from these types of sanctions violations fines have forced financial institutions to reexamine their relationships with correspondent banking.[61] Some of the largest fines paid by financial institutions actually stem from *sanctions* violations as opposed to AML compliance violations.

"De-risking": An Unintended Consequence of AML Compliance

A 2017 article in *The Economist* noted that the primary goal of AML laws (removing the ability of bad actors to cleanse their illicit money) could come into conflict with promoting financial inclusion as a means to promote economic development.[62] So-called "de-risking" lies at the root of the problem. To decrease the chance of being fined, banks engage in de-risking—the process under which financial institutions refuse to provide services to customers labeled as a high-risk for money laundering, as computed by using the customer's personal information and geographic location.[63] *The Economist* also noted that such "de-risking" did not actually reduce the risk of financial crimes. Instead, it may actually increase the risk of those individuals becoming involved in illegal transactions by forcing them to engage in cash-based transactions and or to use unregulated financial networks (shadow banking).[64]

[56] *See, e.g.,* Federal Reserve Board Cease-and-Desist Order in the matter of Wells Fargo & Company, Docket No. 18-007-B-HC (Feb. 2, 2018) (imposing restrictions on growth and limitations on the activities of Wells Fargo in response to widespread consumer abuses and other compliance breakdowns).

[57] Wesley Laine, *OFAC, the dollar and US sanctions* (Fall 2016), (unpublished) at 11.

[58] *Id.*

[59] U.S. Department of the Treasury. "Treasury Reaches Largest Ever Sanctions-Related Saribas SA for $963 Million." *Treasury Reaches Largest Ever Sanctions-Related Settlement with BNP Paribas SA for $963 Million.* N.p., 30 June 2014. Web. https://www.treasury.gov/press-center/press-releases/Pages/jl2447.aspx

[60] Laine, *supra* note 53.

[61] A correspondent banking account is one used by a domestic financial institution to receive funds or make transactions from foreign banking entities.

[62] *The Economist, The unintended effects of rules aimed at stopping financial crimes (Aug. 3, 2017)*, https://www.economist.com/the-economist-explains/2017/08/03/the-unintended-effects-of-rules-aimed-at-stopping-financial-crimes.

[63] *Id*.

[64] *Id*.

De-risking became a banking industry strategy primarily as a response to the heavy fines imposed by OFAC for violation of U.S. sanctions. Banking entities would stop providing their financial services "not so much as a legal decision, but rather as a risk management decision."[65] Because banks are unable to identify individual risky actors with accuracy on an efficient basis, these institutions will cut off services "on a wholesale basis" to entire countries, regions, or customers.[66] Preliminary studies show that "smaller emerging markets and developing economies in Africa, the Caribbean, Central Asia…may be the most affected."[67]

Aware of this criticism, one international consortium of regulators, the FATF, issued a supplemental guidance on how to perform KYC or customer due diligence while reducing the problem of "de-risking." The supplement proposed an initiative to support access to basic financial services and products for those who are either underserved or completely unserved. Individuals within those categories (and their transactions) would instead be subject to a less-stringent due diligence regime that could (1) exempt them from AML controls by a showing of their low-risk status; (2) subject them to a simplified due diligence program; or (3) make use of new forms of identify documentation and digital solutions.[68]

Alternative Benefits of AML Compliance

Despite AML / BSA's principal aim – countering funding for terrorism and eliminating bad actors who skirt economic sanctions – there may be other benefits that arise out of the mandatory information disclosures incumbent on financial institutions. Law enforcement officials may be alerted to otherwise unknown instances of criminal behavior through SARs. For example, the criminal investigation into Eliot Spitzer (which culminated in criminal prosecutions for some individuals for sex work) began as a result of North Fork Bank flagging activity on Spitzer's account and filing an SAR.[69] Beyond this dramatic example, law enforcement officials have noted that there may be "soft information" or other details contained in SARs that can assist with law enforcement efforts. This type of information would likely not be contained in know-your-customer or transaction-level data. Given that some criminal investigations rely on building or augmenting a case through iterative reports, it is possible that purely algorithmic ways of dealing with SARs would not be able to utilize this information optimally.

Understanding Blockchain Technology

Given high compliance costs, financial institutions are exploring the possibility of utilizing blockchain technology (specifically an online ledger) as one possible alternative to traditional

[65] Laine, *supra* note 53.

[66] *Id.*

[67] *Id.*

[68] Financial Action Task Force, *Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion with a Supplement on Customer Due Diligence* (Nov. 2017), 2, http://www.fatf-gafi.org/media/fatf/content/images/Updated-2017-FATF-2013-Guidance.pdf.

[69] *FBI Watched Spitzer Before February Incident*, THE WASHINGTON POST (Mar. 12, 2008), https://www.washingtonpost.com/wp-dyn/content/article/2008/03/11/AR2008031100380_2.html?sid=ST2008031102183

compliance.[70] Blockchain technology first appeared in 2009 as the public ledger that recorded Bitcoin transactions.[71] Bitcoins are digital currency traded directly from one user to another (peer-to-peer) which means that there must be some way to verify transactions between two Bitcoin accounts so that the same Bitcoin would not be "spent" twice by the same person.[72] Because Bitcoin was conceived as a way to exchange currency outside of the traditional financial system and without use of a trusted third-party such as a bank to process the transactions, a new technology was created to solve the problems of verification and double spending.[73] This technological breakthrough was the blockchain ledger. The blockchain would replace the trusted third-party and serve as the ledger recording each transaction. It would be able to verify payment history and provide proof of the number of Bitcoins associated with each Bitcoin owner's account at any given moment.[74]

This technology functions as a distributed ledger displaying all transactions to ever occur. For Bitcoin, this blockchain ledger simultaneously exists identically on thousands of computers spread around the world ("nodes") and is made publicly available.[75] Each new Bitcoin transaction is recorded by adding another "block" to the "chain" and is then reflected on the public ledger shared by every node.[76] Despite being open and publicly available, the blockchain is counterintuitively extremely trustworthy and secure because every single node reflects the same ledger at the same time—producing a "consensus mechanism" whereby each of the nodes must be in agreement on how to update the blockchain for each transaction.[77] In this sense, it is the sheer force of thousands of computers being in agreement that makes the blockchain virtually incorruptible and a trusted, public source capable of verifying each transaction.[78] *The Economist* provides a helpful example:

> Let us say that Alice wants to pay Bob for services rendered. Both have Bitcoin "wallets"—software which accesses the blockchain rather as a browser accesses the web, but does not identify the user to the system. The transaction starts with Alice's wallet proposing that the blockchain be changed so as to show Alice's wallet a little emptier and Bob's a little fuller.
>
> The network goes through a number of steps to confirm this change. As the proposal propagates over the network the various nodes check, by inspecting the ledger, whether Alice actually has the Bitcoin she now wants to spend. If everything looks kosher, specialized nodes called miners will bundle Alice's proposal with other similarly reputable transactions to create a new block for the blockchain.[79]

[70] *See* Yassi Bello Perez, *8 Banking Giants Embracing Bitcoin and Blockchain Tech*, COINDESK (July 27, 2015), www.coindesk.com/8-banking-giants-Bitcoin-blockchain/ [perma.cc/VX6S-F45N].

[71] *The Great Chain of Being Sure About Things*, ECONOMIST (Oct. 31, 2015), www.economist.com/news/briefing/21677228-technology-behind-Bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable [perma.cc/KC8S-RZ9N].

[72] *Id.*

[73] *Id.*

[74] *Id.*

[75] *Id.*

[76] *Id.*

[77] *Id.*

[78] *Id.*

[79] *Id.*

But to make the blockchain incorruptible, each block in the chain contains a unique "hash" (a string of digits) which serves as the link between the blocks. Each block connects to the previous block on the chain by including a copy of the previous block's hash. This is replicated all the way back to the initial block on the blockchain.[80] If any single digit is changed, it will result in a different hash for every single block—even in the earliest blocks. Thus, any tampering will necessarily cause a change to the entire chain and will be rejected.[81] As previously mentioned, the blockchain ledger's incorruptibility comes from the fact that it works from consensus—any single node that could be hacked to try to change the ledger would be rejected because it would not be in consensus with the thousands of other ledgers hosted on nodes around the world that are constantly checking for uniformity. Therefore, the only way to fraudulently alter the ledger would be to hack 51% of the nodes at the exact same time using the exact same change in a single block's hash. This is known as the "51% attack" and is thought to be virtually impossible:[82]

> Imagine that Alice changes her mind about paying Bob and tries to rewrite history so that her Bitcoin stays in her wallet. If she were a competent miner she could solve the requisite puzzle and produce a new version of the blockchain. But in the time it took her to do so, the rest of the network would have lengthened the original blockchain. And nodes always work on the longest version of the blockchain there is . . . To force the system to accept her new version Alice would need to lengthen it faster than the rest of the system was lengthening the original. Short of controlling more than half the computers—known in the jargon as a "51% attack"—that should not be possible.[83]

Thus, the true value of the blockchain lies in its use as a verified and trusted ledger.[84] Beyond Bitcoin, blockchain has a number of other potential uses because "the immutability, immediacy and transparency of information captured within a blockchain means that all necessary data can be recorded in shared ledgers and made available in near real time."[85]

Blockchain Technology and AML Compliance Costs

Because of blockchain technology's ability to present the "truth" of a transaction to all parties with access, there have been many proposals about how to best adopt blockchain to other uses. According to Julio Faura, the head of innovation at Santander Bank, "[blockchain's] distributed ledger is [a] very elegant way to solve financial problems" in the financial services industry.[86] Goldman Sachs estimates that blockchain technology for AML compliance mechanisms can save financial institutions an estimated of $3-5 billion.[87]

[80] *Id.*

[81] *Id.*

[82] *Id.*

[83] *Id.*

[84] Cliff Moyce, *How Blockchain Can Revolutionize Regulatory Compliance*, CORP. COMPLIANCE INSIGHTS (Aug. 10, 2016), corporatecomplianceinsights.com/blockchain-regulatory-compliance/ [perma.cc/D9KA-RENB].

[85] *Id.*

[86] Matthew Finnegan, *Why Banks Are Betting On the Blockchain - Not Bitcoin - To Transform The Financial Sector*, TECHWORLD (Aug. 4, 2016), www.techworld.com/e-commerce/why-banks-are-betting-on-blockchain-transform-financial-sector-3621840/ [perma.cc/4JDK-XWRX].

[87] *See* Goldman Sachs, *supra* note 49, at 71.

However, many banks remain skittish about allowing customer information to be stored in such an accessible database. This is where a closed or permissioned blockchain would be useful. While the blockchain technology underlying Bitcoin is a public ledger, the technology can also be adapted to become semi-private or "permissioned." This would allow for a policymaker to theoretically take advantage of a distributed ledger while mitigating privacy concerns by limiting access to certain designated parties.[88] A permissioned blockchain behaves in the same way as a public distributed ledger except that any entity seeking access must be validated or pre-approved.[89] Permissioned blockchains work where there is already an element of trust established between the participants—for instance, financial institutions that already have well-developed relationships.[90] A recent study published by Barclays Bank posited that a permissioned blockchain would be a groundbreaking innovation in the AML space by having a centralized version of the consensus-based "truth" accessible to all relevant parties.[91] Barclays believes this would create a system starkly different from the current AML regime where "every bank, government department and law firm has their own paper copy of the truth."[92] Thus, the centralized ledger could eliminate much of the duplicative work and back-and-forth processes between these entities that cause massive inefficiencies in the AML system.[93] These efficiencies are described below.

When a bank gains a new customer, a litany of due diligence requirements is triggered to ensure the customer is opening the bank account or conducting a transaction for a legitimate purpose. If information about the customer existed in a tamper-proof blockchain ledger that each financial institution could access, many costs incurred to "get to know" the customer could be avoided.[94] As an alternative to the current system, banks could access verified information about a client that is new to *that* bank based on the information pertaining to that customer produced by other financial institutions and stored on the blockchain ledger.[95] In essence, the diligence procedures performed by one bank can be piggy-backed and enhanced by other banks to comply with that bank's own internal procedures.[96] The blockchain would essentially create and store a customer's digital identity for use only by other financial institutions and regulators after the customer's identity and information has been verified once—creating for a client a "digital passport for transacting in financial services."[97] Banks could then amend existing data or upload new information about the customer to the blockchain after each new transaction or when the customer's information has been changed.[98] The blockchain's role would be to provide each institution with "proof-of-process, so all that steps are easily traceable and regulators can be confident about the veracity of the

[88] *See Id.* at 10.

[89] *See Id.*

[90] *See Id.*

[91] SIMON TAYLOR, BARCLAYS BANK PLC, BLOCKCHAIN: UNDERSTANDING THE POTENTIAL 3 (2015), www.barclayscorporate.com/content/dam/corppublic/corporate/Documents/insight/blockchain_understanding_the_potential.pdf [perma.cc/BBF7-QE58]

[92] *Id.*

[93] *See Id.*

[94] *See* Moyce, *supra* note 79.

[95] *See Id.*; Matthew Britton, *Could Blockchain Solve the KYC/AML Challenge?*, BCS Consulting (Sept. 29, 2016), www.bcsconsulting.com/blog/new-technology-can-enable-human-bank/ [perma.cc/FC74-7AE6].

[96] *See* Moyce, *supra* note 79.

[97] Britton, *supra* note 90.

[98] *See Id.*

information."[99] Conversely, in the current system, it is estimated that KYC requests can take 30 to 50 days to complete satisfactorily[100] and involve duplicative work by multiple institutions. These banks have to obtain and verify copious amounts of documentation each time the same customer opens up an account with a new financial institution. Furthermore, using a blockchain for customer-related compliance processes may benefit bank customers as well. A recent study by Bain concluded that bank customers are also frustrated by the current KYC system whereby they have to provide the same documentation to different banks and wait weeks for access to a new account.[101]

Beyond reducing client on-boarding costs, blockchain technology can also assist with other AML compliance demands on a transaction-by-transaction basis. Those critical of the current AML scheme argue that the present approach encourages banks to hire excess employees and invest too much money in AML compliance despite a lack of certainty on the current regime's efficacy.[102] The current system forces employees to comb through a financial institution's records to check whether the transactions were suspicious—with much of this process duplicated on both sides of a single transaction.[103] These critics posit that blockchain technology would allow banks on both ends of a transaction to quickly verify the credentials of all parties to a transaction.[104] Furthermore, with all of the transaction data stored and verified on the distributed ledger, it may be easier for banks and regulators to use algorithms to analyze and detect suspicious patterns and payments at an aggregate level.[105] This permissioned blockchain would not only hinder the ability of criminals to use financial institutions for illegal transactions, but also allow banks to fully take advantage of a Section 314(b) sharing program to immediately alert fellow institutions about suspicious activity.[106] If a bank discovers a suspicious transaction, then each bank where the customer has an account could be immediately alerted to prevent future suspicious transactions.[107] Using such a system, stakeholders would no longer receive post-hoc reports about isolated or individual transactions but would instead be able to monitor entire sets of aggregate transaction data in real time.[108]

Proponents of adopting blockchain note that regulators would also stand to benefit greatly from this technology.[109] Regulators would also be able to view each transaction posted on the blockchain as it occurs.[110] Proponents argue the blockchain would allow regulators to take a more proactive approach to analyzing suspicious transactions or patterns alongside or in tandem with banks.[111] By having more eyes on the system at any given time, the probability of detecting illegal activities likely increases, too. Thus,

[99] Moyce, *supra* note 79; *see also* Britton, *supra* note 90.

[100] JEREON VAN OERLE & PATRICK LEMMENS, ROBECO, DISTRIBUTED LEDGER TECHNOLOGY FOR THE FINANCIAL INDUSTRY 13 (2016), www.robeco.com/images/201605-distributed-ledger-technology-for-the-financial-industry.pdf [perma.cc/74ND-ZJTA].

[101] *See* Matthias Memminger, Mike Baxter & Edmun Lin, *You've Heard of Fintech, Get Ready for 'Regtech'*, AM. BANKER (Sept. 7, 2016), www.americanbanker.com/bankthink/youve-heard-of-fintech-get-ready-for-regtech-1091148-1.html [perma.cc/CA3W-PVZ8](noting also that "Half to three-quarters of onboarding requests never reach the final stage of account opening" wasting customers' time and effort).

[102] *See* Zafar, *supra* note 28.

[103] *See Id.*

[104] *See Id.*

[105] *Id.*

[106] *See Id.*

[107] Britton, *supra* note 90.

[108] *See* Moyce, *supra* note 79; Zafar, *supra* note 28.

[109] *See* Moyce, *supra* note 79.

[110] *See Id.*

[111] *See Id.*

proponents conclude that this technology could dramatically reduce the time and effort currently spent on compliance, and, therefore, halt the growth of compliance costs while also "improving the quality, accuracy and confidence of and in the process."[112]

Financial Institutions and Start Ups Exploring Blockchain Use for KYC/AML

A number of startup companies have begun to harness the technology underlying Blockchain to build tools that could be used by banks and regulators to make compliance more efficient.[113] Some firms, such as Elliptic and Coinfirm, are using blockchain technology with an eye towards solving AML problems at financial institutions.[114] Another startup, Gem, is focused on digital identities and believes that it has potential applicability for AML compliance use in financial institutions.[115]

In addition, many established financial institutions, including Barclays, UBS, Deutsche Bank, Santander, and Bank of America,[116] are exploring ways to utilize blockchain technology either by developing their own technology or partnering with blockchain-based firms.[117] Bank of America has already applied for 15 blockchain-based patents.[118] Even IBM has entered into the KYC blockchain world by successfully testing blockchain-based KYC technology with the French banking and insurance group Crédit Mutuel Arkéa.[119]

Blockchain Technology: Enabling Money-Laundering?

Despite promising applications of blockchain technologies, certain aspects of cryptocurrencies specifically may also hinder anti-money laundering efforts. For example, to open an account with a traditional bank, a customer must provide a government-issued photo ID or other identity-verifying documents. In contrast, to create a Venmo account, a customer merely signs up using a phone number and email address.[120] In this example, this new technology may lower the barriers to accessing financial services for certain "risky" individuals and actually contribute to financial inclusion.[121] However, the anonymous nature of many of these new financial technologies could make it more difficult to detect,

[112] *Id.*

[113] *See* Accenture, Distributed Consensus Ledgers for Payment (2015), www.accenture.com/t20151002T010405__w__/us-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub_22/Accenture-Banking-Distributed-consensus-ledgers-payment.pdf [perma.cc/B9EH-KSBD].

[114] *See id.*; Richard Kastelein, *Coinfirm and Billon Team Up to Better Blockchain AML and Compliance*, Blockchain News (Sept. 3, 2016), www.the-blockchain.com/2016/09/03/coinfirm-billon-team-better-blockchain-aml-compliance/ [perma.cc/5JUP-UG5Y].

[115] *See* Bryan Yurcan, *How Blockchain Fits into the Future of Digital Identity*, Am. Banker (Apr. 8, 2016), www.americanbanker.com/news/bank-technology/how-blockchain-fits-into-the-future-of-digital-identity-1080345-1.html [perma.cc/U858-5EBF].

[116] *See id.*; Alice Woodhouse, *Blockchain Technology Can Help Banks Beat Money-Laundering, Hong Kong Regulator Says*, S. China Morning Post (June 8, 2016), www.scmp.com/business/banking-finance/article/1969769/blockchain-technology-can-help-banks-beat-money-laundering [perma.cc/RB7L-K366].

[117] *See* Finnegan, *supra* note 81.

[118] Woodhouse, *supra* note 111.

[119] Avi Mizrahi, *IBM Successfully Tests Blockchain KYC with France's Crédit Mutuel Arkéa*, Fin. Magnates (June 30, 2016, 2:53 PM), www.financemagnates.com/cryptocurrency/innovation/ibm-successfully-tests-blockchain-kyc-with-frances-credit-mutuel-arkea/ [perma.cc/FJ6E-9E4V].

[120] Venmo, How to Sign Up, https://help.venmo.com/hc/en-us/articles/209690068-How-to-Sign-Up.

[121] World Bank, FinTech and Financial Inclusion, http://pubdocs.worldbank.org/en/877721478111918039/breakout-DigiFinance-McConaghy-Fintech.pdf

trace or enforce penalties for illegal transactions utilizing such technology. One other worry that some financial institutions could raise is the possibility that they could be exposed for past failures highlighted by successful newer technologies.

Regulatory Reaction

Former Comptroller of the Currency Thomas J. Curry responded positively and stated these new technologies afford ways to reduce costs and increase efficiency of AML compliance.[122] The Office of the Comptroller of the Currency is one of the U.S. financial regulatory agencies in charge of monitoring and enforcing BSA compliance for national banks. However, other financial regulators have reacted more mildly and noted some concerns. The Consumer Financial Protection Bureau has raised general concerns that vendors providing compliance-related services are too slow to adopt their technology to meet regulatory requirements.[123]

Some foreign regulators have taken a more accommodating stance regarding adopting blockchain to solve financial services compliance problems. The U.K. Financial Conduct Authority (FCA) is actively exploring potential uses of blockchain technology for financial services companies to meet U.K. AML obligations. Christopher Woolard, an executive member of the FCA Board, recently stated that the FCA is "particularly interested in exploring whether block chain technology can help firms meet know your customer or anti-money laundering requirements more efficiently and effectively," and that "we are engaged in discussions with government and industry on this issue."[124] Similarly, Benedicte Nolens, a former Senior Director at the Hong Kong Securities and Futures Commission, recently stated that blockchain has a real opportunity to address a "pretty significant inefficiency" with the current AML system by removing duplicative efforts and creating a record of all checks carried out for each client.[125] However, some foreign regulators echoed the CFTC and similarly urged caution. Nolens qualified her statements by directing financial institutions to ensure that any technology they are using is compliant with the rules as regulations can be slow to catch up to innovative technology.[126] The Bank of England, England's central bank, noted with respect to blockchain technology that "[f]urther research would also be required into how digital identity management could be achieved while balancing privacy considerations."[127]

Most U.S. regulators are thus far taking a somewhat measured approach when it comes to blockchain technology, which has led some commentators to state that regulatory acceptance faces an "uphill battle."[128] At a recent conference, David Mills, Assistant Director of Operations and Payment

[122] *See* Katie Wechsler & Zachary Luck, *The Federal FinTech Promised Land*, 19 Fintech L. Rep. 2 (August 2016).

[123] *See Id.*

[124] Christopher Woolard, Fin. Conduct Authority Dir. of Strategy and Competition, Speech at the FCA UK FinTech: Regulating for Innovation Conference (Feb. 22, 2016), www.fca.org.uk/news/speeches/uk-fintech-regulating-innovation [perma.cc/AN5B-ZCD9].

[125] Woodhouse, *supra* note 111.

[126] *Id*.

[127] BANK OF ENG., OPEN BANK RESEARCH AGENDA 31 (2015), www.bankofengland.co.uk/research/Documents/onebank/discussion.pdf [perma.cc/N2BE-S5ZG].

[128] Henry Engler, *Blockchain Faces Maze of Regulatory Complexities, Questions and Challenges*, Thomson Reuters (Feb. 23, 2016) , blogs.thomsonreuters.com/answerson/blockchain-faces-maze-of-u-s-regulatory-complexities-questions-and-challenges/ [perma.cc/F6EN-8GM2].

Systems at the Federal Reserve, noted that there were a number of risks associated with the use of such technology. He cautioned that we need to "understand the limits of rich information and the tradeoff over the privacy of individuals…[w]e need to strike a balance between the two."[129] Mills also sympathized with the notion that there appears to be a lack of consensus among the regulators with respect to blockchain technology but said regulators are eager to learn more about it.[130]

Finally, while FinCEN has not officially weighed in on using blockchain for AML compliance, a 2015 FinCEN enforcement case against a blockchain company may provide insight into the thinking at one point in the past. Ripple Labs was a startup that used blockchain technology to process and settle transactions between financial institutions. According to the company, "Ripple solutions lower[ed] the total cost of settlement by enabling banks to transact directly, instantly and with certainty of settlement."[131] However, FinCEN stated Ripple violated AML requirements.[132] Ripple was given a $700,000 fine—a significant blow for a startup company—and ordered to enhance its AML compliance across its platform.[133] Many industry observers opined that FinCEN's enforcement action had the potential to create a chilling effect on bank partnerships with blockchain-based companies.[134] While Ripple's use of blockchain was not intended as an AML compliance tool, this enforcement action still illustrates the difficulties that banks face when adopting new and uncertain technology.[135]

Conclusion and Instructions

The director of FinCEN would, above all, like to hear your recommendation about (1) potential reforms that could improve the current AML compliance scheme; and (2) specifically, whether blockchain (or other technologies) should be seriously considered as one possible solution to AML compliance costs. Please also note that financial institutions will be hesitant to adopt the technology without it first being approved by regulatory bodies.[136] Please also consider how your proposed reform fits into the current liability regime. In addition, please acknowledge how issues over privacy, security, or financial inclusion issues may affect your answers.

Please consider the following questions when creating your presentation:

- Does the Academic Proposal (specifically, Sections 3 and 5) in Appendix I provide a satisfactory solution to fix the problems of the current regime?
    - Concretely, would you recommend that FinCEN or some governmental agency create a centralized CDD agency? If so, should it be controlled or run by (a) the government; (b) an industry group; (c) financial institutions themselves; or (d) some other "gatekeeper" or regulator?

[129] *Id.*

[130] *Id.*

[131] *Company*, RIPPLE (last visited Oct. 30, 2016), ripple.com/company [perma.cc/76ZW-FV64].

[132] *See* Sarah Todd & Ian McKendry, *What Ripple's FinCEN Fine Means for the Digital Currency Industry*, AM. BANKER (May 6, 2015), www.americanbanker.com/news/bank-technology/what-ripples-fincen-fine-means-for-the-digital-currency-industry-1074195-1.html [perma.cc/YQP9-AXE3].

[133] *See Id.*

[134] *See Id.*

[135] *See* Goldman Sachs, *supra* note 49, at 77.

[136] *See Id.*

  - Should legislative or administrative actors modify the current liability regime?
  - Should the standards for due diligence be changed in any way?

- If a centralized shared database is adopted, what would be the scope of the information shared and how would this new system apportion liability amongst responsible actors (which could potentially include FinCEN itself)?
  - Relatedly, what sets of information that financial institutions hold ought to be shared (or put into a centralized database)? What are the merits or drawbacks of more or less information being stored in such a system?
- How might other current technological developments apart from Blockchain affect your judgment on the proposed reform? Are those other technologies or modifications to a pure blockchain approach (e.g., permissioned ledgers, machine learning, etc.) that could serve either as complements to or substitutes for the proposed reforms contained in the Appendix materials?

Appendix I – Academic Proposals

Executive Summary

1. The current AML regime forces regulated entities to incur huge compliance costs, yet seemingly generates unsatisfactory results.
2. Two potential reasons that the regime may generate low quality of information could be (a) that the system incentivizes defensive filing, and (b) pushes customers outside the legal banking sector due to "de-risking."
3. This proposal suggests that policymakers adopt an act-based liability regime for violations of Customer Due Diligence ("CDD") requirements.
4. Entities that fail to file Suspicious Activity Reports ("SARs") should be held strictly liable for these errors to prevent inefficient outcomes.
5. Blockchain technology both enables money-laundering schemes via cryptocurrencies but may also provide tools, such as a distributed-ledger system, which could strengthen AML programs by increasing information sharing.
6. Relatedly, this proposal suggests that CDD should be conducted centrally to reduce costs stemming from redundancies, either by a formal governmental agency or by a distributed blockchain ledger.
7. A private cause of action holding banks liable to customers for SAR-related delays should be introduced to decrease defensive filing of SARs.

Theoretical Foundations of AML Law

Economics are one possible framework that can be used (and is used in this proposal) to analyze motivations leading to criminal behavior. According to famous economist Gary S. Becker, criminals commit crimes when the expected return of committing a crime outweighs its expected sanction (probability of imposition of penalties multiplied by the magnitude of actual sanctions).[137] As a result, it is intuitive to combat crime by diminishing potential or proceeds from committing a crime and/or by imposing sufficient penalties on people.

In microeconomic terms, laundering money provides criminals with a means to convert their illegal funds into legal funds that increase their purchasing power by virtue of its higher purchasing power.[138] Because illegal funds cannot directly be used for investment or consumption, they only store "potential" purchasing power, whereas funds that have been laundered and are now legal *can* be spent directly, and now contains "actual" purchasing power. Even absent anti-money laundering laws, criminals may still have difficulties publicly spending their cash. In addition, criminal organizations need to wash their illicit income to escape potential detection and confiscation.

[137] *See* Gary Becker, *Crime and Punishment: An Economic Approach*, 76 J. POL. ECON. 169, 183 (1968).

[138] Donato Masciandaro, *Economics of Money Laundering: A Primer*, 2 (Paolo Baffi Ctr. Bocconi Univ. Working Paper No. 171), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=970184, [reader may require academic or account access].

Two separate events that affect the ultimate end result for the criminal must be analyzed. First, the criminal must decide whether to launder their money. If they decide to engage in money laundering, a second event determines the outcome–whether law enforcement will detect the laundering.[139] Laundering money provides a potential benefit to the criminal who can now reinvest illicit profits into lawful, profitable activities. The cost to the criminal of the laundering is the increased probability of detection as well as an additional sanction for the laundering activity itself. This model predicts that money laundering is positively associated with the amount of illicit gain, together with the relative profitability of money that is reinvested in other profitable activities, as compared to the lesser profitability of dirty money. Money laundering is negatively associated with the risk of detection of the crime, the severity of sanctions, and costs incurred at the first money laundering stage.[140] To combat money laundering, governments should increase the probability of detection, impose higher sanctions, and increase costs faced by money launderers. Anti-money laundering is necessary to prevent criminal activity from flourishing because of the increased value of newly cleansed money.

In most circumstances, however, money laundering is not performed by the same criminals who committed the underlying crime, but instead is performed by "professional money launderers." The separation of the role of money-laundering from the role of committing an underlying criminal act effectively professionalizes the business of money-laundering. The model must account for the interaction between criminals and money launderers.[141] Thus, the model ought to be expanded into a three-stage model by adding a "bargain process" between criminals and money launderers.[142] Now, the model contains three important stages that all affect the outcome for the criminal actor: (1) the decision to launder (or not); (2) how the proceeds will be allocated between the criminal and the launderer; and (3) whether law enforcement catches the illegal laundering. The expansion of the model also introduces two new variables that must be considered: (1) actions that deter *money launderers*, separate and apart from the criminal who committed the initial crime, and (2) the probability of detection of money laundering processes. Both deterrents have a negative effect on money laundering.[143] However, the latter has a weaker effect than the former because it has more of an impact on distribution of gains between criminals and money launderers, rather than the total amount of money laundering gains.[144]

This microeconomic model also has macroeconomic implications. From a macroeconomic perspective, all illicit gains can be spent in three ways: (1) consumption, (2) investment in the illegal sector, or (3) investment in the legal sector. Unless the actor who received illicit gains chooses to consume those gains, the wealth accumulated must be laundered at least once. The model predicts, therefore, that without some other actor stopping money laundering, criminals can continually accumulate wealth by laundering and reinvesting. This model indicates that the only way to stop such a cycle is to enact laws that increases the cost of money-laundering to the criminals or money launderers.

[139] Masciandaro, *infra* note 18, at 9.

[140] *Id.* at16.

[141] Killian J. McCarthy et al., *Modeling the money launderer: Microtheoretical Arguments on Anti-Money Laundering Policy*, 43 INT'L REVIEW L. & ECON., 148, 149-150 (2011), [reader may require academic or account access].

[142] *Id.* at 151-152.

[143] *Id.* at 151.

[144] *Id.* at 154.

The models introduced above have rationalized the current anti-money laundering law regime. On top of criminal deterrence, which is shouldered by traditional criminal law, there are two prongs of anti-money laundering laws—criminalization and regulation. On one hand, the government criminalizes money laundering, which is devoted to deterring professional money launderers as well as increasing the severity of sanctions. On the other hand, the government sets rules for financial institutions and delegates reporting obligations to them for detecting suspicious transactions. The regulation of financial institutions increases the cost of money laundering and enhances the probability of detection.

The Functioning of AML Laws

As introduced above, it may pay to impose sanctions only on financial institutions which have facilitated the money laundering process. These sanctions would increase the cost of laundering money for the individual customers that launder money. However, it would require financial institutions to report too many suspicious transactions.

According to Becker's theory, a rational, risk-neutral wrongdoer with unlimited-assets is indifferent to any combination of detection probability and expected sanction so long as the multiple of those factors remains the same. However, the cost of any given combination has different outcomes for a law enforcement agency. This is because the financial costs incurred by law enforcement to slightly increase the chances of detection (e.g., investment in more employees reviewing transactions) is higher than a marginal increase in fines or penalties that would be imposed on criminals for laundering money. This disparity between the costs of two methods of reducing the amount of money laundering implies that the state should maximize financial penalties that launderers would suffer in order to save on costs of having to invest in alternative and burdensome methods that increase the probability of detection.[145] Essentially, it is a better payoff for the government to simply increase the fines for money laundering as opposed to increase its spending on detection mechanisms, given that these are both ways that the government can reduce the amount of money laundering that a rational actor would undertake. However, in the real world, a rational actor can have limited assets and may be quite risk-averse. The former feature introduces the judgment-proof problem and the cost of imprisonment, and the latter generates unwanted overdeterrence.[146] Both features, combined with the concern of marginal deterrence,[147] make the high-sanction-low-probability combination less appealing. Hence, this model suggests that policymakers must (and inevitably will) focus on enhancing the chances of detection rather than simply increasing penalties.

Because the investment in enhancing the probability of detection is necessary, the state should shift its focus on how to increase detection at the lowest cost. One solution is to introduce a gatekeeper into the regulatory regime in an effort to improve the likelihood of detection at a lower cost. This would be successful if the gatekeeper has more information or ability than the State. In order for the information-sharing performed by the gatekeeper to be economically efficient, that gatekeeper must satisfy four conditions (as outlined by Professor Kraakman): (1) efficacy, (2) cost, (3) comparative advantage, and (4)

[145] *Id.*

[146] *See generally,* Steven Shavell, Foundations of Economic Analysis of Law (2004).

[147] *Id.*

private enforcement incentives.[148] Today, private-sector gatekeepers are common in our legal system, such as corporations in the context of corporate crime[149] or professionals in the context of initial public offerings.[150]

Banks and other reporting entities not only fit the aforementioned requirements of efficient gatekeepers, but may be better gatekeepers. The first two advantages arise out of the fact that banks must report transactions merely based on suspicion, rather than based on some higher standard such as negligence or knowledge. Given that banks are unlikely to have invested much into any particular transaction at the time at which they analyze a transaction for being "suspicious," they may have less of an incentive to finalize that transaction. In addition, if banks must have a high level of information and subjective intent in order to be liable for a failure to report suspicious activity, that could create a perverse incentive whereby banks may refuse to examine transactions in order to avoid ever obtaining the amount of information that could make them liable for failures to report illegal transactions. Instead, having a very low reporting threshold based on mere suspicion, instead of knowledge or negligence, can mitigate perverse effects that prevent banks from knowing details of transactions to escape from their liability.[151] Finally, the immunity granted to institutions that simply report suspicious activity provides certain ex-ante incentives that encourage banks to share and collaborate on information.[152] In sum, banks as gatekeepers are not only efficient in generating information at a lower cost for the law enforcement, but are "collaborative" ones who may have superior incentives to share information as compared to other potential gatekeepers.

International Actions and Recent Development

The rigorous development of international trade and the resulting capital liquidity around the world has called for global collaboration on enacting and enforcing AML laws. As a response, the G-7 countries formed the Financial Action Task Force (FATF)[153] which issued 40 Recommendations which comprise a framework of measures which countries should implement to combat money laundering and other ills. Some Recommendations imposed the gatekeeper liability on banks and other financial institutions for failing to conduct CDD or file SARs to combat laundering.[154]

The FATF and similar regional bodies such as the Asia/Pacific Group (APG) regularly conduct mutual evaluations of member state financial institutions which include on-site visits. If a member state is found to have incomplete or unsatisfactory compliance with certain international standards, then that member state will be put on a watchlist and risks negative consequences. Even though member states try to achieve full compliance, the cost-effectiveness of programs said to meet the full compliance level is

[148] Reinier H. Kraakman, *The Anatomy of a Third-Party Enforcement Strategy*, 2 J. L. ECON. & ORG. 53, 57 (1986).

[149] *See generally,* Jennifer Arlen & Reinier Kraakman, Controlling Corporate Misconduct: An Analysis of Corporate Liability Regimes, 72 N.Y.U. L. REV. 687 (1997); A. Mitchell Polinsky & Steven Shavell, Should Employees be Subject to Fines and Imprisonment Given the Existence of Corporate Liability?, 13 INT'L REV. L. & ECON. 239 (1993); Alan O. Sykes, The Economics of Vicarious Liability, 93 YALE L. REV. 1231 (1984); Lewis Kornhauser, An Economic Analysis of the Choice Between Enterprise and Personal Liability for Accident, 70 CAL. L. REV., 1345 (1982).

[150] *See e.g.,* John C. Coffee, Jr., Gatekeeper Failure and Reform: The Challenge of Fashioning Relevant Reforms, 84 B.U. L. REV. 301, 301-364 (2004).

[151] *Id.* at 802-803.

[152] *Id.* at 841-843.

[153] Fin. Action Task Force (FATF), *Who We Are*, http://www.fatf-gafi.org/about/ (last visited:03/31/2019).

[154] Fin. Action Task Force (FATF), *The 40 Recommendations*, 2004, http://www.fatf-gafi.org/media/fatf/documents/FATF%20Standards%20-%2040%20Recommendations%20rc.pdf (last visited:03/31/2019).

unknown. The compliance program has incurred glaring social costs, the burden of has fallen on banks and society.[155] Fearing harsh penalties,[156] banks either withdraw their business from high-risk areas (called "de-risking") or invest more in compliance.[157] De-risking leaves those unbanked to suffer from less access to banking service and forces them to use the shadow banking system.[158] The limited access to legitimate banking service, together with the proliferation of shadow banking, burdens society with high social costs. Alternatively to de-risking, banks are forced to invest an unprecedentedly high amount of money in AML compliance.[159]

These costs appear unjustifiable given studies which show the limited effectiveness of the current AML regime. First, the estimated amount of laundered dirty money has remained 2-5% of global GDP per year since 1998,[160] which suggests that AML efforts have had minimal impact. Second, more than half of the FATF member states receive low evaluation scores on the tests of CDD (Recommendation 10) and SARs (Recommendation 20).[161] The low scores likely indicate the standard is unachievable because banks have already invested heavily in compliance efforts. Both unsatisfactory outcomes call for a thorough investigation of the current AML regime.

Problems

Banks have far more knowledge and information than governmental regulators regarding bank customers and their money flows. This advantage should put banks in a better position to detect suspicious activities. According to the model above, the current regime is inefficient because of a number of problems, including but not limited to high compliance costs and expenses, the low quality of available information, draconian penalties for non-compliance, and decreased financial inclusion of unbanked or under-banked populations.

[155] Martin Gill & Geoff Taylor, *Preventing Money Laundering or Obstructing Business? Financial Companies' perspectives on 'Know Your Customer' Procedures*, 44 BRIT. J. CRIM. 582, 582-594 (2004) (showing the banking industry's reaction to know-your-customer program).

[156] In 2018, an aggregate of $771.26 million in BSA/AML monetary penalties were assessed against 13 financial institutions. *See* BankersOnline, *BSA-AML Civil Money Penalties*, https://www.bankersonline.com/penalty/penalty-type/bsa-aml-civil-money-penalties (last visited:03/31/2019).

[157] Fin. Action Task Force (FATF), *FATF Clarifies Risk-Based Approach: Case-By-Case, Not Wholesale De-Risking* (23/12/2014), http://www.fatf-gafi.org/documents/news/rba-and-de-risking.html (last visited: 03/31/2019); Fin. Action Task Force (FATF), *Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion* (11/2017), http://www.fatf-gafi.org/media/fatf/content/images/Updated-2017-FATF-2013-Guidance.pdf (last visited: 03/31/2019).

[158] Fin. Action Task Force (FATF), *FATF Clarifies Risk-Based Approach: Case-By-Case, Not Wholesale De-Risking* (23/12/2014), http://www.fatf-gafi.org/documents/news/rba-and-de-risking.html.

[159] KYC360, *Anti-Money Laundering Compliance Costs Hit $25 Billion Annually–Study* (10/16/2018), https://kyc360.com/news/anti-money-laundering-compliance-costs-u-s-financial-services-firms-25-billion-annually-study/; LexisNexis, *The True Cost of Anti-Money Laundering Compliance–European Edition* (09/2017), https://risk.lexisnexis.com/global/-/media/files/corporations-and-non-profits/research/true-cost-of-aml-compliance-europe-survey-report-pdf.pdf (last visited: 03/31/2019). (estimating the U.S. banks have invested more than $25 billion and the European banks are investing more than $83.2 billion in AML compliance), [reader may require academic or account access].

[160] U.N. OFF. DRUGS & CRIME, MONEY LAUNDERING AND GLOBALIZATION, https://www.unodc.org/unodc/en/money-laundering/globalization.html (last visited: 03/31/2019); Michael Camdessus, *Money Laundering: the Importance of International Countermeasures* (02/10/1998), https://www.imf.org/en/News/Articles/2015/09/28/04/53/sp021098 (last visited: 03/31/2019); *See* also Ali Alkaabi, George Mohay, Adrian McCullagh & Nicholas Chantler, *A Comparative Analysis of the Extent of Money Laundering in Australia, UAE, UK and the USA*, SSRN 3 (2010) (summarizing and tabulating previous estimations from 1995 to 2009), https://ssrn.com/abstract=1539843, [reader may require academic or account access].

[161] Fin. Action Task Force (FATF), *Consolidated Table of Assessment Ratings*, FATF (03/01/2019), http://www.fatf-gafi.org/media/fatf/documents/4th-Round-Ratings.pdf (last visited: 03/31/2019).

High Compliance Costs

To comply with AML standards, banks must conduct both customer due diligence (CDD) and process and file suspicious activity reports (SARs), both very costly requirements. For example, to conduct CDD, banks must hire and train more front-line staff to collect documents provided by customers as well as verify their accuracy. Moreover, the AML regimes not only require basic *first-time* due diligence but an *ongoing* CDD process for all customers. In addition, enhanced CDD processes must be created for specific customers who present a higher risk of potential money-laundering activities, such as politicians and their relatives.

SAR filing imposes another significant cost on banks. There are far more transactions that occur than the number of customers a bank serves. Moreover, the information regarding transactions is more monotonic and computerized. Hence, it is less practical to analyze this kind of information by human effort. Modern technologies and algorithms can perform these analyses, but the required technology is expensive and specialized. Banks either purchase software from outside vendors or develop their own systems; both approaches require considerable investment and constitute large financial burdens for small depository institutions, such as saving and loan companies or local credit unions. These smaller institutions may not even fully exploit the advantage of “big data” while paying a similar price.

Low Quality Information

Banks, when collecting information on behalf of law enforcement, generate information that is of minimal value. This occurs for two reasons. First, it is objectively true that the current AML compliance regime cannot possibly completely identify all money launderers or identify (and prosecute) all illegal transactions. Facing considerable amounts of information, it is neither practical nor cost-effective for banks to catch all money launderers. Moreover, money launderers are sophisticated actors constantly attempting to circumvent banks’ practice and secure their illegal proceeds. Banks may be able to ascertain some patterns which money launderers are likely to follow, and use those to identify customers or transactions that match such patterns. However, those patterns may not adequately characterize all money laundering methods and sometimes mistakenly capture legal transactions. Such obstacles are external limits on the quality of information generated by banks.

The combination of a legal standard of “suspicion” coupled with immunity for banks subjectively disincentivizes financial institutions to improve information quality. The suspicion standard is a double-edged sword. On one hand, it permits banks to report transactions, without certainty of their illegality which results in the transmission of more information to law enforcement.[162] On the other hand, it may reduce the value of information within SARs. The financial regulator has a limited capacity to review all reports and now receives even more information from banks, which may dilute the value of information received. Banks may even be incentivized to file defensive reports, not only to evade liability stemming from alleged failures to report,[163] but also to lower the probability of being detected by law enforcement.

[162] Gadinis, *supra* note 4, 802.

[163] Előd Takáts, A Theory of "Crying Wolf": The Economics of Money Laundering Enforcement, 27 J. L. ECON. & ORG. 32, 59-60 (2011).

Draconian Penalties

High penalties may also lead to inefficient AML outcomes. Generally, to achieve optimal deterrence, the law enforcement agency sanction or penalty should be adjusted for the probability of law enforcement detection and imposition of the sanction, such that the expected sanction is equal to the amount of social harm created. In the context of AML, the penalties that could be imposed on banks to induce them to collaborate on AML should match the social harm this collaborative effort would have been able to deter. In an ideal world, simply setting penalties at an extremely high level because rational players always behave optimally when the *expected* sanction is set equal to the harm created.

In the real world, however, federal agencies have imperfect information. They may miscalculate the amount of harm or the probability of detection by law enforcement. This could cause them to set the sanction at a level that is above the optimal sanction amount. In a fault-based regime, such a scenario could lead to either over- or under-enforcement when a law enforcement agency fails to observe real behavior (or receive perfect information) and erroneously finds a bank negligent. This failure to observe real behavior forces banks to take rational, but socially undesirable, actions to hedge against this overenforcement. Banks would likely go through a heightened scrutiny process that might be inefficient or even useless only to persuade law enforcement of bank compliance. They would also file more reports to be immune from uncertain liability. The inefficiency associated with the law enforcement agency's error is exacerbated by harsh penalties. Consider the following example:

> **Example 1.** Let us assume that the economically efficient, or optimal investment, in CDD compliance for a bank is $10 million. The penalty imposed on noncompliant banks is $150 million with a probability of 10% that law enforcement detects the noncompliance and imposes the penalty. Thus, from the perspective of the bank, the expected cost of noncompliance (financial sanction of $150 million multiplied by the 10% probability of its imposition) is $15 million. However, the law enforcement agency is unable to perfectly estimate the bank's expenditures on compliance. Rather, they might overestimate (50% chance) or underestimate (50% chance) this figure because they do not know exactly how much money the bank will invest in its anti-money laundering procedures. The misperception is symmetric, and we will assume that their error in estimation comes out to be 30% of the actual investment in compliance. That is, when a bank actually invests $10 million in CDD compliance, it is equally probable that the government perceives their investment as $7 or $13 million.

In the above case, if law enforcement overestimates the amount of money banks have invested in compliance, that does not lead to an inefficient outcome because law enforcement's error will not result in a sanction and will not increase the expected costs that the bank will incur. However, if law enforcement *underestimates* this figure, the bank would expect to suffer a $15 million fine. Now, the actual cost for banks is $17.5 million. The actual cost is calculated by adding the original investment of $10 million plus the potential expected sanction. The expected sanction is equal to the amount of the sanction ($150 million) multiplied by the probability of detection by law enforcement (10%) multiplied by the probability that law enforcement has underestimated the amount the bank has invested in compliance (50% or .50).

This suggests that banks may try to increase their investment in compliance to account for the possibility of law enforcement's estimation error. Now, they will invest $14.28 million (or $10 million divided by the probability of 70%). This amount of compliance is still less than the amount they would pay if they invested $10 million and were fined, however, it creates $4.28 million of dead weight loss or waste because the *optimal* amount of deterrence is $10 million, but the bank is spending an additional $4.28 million without seeing an appropriate increase in deterrence for this effort. Nevertheless, if the sanction is lowered from $150 to $120, banks would invest zero and expect to pay a $12 million penalty ($120 million multiplied by the 10% probability of imposition with no chance of estimation error by the government) which still creates waste of $2 million (although less than $4.28 million). As a result, more lenient (but still efficient) penalties can mitigate inefficient investment due to law enforcement error. In contrast, draconian penalties exacerbate the inefficiencies generated by the bank when the government is unable to accurately or perfectly estimate the bank's compliance effort.

On top of the inherent problem of interaction between harsh penalties and court error, draconian penalties are also intertwined with the second problem, low quality information. As mentioned above, when penalties are set sub-optimally high, banks are inclined to invest more in compliance programs and file more defensive reports, resulting in additional low-quality information. Even more disturbing, when more defensive reports are filed and the probability of detection is lowered because of limited resources available to law enforcement or financial crime regulators, sanctions would normally be raised to restore reduced deterrence effect. This results in a vicious cycle. As a result, the scale of penalties should be scrutinized.

Please note that the above example is replete with assumptions in order to create a more simplistic model that allows us to scrutinize the effect of large financial penalties on different actors' decisions. In reality, a number of other important factors (not considered here) play a role in the decision-making process. For example, financial institutions must decide the amount of spending on lobbying, actuarial analyses, litigation–all of which likely affect how much a given bank decides to invest into compliance with CDD measures. Likewise, regulatory bodies also have to navigate a set of interrelated decisions concerning maximizing penalties, retaining sanction funds, and securing political support for its budgetary requests.

Decreased Financial Inclusion

One last problem brought by AML enforcement is reduced financial inclusion. According to The World Bank, financial inclusion means that: "…individuals and businesses have access to useful and affordable financial products and services that meet their needs—transactions, payments, savings, credit and insurance—delivered in a responsible and sustainable way." [164]

In big cities, financial inclusion is rarely an important issue. However, isolation from financial services is a pervasive and important problem for people in underdeveloped countries or rural areas in developing countries. Those excluded indirectly suffer from AML enforcement because when banks are faced with harsh penalties but have no effective way to enact compliance programs that save them from sanctions, banks will reduce the number of customers they serve based on their risk. As AML requirements get stricter, even law-abiding customers may have difficulty providing the appropriate documentation to verify their identity. While it may be easy to prove identity or verify income in countries that publicly store

[164] The World Bank, *Financial Inclusion: Overview*, https://www.worldbank.org/en/topic/financialinclusion/overview.

information (or using easy-to-access and reliable private information such as a pay stub), there are, nonetheless, cases where people lack official or privately-issued documents to support their identification (*e.g.*, self-employed farmer in Southeast Asia). When the law becomes stricter, banks abandon such customers to prevent further risk of being punished. Such abandonment is called "de-risking," which has substantially reduced financial inclusion. People who are categorized as "risky" or people who simply live in risky areas are denied access to financial services provided by banks. Such denial forces them to use informal and underregulated financial services and contributes to the growth of shadow banking. Consequently, those people are removed from regulatory oversight. It becomes more difficult for law enforcement agencies to get more information and to better combat money laundering.

Summary

The aforementioned four problems are the most significant encountered by banks or other players in the financial industry. From these problems, we can identify the three common players in any AML regime– law enforcement agencies, banks, and customers. These different players have different incentives. Law enforcement agencies wish to achieve optimal deterrence at the lowest cost. Banks seek to maximize their profit. Customers want access to inexpensive, complete and efficient financial services.

Two important issues arise from scrutinizing player behaviors. The first involves whether the players behave efficiently and, therefore, socially desirable ways. Three of the problems mentioned above are concerned with efficiency–whether banks can reduce the cost of compliance (problem 1) and produce more valuable information for law enforcement agencies (problem 2) without hindering customers' financial inclusion (problem 4).[165] These problems correspond to each players' incentives. The second issue involves distributional concerns about how costs and benefits are allocated among players. This inquiry can be insightful to further understand whether to qualify a proposal because of regressive distributive effects.

Analysis

It is necessary to first briefly introduce liability regimes categorized by economic analysis, and apply the analysis to the bank's current AML obligations, followed by identification of the comparative advantages of banks as AML gatekeepers. Finally, the private incentives under the current regime must be addressed, including analysis of why private rational choices deviate from social optimality.

Liability Regimes and AML Compliance

There are two sections in this part. I will first introduce different types of liability regimes and then describe the circumstances in which they should be used. Next, I turn to investigate banks' compliance obligations under the current regime and what type of liability regime *should* be adopted to incentivize optimal levels of bank compliance.

[165] Draconian penalties are not necessarily problematic. In fact, Becker's model implies that the higher the penalties are, the lower the probability of detection can be, which saves more resources. Hence, draconian penalties are not the core problem which must be addressed address, but resulting *effects* of such penalties resulting from errors made in fault-based regime. Accordingly, therefore, this Academic Proposal will focus on how best to mitigate the detrimental effect of such penalties instead of simply lowering the level of penalties.

Strict-Liability, Fault-Based, Harm-Based, and Act-Based Regimes

There are undeniably many ways to categorize different liability regimes. To be consistent with the methodology of this proposal, liability regimes are approached from the perspective of economic analysis. Professor Steven Shavell categorizes liability regimes in a 2x2 matrix along two axes: (1) the alternatives of harm-based and act-based on one axis, and (2) fault-based and strict-liability on the other axis.[166]

The difference between the entries on the vertical, first axis is based on when the liability attaches. A harm-based regime is characterized if the liability of the wrongdoer attaches when the harm is created. Alternatively, an act-based regime is characterized if the liability of the wrongdoer attaches just after the misconduct occurs.

The difference between the entries on the horizontal, second axis is the condition of imposition of sanction. A fault-based regime is governed by whether the misconduct is "desirable," that is, the gain of such misconduct outweighs the created harm. Alternatively, a strict-liability regime exists where the sanction is always imposed when harm is created by misconduct.[167]

The four types of regimes are shown below:

Table 1. Liability Regimes

	Strict Liability	Fault-Based
Harm-Based	*e.g.*, felony murder	*e.g.*, negligent homicide
Act-Based	*e.g.*, safety regulation	*e.g.*, criminal attempt

Harm-Based Strict Liability. The regime of harm-based strict liability requires the lowest level of information for the law enforcement agency. The law enforcement agency need only know the level of harm in order to impose a sanction. However, because the actual sanction is always larger or at least equal to the harm (which requires a higher level of assets), the deterrence effect may be diluted. Additionally, the administrative cost of imposing sanctions is higher than fault-based regime because the sanction is unconditionally imposed whenever the harm is caused and known to the law enforcement agency.[168]

Harm-Based / Fault-Based Liability. In contrast, when the fault-based regime is employed, the law enforcement agency not only needs to know the level of actual harm, but also needs to know the likelihood of harm and the benefit to the wrongdoer from the misconduct, to determine whether the misconduct is "undesirable" and should be punished. However, this information is only required to decide whether to impose a sanction, but the expected sanction itself can be set above the level of actual level of harm because the sanction will not be imposed in situations where the wrongdoer is performing socially-desirable conduct. There is no chilling effect or over-deterrence associated with this higher sanction.[169] The conditional imposition of sanctions saves administrative costs, as well as enforcement costs, particularly for non-monetary sanctions.[170] However, the more demanding level of required

[166] SHAVELL, *supra* note 10, at 474-479.

[167] *Id.*

[168] *Id.* at 475.

[169] *Id.* at 466-467.

[170] *Id.* at 496-497.

information makes it more vulnerable to errors resulting from imperfect information. When the law enforcement agency has imperfect information and commits an error, it may over-deter and decrease desirable misconduct, incur enforcement costs and chill beneficial actions of law-abiding people. Such over-deterrence can be exacerbated by the higher-than-harm sanction. It is also possible that some undesirable misconduct is under-deterred.[171]

Act-Based Liability. In an act-based liability regime, the wrongdoer is liable immediately after the misconduct is completed. Because the harm is uncertain when the liability is imposed, the expected sanction should be set according to the *expected* harm instead of the *actual* harm. As a result, the law enforcement agency now needs to have information regarding the probability and the scale of expected harm (act-based strict liability) in addition to the gains associated with the misconduct (act-based fault-based liability).[172] Similarly, the act-based strict liability and act-based fault-based liability have the same advantages and disadvantages as their harm-based counterparts. However, the unique advantage for act-based liability is that it reduces the level of imposed sanction and therefore solves the judgment-proof problem, as well as saving enforcement costs.[173] This is the reason why act-based liability is always employed in response to misconduct that creates tremendous social harm, *e.g.*, most traditional crimes.

As described above, different liability regimes have their own merits. The application of each model is dependent on the information that the law enforcement agency has, the level of harm, the level of sanction, and the administrative and enforcement costs.

Banks' AML Compliance Obligations and Their Liability Regimes

General Compliance. Generally, banks have various AML compliance obligations. For example, the BSA requires financial institutions to establish an anti-money laundering program which includes (1) establishment of internal policies, procedures, and control, (2) appointment of a compliance officer, (3) ongoing employee training, and (4) an independent audit function to test the program.[174] However, only two of these requirements will be addressed—customer due diligence (CDD) and suspicious activities reports (SAR).

Customer Due Diligence. According to the Financial Crimes Enforcement Network (FinCEN), a CDD program includes four core requirements. Designated financial institutions are required to "establish and maintain written policies and procedures…reasonably designed to:

1. identify and verify the identity of customers;
2. identify and verify the identity of the beneficial owners of companies opening accounts;
3. understand the nature and purpose of customer relationships to develop customer risk profiles; and
4. conduct ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information."[175]

[171] *Id.* at 497-499.

[172] *Id.* at 478.

[173] *Id.* at 501.

[174] 31 U.S.C. § 5318(h)(1)(A) – (D).

[175] Financial Crimes Enforcement Network, Information on Complying with the Customer Due Diligence (CDD) Final Rule, https://www.fincen.gov/resources/statutes-and-regulations/cdd-final-rule.

The first core requirement, called a Customer Identification Program ("CIP"), generally includes the following components— (1) verification of the identity of the person seeking to open an account, (2) a maintenance record containing information collected for verification, and (3) a check of the customer's name against terrorist lists.

The second core requirement of CDD is targeted at corporate accounts and discovering a corporation's beneficial owner, which, by definition, includes individuals who either own at least a 25% of equity interest or carry significant responsibility or control.[176] This requirement prevents individuals from hiding their identity behind a corporate veil.[177]

The third core requirement, developing a risk profile of a customer, is defined by FinCEN as gathering appropriate information about a customer at the time of opening an account so as to develop a baseline against which to compare later transactions to assess whether a later transaction is suspicious. In practice, such information can include the type of the opened account, the services provided, the customer's income level, or other circumstantial facts.[178]

The last element of ongoing monitoring is an event-driven requirement to update information (as opposed to continually or periodic updates). Typically, banks are required to update a customer's profile when they detect something relevant to reassess or reevaluation of the risk. Unexplained overseas funds transfer or significant change in the volume of customer activity can be examples.[179]

Both civil and criminal penalties may attach for violations of the above rules. For each single negligent violation of a BSA requirement, a penalty of not more than $500 may be assessed. However, for a pattern of negligent violations, an additional penalty not exceeding $50,000 can be imposed. In contrast, a willful violation can lead to penalties of up to $25,000. A separate violation is deemed to occur for each day, at each office, branch, or place of business at which a violation occurs.[180] Criminal penalties generally target individuals and can amount to $250,000 and/or imprisonment of up to five years.[181]

Suspicious Activity Reports. Financial institutions are required, at a minimum, to file SARs when an institution "knows, suspects, or has reason to suspect" that a transaction is suspicious as defined by the rule.[182] Although financial institutions enjoy discretion they remain obliged to conduct due diligence when determining whether or not the transaction is suspicious. Such due diligence includes an examination of the available facts, background, and possible purpose of the transaction.[183] Currently, financial institutions file reports to FinCEN. While there is no cost of filing, institutions incur costs in order to detect suspicious transactions and prepare reports before filing.[184] FinCEN received about 800,000 SARs in 2019.[185]

[176] Michael Levi, Federal Money Laundering Regulation: Banking, Corporate & Securities Compliance, 7A-6—7A-7 (2018).

[177] *Id.* at 7A-3.

[178] *Id*. at 6-36 – 6-37.

[179] *Id.* at 6-37

[180] *Id.* at 7-8.

[181] *Id.* at 7-9.

[182] *Id.* at 14-19.

[183] *Id.*

[184] *Id.* at 12-3.

[185] Financial Crimes Enforcement Network, *Suspicious Activity Report Statistics (SAR Stats*), https://www.fincen.gov/reports/sar-stats.

Several points are noteworthy. First, while filing immunizes financial institutions from penalties associated with SARs, institutions can still incur liability due to noncompliance with other AML components (*e.g.*, such as CDD or recordkeeping requirements).[186] Second, all information revealing the existence of SAR is confidential.[187]

Similar to the penalties associated with failure to comply with CDD rules, the violation of SAR rules leads to the possibility of both civil and criminal penalties. The former includes a $500 civil penalty for each single individual negligent violation and a penalty of up to $50,000 for a pattern of negligent activity. A willful SAR violation can lead to a civil penalty of up to $25,000 or the amount of the transaction (capped at $100,000).[188] Any person willfully violating SAR reporting requirements may suffer a fine of up to $250,000 and/or imprisonment of up to five years.[189]

Summary. According to the statute, all possible violations require (at a minimum) some level of fault (negligence) but do not require an occurrence of actual harm. Therefore, based on the categories described above, both liability regimes are act-based, fault-based liability regimes.

Banks' Comparative Advantage in Information Collection

As analyzed, the law enforcement relies on the information collected and generated by banks and other reporting entities. Many believe it is efficient to delegate such responsibility to banks due to their comparative advantages, including proximity to such information, professionality, and fewer conflicts of interest. Nevertheless, it is worth reexamining the accuracy of these claimed comparative advantages. It is first necessary to analyze the type of information currently collected by banks, and then analyze the areas in which banks have a comparative advantage.

Two Dimensions of Information

Under the current regime, banks collect customer-related information when conducting CDD and transaction-based information when the customer activates a transaction. Several differences can be drawn between these kinds of information. First, the timing of collection of both types of information is different. Banks usually collect customer-related information prior to building a business relationship or having accounts be opened. In contrast, financial institutions collect transaction-related information on an ongoing basis after each transaction occurs (and after the relationship has been formed). Second, the collection of customer-related information requires more effort from both banks and customers. A well-conducted CDD needs customer collaboration as well as bank verification. However, the collection of transaction-related information is relatively inexpensive and undemanding with the help of automated systems because most transactions, whether online or offline, are computerized.[190] In practice, however, modern AML compliance systems sometimes capture information that is not easily categories as either customer-related and transaction-based, for example, video archives of customer interactions. These

[186] LEVI, *supra* note 40, 12-5.

[187] *Id.* at 14-33.

[188] *Id.* at 14-54.

[189] *Id.*

[190] LEVI, *supra* note 40, 12-15 – 12-16.

supplemental materials have sometimes proven helpful to subsequent criminal investigations into potentially illegal conduct.

Similarly, banks are actually performing two types of actions with respect to information: collection and analysis. The bank collects the information and then analyzes it (as well as files reports where appropriate based on the analysis). The collection and analysis components of information-gathering are logically separable. For instance, a bank could turn over all collected information to a professional analysis company. The bank could also outsource its due diligence to other institutions to help verify the customer's identity.

These two dimensions of information generation create four subsets of information-generating roles: customer-related information collection, customer-related information analysis, transaction-related information collection, and transaction-related information analysis.

Interplay between CDD and SAR

The analysis of both customer-based and transaction-based information is interdependent. For example, to better detect a suspicious transaction, the bank needs to understand the customer's profile. Similarly, banks need to know the essence of planned transactions to determine the intensity of necessary customer due diligence and customer profile updates.

This interrelated relationship leads to the conclusion that the level of customer due diligence affects the accuracy of the detection of suspicious transactions. The knowledge of past or proposed transactions further determines the level of customer due diligence. For example, consider that a bank has information regarding a depositor's occupation and annual income—a custodian whose monthly salary is $3,000. That bank would be better positioned to detect the abnormality of a transaction of $500,000 in the customer's account as compared to a similar transaction in an account of high-income sports-team owner.

Similarly, banks may have different procedures for determining the suspiciousness of a small foreign exchange transaction, as compared to a million-dollar wire transfer. In one case, the bank may merely check the depositor's identification, but in the other would scrutinize carefully and require more documentation.

Interdependency as the salient feature of two-stage monitoring has rarely been mentioned in previous gatekeeper liability literature, yet it has significant implications for designing a liability regime. Specifically, when banks can be immune from liability simply by filing reports, they do not have incentives to conduct scrupulous due diligence, and the quality of their reports suffers substantially. As a result, to induce optimal investments in CDD, banks cannot be immunized from liability simply by virtue of having filed appropriate SARs.

Banks' Comparative Advantages

Even though the bank is currently obliged to shoulder all four subsets of information generation, the bank does not necessarily have a comparative advantage in creating all of them. The determinants of comparative advantage are effort, capacity, and quality. Between collection and analysis, banks are more likely to have comparative advantages in collecting as compared to analyzing information. The proximity to the information allows banks to enjoy some advantages in collecting information. For example, when collecting customer-related information, the bank employee can directly observe the document as well as the applicant's appearance. It is also inexpensive to collect transaction-related information for banks in this digital era because all transactions are stored on the computer. On the contrary, banks do not have a comparative advantage when it comes to *analyzing* the collected information. The efficacy of any AML information analysis is dependent on sample size. Sample size, in this sense, can be both cross-sectional and temporal. When the banking industry is fragmented, and each bank serves only a small group of customers, the bank is less likely to derive a meaningful result from such a small sample size of customers. Similarly, when the clientele is stable or few transactions are activated, the bank is also less likely to identify a new mode of suspicious transactions. Outsourcing the analysis to professional analysts can help aggregate the sample size and yield a more meaningful result. As a result, banks have lower comparative advantages in analyzing information.

However, even though banks seemingly have advantages in collecting information, it does not mean that the job may not be delegated or outsourced. For customer-related information, it is difficult to conclude that customer due diligence should definitely be conducted by a bank employee in the bank. However, it is undeniable that no other institutions can stand in a better position to collect transaction-related information because the primary source of information lies in the bank's system. Any other institution can never collect such information without access to the bank's system. Also, it seems absurd to require customers to "register" planned transactions before instructing banks to activate it. In short, banks have unique comparative advantages in collecting transaction-related information but replaceable comparative advantages in collecting customer-related information. When the market is fragmented, small banks ought not analyze information.

Private Incentives and Social Welfare

Law Enforcement Agencies

The primary purpose of law enforcement is to reduce crimes by deterring, incapacitating, and/or rehabilitating individuals. The first method takes a more ex ante perspective whereas the latter two are more grounded in ex post views. Only deterrence will be considered.

Assuming all actors are rational, criminals would perform a normal cost-benefit analysis when deciding to commit a crime. Crimes are harmful to society but beneficial to the individual wrongdoer. Accordingly, the government should punish criminals to deter them from committing socially harmful crimes. To achieve this goal, policymakers should set the expected sanction exactly equal to the generated social harm. If wrongdoers are rational and risk-neutral, they are indifferent to any magnitude-probability combination of sanction so long as the expected sanction (*i.e.*, the amount or gravity of the sanction multiplied by probability of imposition) remains the same. While wrongdoers are indifferent, different combinations do have different implications for law enforcement. In particular, increasing financial penalties is less costly for the government than investing resources in increasing the probability of detecting wrongful activity. Doubling the financial penalty costs law enforcement little but halving the probability of its imposition requires heavy investments in investigating resources.

In the real world, monetary sanctions cannot be set extremely high for several reasons. First, wrongdoers are not infinitely rich, meaning they may be "judgement-proof" when the imposed monetary sanction is higher than their assets or income-earning ability. Limits on wrongdoers' wealth and income dilute the deterrent effect. Incarceration is one method to solve the limited-assets problem. However, when sanctions take a non-monetary (imprisonment) form, the costs to law enforcement of imposing his type of sanction increases. Unlike monetary sanctions, which merely involve wealth transfer and involve no efficiency implications, penal incarceration requires that the government construct prisons, and hire guards, etc. In addition, prisoners and their family members suffer a utility loss from these non-monetary sanctions. This makes the particular combination of a high non-monetary penalty, coupled with a low investment in detecting wrongdoing, even less appealing. Moreover, the low amount of deterrence from incarceration may provide another reason against increasing incarceration as a form of deterrence. While costly, enhancing the probability of detecting money laundering is necessary and desirable when compared with increasing the non-monetary sanction.

Assuming it is necessary and desirable to increase the probability of punishment, a system designer should attempt to minimize costs associated with such an approach. One answer is to introduce gatekeepers (banks in the AML context) or actors who are more capable of generating information required to impose a sanction. By directly observing customers' profiles and transactions, banks can access such information faster and identify abnormal patterns earlier than law enforcement. Therefore, delegation of collection and reporting of information to banks ought to reduce overall costs.

To induce banks to perform this role, policy makers must either reward banks for providing this information or punish them for noncompliance. Given the government's limited resources and budget, it would be hard to reward banks.[191] Therefore, it makes sense to punish banks for failing to comply with AML gatekeeping obligations. Law enforcement must then make two decisions— (1) setting expected sanctions on criminals for money laundering, and (2) setting expected sanctions on banks for noncompliance. As mentioned above, setting the expected sanction on criminals is constrained to a certain level of sanction based on the amount of marginal deterrence, imprisonment costs, and related probability of detection. As to setting the sanction on banks, Becker's model is again applicable. Sanctions should be monetary, and the judgment-proof issue (insufficient assets) is less likely to occur. Therefore, it would be rational for the law enforcement agency to set a higher monetary penalty and spend less money on enforcement (lower probability of imposition). Moreover, the more information law enforcement receives from banks, the easier and less expensive it is for law enforcement to apprehend criminals. They are also likely to be incentivized to set expected sanctions at too high of a level (to generate more information) because, here, law enforcement is not required to bear the cost of information generation. The incentive to save enforcement costs can consequently lead to draconian levels of penalties and sub-optimally high expected sanctions.

[191] Unlike some whistleblower regimes, the ultimate goal of an AML regime is to punish individual criminals via imprisonment. Instead, in an SEC-type whistleblower regime, the ultimate entity on whom the sanction is imposed is a corporation whose penalty is monetary. Hence, it is viable to finance whistleblower rewards via the imposed penalties in those contexts; however, that is not possible in the AML context.

Banking System

In terms of incentive, banks are corporations whose primary goal is to maximize profits. To do so, banks should provide their services to the point where marginal revenue equals marginal cost. To illustrate how AML law plays a role in banks' incentives, the analysis is simplified and focuses on the business relationship between customers and banks.

On the revenue side, implementation of AML law does not have a definite effect on bank revenue. For example, it is imaginable that depositors are deterred by time-consuming verification processes and, therefore, engage in business relationships with fewer banks to reduce the time taken by verification. However, the result is that depositors will deposit their funds in fewer banks, with a different distribution of funds among the various banks, and the total amount of deposited monies will remain the same. In such a case, revenue does not necessarily decrease, however, each bank's relative market share might change. It is also possible that in some places (*e.g.*, China) people cannot live without bank accounts to either receive any wages or to use an almost exclusively electronic payment system. There, the elasticity of demand (a measure of how much demand changes in response to a change in price) can be so steep that demand for deposits would remain unchanged when AML law is implemented. It is empirically unclear how AML law affects banking institution's revenue streams.

In terms of costs, AML penalties could have potential ramifications for banks. A financial institution must choose between compliance or noncompliance. The former leads to investment in staffing, software, and programming. In concrete terms, banks need to recruit and train staff to meet AML standards. Banks would also install software and institute programs to better detect abnormal transactions. Some banks would even have to reform their organizational structure to implement best AML practices. All of these amount to massive costs. In contrast, should the bank choose not to comply, it faces harsh penalties. As a result, as a rational profit-maximizer, banks would try to strike a balance between compliance and noncompliance to minimize their expected overall expenditure. Additionally, banks would compare marginal cost and benefit for each group of customers. When a specific customer's marginal cost is higher than the marginal benefit provided to the bank, that customer would be rejected or not served by the bank. This is likely with a certain risky group of customers and is the motivating reason behind de-risking.

Under the current regime, it seems that banks trend towards choosing to comply with AML standards, as can be deduced from the fact that no banks have been repeatedly fined for the same type of fault. This high level of compliance implies that the cost of compliance is lower than the cost of expected sanctions, which means that it is inefficient and irrational to not comply. This may echo the proposition set forth in the preceding paragraph–the sanction level may not be optimal.

Compliance is desirable when the regime is well-designed, and the sanction reflects the real social cost. However, if the regime fails to account for externalities associated with compliance, it causes socially undesirable results. The current AML regime may be such an example. First, CDD obligations are not results-based, which prevents banks from obtaining information efficiently. When a customer opens several accounts at several banks, the customer is required to provide the same information and spend similar amounts of time simply to go through an identical verification process. This repetitive process is extremely inefficient. Nevertheless, because banks are threatened by harsh penalties, they care about the bank's avoidance of penalties and not the socially optimal process. Accordingly, banks are motivated to conduct their own CDD process and deterred from using information collected by fellow banks. Secondly, SAR filing is also problematic. While setting the triggering standard for filing an SAR at the low level of "suspicion" may induce more information generation, it also invites banks to engage in defensive filing relative to normal transactions which trigger only negligible suspicion of money laundering, but which are almost certainly complaint with AML laws. Exempting banks from very high penalties, combined with the low cost of filing SARs, exacerbates such defensive filing. Defensive filing helps banks avoid huge fines but incurs huge social costs. It dilutes the information value of information provided to law enforcement. Bombarded with defensively filed reports and a limited budget, law enforcement is less capable of combating crime. To illustrate, a numerical example is provided below:

> **Example 2.** Suppose there are 100 transactions of which 20 are actual money-laundering-related transactions. Filing a SAR costs a bank $18, and the **expected** sanction for failure to file is $100. The law enforcement agency can handle or investigate a total of 15 cases due to budget constraints.
>
> Now, the banks can only identify (i.e., 100% sure) 10 out of 20 money-laundering-related transactions but are still 50% confident that the remaining 10 are also illicit money laundering. Also, it suspects (erroneously) that 25 of the remaining 80 transactions are illegal with 20% certainty.

When banks choose to file only when they are 100% certain (Scenario 1), all reports can be handled and investigated by the law enforcement agency (they would forward 10 transactions). When banks instead report solely because of a lower suspicion standard, say 50%, there are 20 transactions reported (Scenario 2). Here 15 cases will be investigated with five left untouched (but reported) by law enforcement. However, when the sanction is set high and banks file defensively, they will file 45 total reports (Scenario 3). The law enforcement agency can still only deal with 15 cases and would encounter difficulty sifting through the reports. Perhaps they will select randomly amongst the reported transactions (any random 15 of the 45). As a result, only 7 of the actual money laundering cases are investigated which is a worse outcome than both Scenarios 1 and 2. This example illustrates the banks behavioral responses to varying schemes. When expected sanction is far higher than filing costs, banks file defensively based on a low level of suspicion.

To summarize, banks weigh their private cost of compliance versus noncompliance in pursuit of profit maximization. Their ignorance of social costs incurred by their behavior should be calculated and incorporated into the AML regime to force them to internalize this cost. Concretely, we must focus on two flaws—how to encourage banks to save CDD costs without reducing information value, and how to prevent banks from engaging in defensive filing.

Social Welfare Implications

The preceding sections analyze how implementation of the current AML regime changes or affects different parties' incentives. To briefly review, law enforcement is motivated to impose higher sanctions on banks to induce as much information-generation as possible. Banks are attempting to escape harsh penalties and are likely over-complying (conducting CDD on their own and filing too many SARs). Facing time-consuming and laborious processes, customers may be deterred from purchasing financial services.

Although choices may be rational from the perspective of any individual party, that choice may reduce overall efficiency (socially). Law enforcement's goal is to maximize deterrence at the lowest cost. Their choices may lead to too much information generation because they do not care whether the amount of generated information is justified by the cost absorbed by banks. The potential of financial inclusion is less relevant for law enforcement.

Secondly, requiring each bank to conduct their own CDD and preventing information sharing creates strong incentives to generate redundant information. Also, the exemption of liability by filing reports fails to force banks to internalize the cost of processing information. Hence, banks are filing too many reports. The redundant CDD process and defensive filing lead to a common result–banks are currently generating a low amount of valuable information.

Under the current regime, it is inefficient to require banks to produce redundant customer information and encourage them to file reports by fully exempting their liability. These actually decrease the value of information provided to any relevant regulatory authority. In addition, the broader concern regarding financial inclusion and regulation of shadow banking should be addressed by the government or receive more scrutiny to address these potential pitfalls of the current regime. The purpose of this proposal is to introduce and analyze a few possible reform policies to address these inefficiencies.

Summary

As demonstrated above, both CDD and SAR regimes currently operate on a fault-based liability scheme. However, under such a liability regime, the rational choices made by law enforcement and banks deviate from the socially optimal equilibrium. Law enforcement saves costs by outsourcing responsibility to conduct CDD/SAR to banks and induces information generation by imposing harsh penalties for bank noncompliance. In response, banks invest tremendous resources in compliance programs yet simultaneously file defensive reports and de-risk from particular demographic or geographic populations. Those circumstances fail to enhance deterrence and inhibit the role of banks as service providers that facilitate capitalism.[192]

Solutions

Based on the problems discussed above, it is necessary to propose several reform recommendations, each of which addresses the aforementioned problems. Commenting on some solutions proposed by other theorists, these recommendations are based on modifying liability regimes, encouraging information sharing, applying blockchain technology, and introducing private causes of action.

Modification of Liability Regime

Act-Based Liability for CDD

To optimize banks' CDD processes, an act-based liability regime should be adopted to induce the optimal level of due diligence.

[192] *See* John Armour et al., Principles of Financial Regulation 275-276 (2016).

> **Example 3.** Suppose a bank implements a CDD program that involves incurring fixed startup costs of $500 and variable costs of $10 per person. This program increases the probability of the bank being able to accurately identify a suspicious transaction from 50% to 90%. In turn, the bank's program and filings increase law enforcement's chances of detecting and punishing money laundering from 20% to 50%.
>
> For a person who commits a low-level offense of, say, extortion, the penalty will be set to $1,000. The social harm generated by this extortion crime is $500. Separately, banks will suffer a $100 penalty for failures to comply with AML laws. Further assume that there are two types of extortion criminals–100 high gain criminals whose penalty is $400 and 100 low gain criminals whose penalty is $300.

In the above example, if the bank ***does not*** implement the CDD regime, the extortion criminals face the following scenario. As a total class, they will be confronted with a $350 sanction. Here, the bank will only catch and file 50% of money laundering transactions. Separately, even if the bank fails to file a SAR, the government still has a 20% chance of catching that transaction. The sanction for this half of the money laundering transactions that flow through the bank is then 0.50 * 0.20 * $1,000 or $100. For the 50% of transactions that are caught and filed by the bank, law enforcement has a 50% chance of catching those filed transactions, meaning that the sanction for this half is 0.50 * 0.50 * $1,000 or $250. The total expected cost (or sanction) facing any person committing extortion is now $350 total. This means that the 100 high gain criminals will still commit the crimes because their expected gain outweighs the expected cost of $350. The other 100 low gain criminals will *not* engage in the criminal conduct.

However, with the help of the customer due diligence program, the expected sanction increases to $470. Now, the bank will catch 90% of transactions and, of those filed transactions, the government will catch and punish 50%. Now, for the transactions that are forwarded to law enforcement, the expected sanction is 0.90 * 0.50 * $1,000 or $450. The expected sanction for the 10% remaining, unfiled (or undetected by bank) transactions is 0.10 * 0.50 * $1,000 or $20. The total expected sanction facing the entire class of extortion criminals is now $470. All criminals are thus deterred.

The increased deterrence benefit from the CDD program is $50,000 (100 more criminals are deterred than before meaning that we can save $500 of social harm from being committed by 100 criminals for a total saved social cost of $50,000). This marginal benefit from the program outweighs the $2,500 cost incurred by implementing the CDD program ($500 + $10 * 200 total criminals). Therefore, the CDD program is socially desirable.

However, consider a harm-based liability regime where banks are ***not*** immunized from liability simply by filing suspicious reports. The bank would now face potential penalties for failing to file SARs. Rational banks must now decide whether it makes sense for them to file or not to file at all.

When a bank *files* (which happens 50% of the time), there is also a 50% chance that law enforcement discovers this crime leading to a total expected sanction of $25 (0.50 * 0.50 * $100 sanction for noncompliance with AML law). However, if the bank decides *not* to file, the total expected sanction harm will be only $20 because law enforcement only detects money laundering 20% of the time (0.20 * $100). Without immunity, rational banks will choose not to submit *any* reports, let alone incur costs to implement a CDD program.

Consider the addition of immunity to the example. Suppose filing incurs a small cost of $1 per report. Now, the bank will decide to file a report for every transaction because the bank would only have to pay $200 instead of implementing a $2,500 CDD program. However, the information value is diminished because the bank's filing of reports for *all* transactions is just as useless as not filing any reports at all.

As a result, the example illustrates how the liability regime for SAR filing affects the earlier decision regarding CDD. No matter whether immunity is granted, independent liability for CDD is desirable. Hence, an act-based liability regime should be adopted for the CDD program.

Strict Liability for SAR filing

Currently, SAR filing requirements are premised on fault-based liability. As discussed, fault-based liability regimes require more information, which has two implications. First, law enforcement incurs extra costs to investigate whether the failure to file met the standard of fault required for bank liability. Second, fault-based regimes incentivize banks to implement seemingly effective (but in fact inefficient) measures to pretend they are not negligent. Although banks may reduce *some* of their inefficient filing efforts due to immunity, banks may still find it rational to masquerade their behavior because it is impossible to report every transaction, and also because sanctions are fault-based and may be higher than the expected harm.

Shifting from fault-based liability to strict liability can not only save investigation costs but prevent overdeterrence stemming from errors estimating negligence and overly high sanctions. Moreover, some banks may actually refrain from introducing advanced measures because they are unrecognized by law enforcement despite their efficient or cost-effective nature. Rather, banks are forced to use inefficient measures because they are recognized by official law enforcement actors. Such inefficiency is exacerbated when the law enforcement agency has outdated knowledge about money laundering tactics or techniques.

To prevent inefficient investment in useless measures, this proposal suggests a shift from the fault-based liability to strict liability for failure to file SARs.

Encouraging Information Sharing

As discussed above, the CDD process is redundant and costly while arguably simultaneously yielding little valuable information. Therefore, policy makers should consider allowing the same information to be used by as many institutions as possible to maximize the benefit of information collection. Currently, information sharing focuses on information about "suspected customers and transactions" among financial institutions and law enforcement. The scope of shared information is rather limited and does not include all collected information.[193] This proposal argues for a broader information-sharing plan that allows more information to be used and shared by all reporting entities. This outcome could be achieved one of two ways. One method is to organize a centralized agency responsible for collecting all required customer information. Another method is a decentralized, industry-run information sharing mechanism.

[193] Levi, supra note 40, §8.

Centralized Agency

The core problem of CDD is that each customer might engage in multiple business relationships with numerous banks or other reporting entities, and the costly and time-consuming CDD is undertaken for each, and produces similar information each time. Furthermore, when such business relationships are continuous, banks are also required to *update* the information, which is similarly repetitive and redundant. A centralized agency responsible for all front-end and follow-up information collection may be cost-saving and desirable.

Imagine some of the transactions that a graduate might undertake—opening a checking and savings account at one bank, applying for a credit card from another, obtaining securities trading account from a broker, and applying for a loan for a new home from a lender. Many people engage in business relationships with multiple banks or reporting entities throughout their life. Under the current regime, each entity is required to conduct their own CDD—and each time incurring substantial costs. In addition, the customer must spend time collecting required documents to provide to the reporting bank or entity. However, creating a centralized agency would reduce monetary and temporal costs incurred by both regulated entities and the customer. The agency could also update a customer’s profile for use by reporting entities, and the savings will increase the longer the agency is involved.

The centralized agency could be created by the government or some consortium of regulated reporting entities. Whether public or private, those subject to AML regulations can sign up as a member and pay a front-end proportional membership fee and one-time retrieval fee. The fees would go towards funding the agency and its employees. Further, to avoid distorting the price of financial services, the fee should be designed properly to reflect or approximate the real usage of information by reporting entities. For example, if a foreign money exchanger or a casino is charged the same amount as banks, that company will raise the price charged to procure their services. Demand is more inelastic for gambling or currency exchange services, meaning that customers are willing to incur the costs that would be passed onto them in these industries (as compared to banking). Thus, they are deterred from using such infrequent services provided by other entities who are charged similar fees. While the fee structure can have implications for the market, it is less problematic than the current practice because costs incurred under the current AML structure might already drive those customers out of the market. The fees charged by the centralized agency are foreseeably lower than costs incurred in the current regime. It must be determined whether the centralized agency or the reporting financial institutions should be responsible for defects or problems in the CDD process. Some would argue that the location of where the sanction is placed has no effect because monetary sanctions are always transmittable to counterparties. Therefore, it is likely that the costs of the penalties would ultimately be shared between banks and the centralized agency. However, in our case, when multiple reporting entities seek information from the centralized agency, it would be counterintuitive and indirect to impose sanctions on reporting entities.

First, the law enforcement agency should know all entities that have been asking for information about that money launderer. However, such information can only be accessed from the centralized agency. Accordingly, the law enforcement agency should obtain such information before making decisions.

Second, in terms of deterrence, the real harm from poor CDD outcomes is reduced accuracy of identification of suspicious transactions. The effectiveness of a CDD program has an impact on second-stage monitoring, because the centralized agency cannot adjust its level of scrutiny beforehand because the agency conducts the due diligence and collection and verification of information before the customer has opened a bank account. Accordingly, the agency can not foresee how many accounts the money launderer will open and what kind of service will be used. As a result, when sanctions are imposed on reporting entities, the aggregate sanction is likely to exceed optimal level and creates over-deterrence. The government may impose sanctions on multiple banks for the same failure which would create an inefficient (too punitive) outcome. It is, therefore, preferable and intuitive to impose sanctions on the centralized agency for information collection issues.

Lastly, other arguments counsel against the creation of a centralized agency. The first is whether a centralized CDD process loses a benefit inherent in multiple checks on the same customer—whether detection of money laundering activity decreases (or launderers escape liability more easily) in the proposed central agency regime if the customer need only go through the process one time. It is more difficult to pass every CDD process at each bank. However, the missing element in this argument is the degree of similarity among different bank CDD programs. When the processes are near-identical, it is useless to conduct CDD multiple times by different banks. The result remains the same as a single bank or a centralized agency. If the processes diverge significantly, then multiple checks do create significant benefits. This issue requires empirical information to resolve. However, considering the required documents and standardized rules, it is likely that banks have substantially similar processes and each bank's additional CDD check produces little marginal benefit compared to the cost.

The second argument against a proposed centralized agency concerns privacy. Such an agency would store, control, and possibly share highly sensitive information with other reporting entities. In response, it is worth clarifying that no additional information is being collected above that collected in the current system. The difference is that in the current regime, the information is collected and possessed by different and isolated financial institutions. With the proposed centralized agency, that information would be owned by the agency and other entities that have business relationships with the customer. This requires a focus on two potential concerns: (1) the scope of released information, and (2) the diffuse or concentrated access to such information. This proposal would only impact the second of those two concerns and needs further investigation.

Multilateral Information Sharing Mechanisms Between Financial Institutions

Another method to encourage information sharing is to allow banks to rely on the information collected by other reporting entities. One possible iteration of this design could be a collaborative platform that allows quick and easy information sharing among industry actors that collect and rely upon AML/KYC information. The underlying rationale is similar to that underlying the creation of a centralized agency, to maximize the use of collected information and save redundant costs of information gathering. The major difference is that this proposed model has a disseminated information structure which has its own advantages and disadvantages.

A concrete explanation of this model can be illustrated as follows. First, banks are allowed to solicit information from other banks which already have a business relationship with the new customer. A customer who has a savings account at the Bank of America wishes to open a checking account at Chase. It would then be possible for Chase to solicit the customer's consent and contact Bank of America to ask for the required AML information. Now, Chase needs to perform only minimal verification to confirm the identity of the new customer to open the account. Chase saves on document collection, some verification costs, and electronic filing costs. In fact, inter-bank information sharing is not uncommon in other areas, such as credit ratings.

Nevertheless, compared to the centralized model, this model has a number of advantages. First, it can introduce market competition such that the bank that most efficiently collects and verifies customer data will be the information provider for the whole industry. Second, the scope of shared information is broader than the centralized model. Because the centralized agency itself is not a financial institution that facilitates customers' transactions, it does not possess any information regarding transactions. However, a reporting entity, such as a bank, does have information about the transaction history as well as an ongoing risk-profile regarding each of its customers. Such information can be more valuable than that generated by a centralized agency. Moreover, the disseminated model mitigates privacy concerns to a degree.

Nevertheless, the disseminated model also comes saddled with several disadvantages. For example, the transaction cost can be high. Without collaboration of the customer, it is unlikely for the bank to know the other entities with which the customer has already transacted. Additionally, we can only rely on information flows if it moves in the direction from more credible to less credible actors. Ideally, information generated under better scrutiny processes would be used by other, less capable entities. Unlike a centralized agency as a single point of comparison or contact, a model using disparate, private actors would create difficulties in controlling the sequence of entities with which a customer transacts. If the customer first engaged with a local bank for a simple savings account and later wants to open a checking account at a big national bank, it is likely desirable that the larger entity conduct its own CDD process rather than using the CDD information obtained by the local bank. Almost definitively, the big bank is more reliable than a local saving and loan company. In such circumstances, the disseminated model might face practical problems when implemented. One other minor but unintended consequence might be that such a model can affect the market by granting those big banks comparative advantages. When all other banks rely on big banks to conduct CDD, customers are encouraged to open accounts provided by those institutions. Those big banks advantage in contacting customers and providing services.

Similar to the agency model, we must decide in the disseminated model where to impose liability for failure to conduct high quality CDD. We can either impose liability on banks that improperly *relied* on the information, or on the bank that *provided* faulty information (relying banks or provider banks). Again, if banks could pass on the costs associated with such information it makes no difference who is punished. If liability is imposed on provider banks, they will calculate a "risk premium" to reflect the increased potential costs that could be incurred from information sharing. The market enables the bank that is most capable and confident in its information quality to charge the lowest price for its provision of such information. Otherwise, relying banks that bear the cost of being sanctioned will do their best to solicit information from reliable banks that provide information. Both seem to be optimal and work well. Nevertheless, in the real world, customers might have different purposes for obtaining different types of financial services. The required information, even though largely overlapping, may vary according to the purpose. Hence, the sufficiency of information collection should be determined based on the services provided. For example, the bank providing international wire transfer service cannot merely rely on a customer profile collected by banks at which the customer only retains a checking account. Accordingly, law enforcement should be able to distinguish the difference and take corresponding actions. It is, therefore, less likely to impose sanctions on the providing banks without looking at the relying banks' practices. If the law enforcement agency failed to do so and attribute such failure to providing banks, then the flow of information will be hindered by the fear of unforeseeable and disproportionate penalties.

Applying Blockchain Technology

Separate from modifying the liability scheme and aforementioned institutional innovation, other new technologies may help complement those reform efforts.

Cryptocurrencies. Cryptocurrencies can pose serious new threats to an AML scheme.[194] Some consider cryptocurrency to be superior to both cash and other mediums of exchange within the current banking system due to its transferability and anonymity. While possible, it is much more difficult and time consuming to transfer large amounts of money using cash–the core reason organized crime leaders need to launder their money.[195] However, cryptocurrency provides a similarly anonymous tool to transfer wealth at a faster pace and a lower cost. Also, compared to the conventional banking system under intensive supervision, criminals who hold cryptocurrency can transfer their wealth to other members without disclosing their identity.[196] Cryptocurrency, when treated as a closed-end system, is not meaningfully distinct from other digital assets that are unregulated (*e.g.*, online gambling currencies). All unregulated digital assets can be transferred anonymously and quickly. However, the gradual development of public recognition of cryptocurrency has transformed it into an open-end system, or one where the currency can be exchanged for fiat currency and become liquid. This process, as applied to cryptocurrency, also helps criminals to launder their money more easily. Now, criminals can use cryptocurrency as a medium when transacting illegal commodities such as drugs and weapons.[197] This medium eliminates the need for the placement stage of money laundering as conducted using normal mediums. As the public comes to recognize and use cryptocurrency as a medium, criminals can directly purchase tangible assets under legal protections afforded to cryptocurrency. The transaction of tangible assets allows the integration stage (where assets are converted into regular mediums) to be completed without governmental supervision. As a result, the existence of cryptocurrency and its widely accepted nature, can significantly facilitate money laundering.

Distributed Ledger. The blockchain technology underlying cryptocurrencies, especially a distributed ledger, can also be used to augment or complement AML compliance. Distributed ledgers allow information to be recorded and updated simultaneously in every block.[198] The distributed ledger transforms the conventional linear information flow into an information network, which ensures that every bank can know the latest status of each customer. The most noteworthy point of the distributed

[194] *See e.g.*, Raffaella Barone & Donato Masciandaro, *Cryptocurrency or Usury? Crime and Alternative Money Laundering Techniques* (BAFFI CAREFIN Ctr. Research Paper No. 2018-101), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3303871, [reader may require academic or account access].

[195] LEVI, *supra* note 40, 1-09.

[196] John W. Bagby, David Reitter & Philip Chwistek, *An Emerging Political Economy of the BlockChain: Enhancing Regulatory Opportunities*, Academy of Legal Studies in Business - National Proceedings 57 (2019).

[197] *Id.* at 26-27.

[198] *Id.* at 6.

ledger is that a blockchain ensures the veracity of information during transmission. It is difficult, if not impossible, to hack and alter the information.[199] Therefore, from the perspective of combating crime, the distributed ledger is safer and more reliable. Adopting distributed ledger technology can enhance the efficiency of the reliance model. Each time the customer goes to *any* bank, the bank can update the customer's information. The latest collected information will then be appended to the customer information stored in other banks' databases.

The distributed ledger technology echoes the analysis of two-dimensional information. In previous sections, I focused on the information collection and concluded that customer-based information should only be collected once but transaction-based information should continue to be collected by respective banks. However, when it comes to analysis of data (rather than collection), a big data pool can generate more insights into a customer's transaction pattern and allows for better detection of abnormalities. A distributed ledger can aggregate data across all reporting entities. This model allows for all transaction information to be updated simultaneously at each bank's database for either further analysis of that transaction or to compare with future transactions.

However, it must be noted that this new technology does not solve the core problem. First, the main issue with inefficient CDD programs stems from redundant efforts to collect the same customer information. Adoption of a distributed-ledger model presumes the transferability of this information across banks. Therefore, a distributed ledger only improves the accuracy and the pace of information-sharing. The distributed ledger only improves but not alter the reliance model. While saving time and cost when transferring information exactly as collected and recorded by the bank, the distributed ledger still cannot guarantee the veracity of the information because the distributed ledger system only records and updates information collected by the bank and contains no inherent or independent truth-checking function. Accordingly, when a bank, intentionally or negligently, conducts unqualified CDD and updates the customer information, the erroneous information will be appended to the blockchain and appear accurate to other banks.

This convenient, fast technology also invites other problems. When information is updated automatically, it becomes more difficult to prevent erroneous information from polluting an error-free record. This can be a particularly acute problem when the error is already recorded in the "chain." A possible preliminary solution could be having other banks verify the information (setting aside the infeasibility of other banks verifying a transaction without their own transaction-level information). Even though they can verify such information, banks would have to collaborate to verify the updated information, which also inevitably generates redundant costs. At worst, due to free-rider problems, each information-receiving bank has insufficient incentive to correct the information and would make no effort to correct inaccuracies. From this point, the automatic nature of distributed ledger can be problematic because it does not prevent accumulation and sharing of erroneous information. In addition, the automatic nature of a distributed ledger can be problematic in terms of liability. When a system assigns liability for errors to relying banks (not providing banks), those entities can do nothing except for opting out of the distributed ledger network to escape liability. Allowing banks to opt-out undermines the

[199] *Id.* at 7-8.

system's expected effectiveness. However, insisting that banks remain in the system might degrade the quality of the information contained in the repository.

Aside from the interplay between blockchain-technology and information sharing, some other concerns could be raised. Any proposal must indicate which (and how many) actors would be involved in the distributed ledger. As the number of entities or institutions using the system increases, all parties would enjoy greater benefits from the larger amount of data generated and shared. However, there could be problems with allowing wider access to such a platform. For example, a group of malevolent individuals could set up a small money service simply to have access to the ledger and monitor when certain transactions or entities have triggered alarms or alerts within the database. Such a possibility undercuts the confidential nature of SARs– normally, SARs are not disclosed to the transacting customers. Second, if a policymaker adopted this multilateral, decentralized approach to data sharing, any proposal must decide whether FinCEN or law enforcement would be able to access the platform. On the one hand, access to the information could help facilitate resolving criminal investigations – sometimes law enforcement agencies use other information contained within the SARs to detect crimes other than money laundering itself. However, providing law enforcement with such access also brings up privacy and efficiency concerns. If FinCEN is able to review the database, would financial institutions still be required to flag suspicious activities or would they be exempt from any liability (as they are now) once they satisfactorily provide adequate information to the database? In addition, there could be separate privacy concerns given that this database would contain large amounts of personal transactional information. Now, that information is being provided to law enforcement in addition to financial institutions.

The introduction of blockchain technology aids in the quick and accurate transfer of information. However, it does not guarantee that the information input into the system is correct. To ensure the quality of information, banks would have to be able to opt-in to the distributed ledger network voluntarily to adequately account for side effects stemming from the imposition of liability onto relying banks. In sum, distributed ledgers can only be a valuable means of transferring information (one aspect of an AML regime) instead of fully replacing the current AML model.

Introducing a Private Cause of Action

The solutions proposed in previous sections deal with modifying liability and reducing redundant costs of information generation. However, these partial solutions do not deal with the problem of defensive filing. Therefore, another solution must be proposed to combat this issue.

This problem has previously been identified and addressed by a theorist named Takáts. In his paper, he argued for increasing the cost of filing to reduce the overall total filed reports.[200] He also illustrated his solution mathematically. However, several questions can be raised in response to such a proposal. First, it is undeniable that increasing the cost of filing can reduce the number of filed reports and force banks to file only the most suspicious transactions. However, as mentioned above, when the expected sanction for a failure to report is exceptionally high and the cost of filing is comparatively negligible, it actually plays an insignificant role in reducing defensive reports. In contrast, if the filing cost is set high, it is also charged for those really suspicious reports. As a result, it is inevitably increasing the

[200] Takáts, *supra* note 27.

total cost of compliance for banks. The increased cost of compliance will exacerbate the problem of de-risking, which is not considered or addressed in Takáts' paper. Moreover, it is difficult to determine the optimal level of any penalties imposed in the real world. This is particularly true in the current regime where law enforcement is already incapable of reading and analyzing all reports filed and correctly identifying which are defensive. In such circumstances, the law enforcement agency is likely unable to accurately set the correct (or optimal) price of filing. Nevertheless, the concept of a higher filing cost is still illuminating. To address the problem of defensive reports, an AML regime should require collaboration from players who possess knowledge to identify which reports are defensive, and in this case, customers themselves ought to be able to verify the information.

In 2010, the British Civil Court of Appeals decided a case involving a customer, Jayesh Shah, and HSBC.[201] At issue was an SAR filed by HSBC after Mr. Shah sought to transfer money out of the country. HSBC had suspected the transaction violated AML laws and filed the SAR. In reply, Mr. Shah asked HSBC to prove the basis of their alleged suspicion. The court finally ruled that "the customer is entitled to proceed with a claim in breach of contract or duty" when the bank failed to carry out the customer's instruction due to suspicion about money-laundering connected to the transaction. This decision changed the landscape of AML regimes. Previously, bank customers could only seek judicial review to challenge decisions made by the governmental agency that had received the SARs from banks. This decision, however, addressed the lack of a private legal remedy for the delay of transactions halted by the filing of an SAR. The decision created conflicts between a bank's obligations to law enforcement under regulatory law and its duties to customers under contract law. On one hand, banks are prohibited from disclosing information regarding SAR filing. On the other hand, banks wish to avoid lawsuits brought by its customers. This case also confirmed that the defendant institution need not show that its suspicion was reasonable. Instead, the defendant institution need only show that its determination that a transaction was suspicious was not irrational.[202]

There are some important lessons in this case. First, it highlighted how banks face conflicting obligations to different parties. It also created an incentive for banks to take SAR filing more seriously. Additionally, it allowed another party with pertinent information to challenge the decision to file a SAR. Even though the court did not intend to address the problem of defensive filing, the decision might be helpful to mitigate such a problem.

Private parties, such as banks and their customers, may have more information and ability to effect change than the government. Governmental actors are quite removed from the transactions and only have access to information as provided by SAR reports filed by banks. Also, the resource constraint limits the government's capacity to read and process all reports filed by the reporting entities. As a result, due to the lack of information and capacity, the government does not have comparative advantage in identifying defensive reports.

Second, allowing customers to sue has other advantages. Incentivized by the damages, customers who strongly believe that the suspicion is unfounded will challenge the content of the report. However, natural separation can emerge. On one hand, a lawful customer who understands the essence of the transaction is able and willing to challenge the filed SAR so as to get compensation for damages. In

[201] Shah v. HSBC Private Bank (UK) Ltd, 2009 WL 6454.

[202] Mikhail Reider-Gordon, *U.S. and International Anti-Money Laundering Developments*, 45 INT'L LAWYER 365, 377-378 (2011).

addition, real money launderers will not initiate suits because bringing one will make their illicit scheme more likely to be detected. Therefore, both the ability and incentive of a lawful customer to challenge a wrongful SAR, and the worries that a money launderer would be caught by initiating suit, suggests that allowing customers to sue would be beneficial.

In detail, the final problem is the design of a regime which allows customers to sue. Conceptually, in order to keep the filing of SARs confidential, the disclosure of filing can be postponed until after the FIU's screening. When the FIU has scrutinized the report and found nothing suspicious or decided not to take action, then the release of such reports can pose little harm to investigation. Moreover, it is reasonable to limit the scope of released reports to only those that do not pass the threshold of further investigation because the filing cannot be said to be "defensive" when the FIU decides to take action after scrutiny. Once the reports have been examined and released, then the bank is allowed and mandated, in the proposed regime, to inform the customer regarding the filing. The customer can then decide to bring the lawsuit or not.

Questions remain about the possible claims. In fact, while difficult to prove the exact amount of harm, it is acceptable that harm is created by the filing itself in an information-sharing regime. When the filing is known to other financial institutions, the customer will likely have to go through a more stringent process of due diligence, and may even be discouraged from or denied certain services. Accordingly, one possible claim which would benefit the customer is the erasure of such records obtained by bringing a lawsuit. However, this proposal does not neglect the tremendous cost associated with litigation. Alternatively, a quicker and more simple way to resolve such disputes may be obtained using an electronic platform similar to those employed in cataloging customer complaints or resolving sales disputes on an online platform. Both parties would upload materials for third-party neutral arbitrators' reviews and decisions.

In fact, the proposed litigation regime is neither infeasible nor inconsistent with current rules.The current safe-harbor rule implies that the financial institutions cannot be liable to their customer for filing reports the breach of their duties to customers under contract law principles.[203] However, some contrary authority exists regarding the extent of this safe harbor provision. The statute appears to indicate (or could be read as saying) that the immunity applies to all statements made in an SAR even if they are not made in good faith or based on probable cause.[204] However, some court decisions have stated that the protection applies only in the case where financial institutions have filed an SAR in good faith[205] or based on an objective identification of a possible violation of law.[206]

By introducing or encouraging the private cause of actions, banks are deterred from filing defensive reports. Compared to the filing-fee model proposed by Takáts, the probabilistic calculation of damages, combined with natural selection between lawful and unlawful customers, saves more cost without exacerbating decreased financial inclusion.

[203] 31 U.S.C. § 5318(g)(3)(A).

[204] LEVI, *supra* note 40, 14-51.

[205] *Lopez v. First Union Nat'l Bank of Florida*, 129 F.3d 1186, 1192–1193 (11th Cir. 1997).

[206] *Bank of Eureka Springs v. Evans*, 353 Ark. 438, 109 S.W.3d 672 (2003).

Appendices

1. Academic Proposal, 22-26 (Section 3), 38-49 (Section 5). [Compliance Costs, Liability Regime, Information Sharing, Blockchain]
2. Stavros Gadinis & Colby Mangels, Collaborative Gatekeepers, 73 Wash. & Lee L. Rev. 797 (2016). [Information Sharing, Liability Regime, Industry Self-Regulation]
3. The Great Chain of Being Sure About Things, The Economist (Oct. 31, 2015). [Blockchain, Distributed Ledgers]
4. Goldman Sachs, Profiles in Innovation: Blockchain 2 – 11, 71 – 7 (2016). [Compliance Costs, Blockchain]
5. Laura Noonan, Banks Face Pushback Over Surging Compliance and Regulatory Costs, Fin. Times (May 28, 2015). [Compliance Costs]
6. Matthew Britton, Could Blockchain Solve the KYC/AML Challenge?, BCS Consulting (Sept. 29, 2016). [Compliance Costs, Blockchain, Distributed Ledgers, Network Effects, Digital Identities]
7. Henry Engler, Blockchain Faces Maze of Regulatory Complexities, Questions and Challenges, Thomson Reuters (Feb. 23, 2016). [Blockchain, Centralized Agency]
8. FCA New Technologies and Anti-Money Laundering Compliance Report, 1 – 4, 11 – 3, 18 – 32 (2017). [Digital Identities, Blockchain, Regulatory Landscape]
9. FinCEN Joint Statement on Innovative Efforts to Combat Money laundering and Terrorist Financing (December 3,2018). [Regulatory Landscape, Centralized Agency]
10. Ross P. Buckley & Rebecca L. Stanley, Protecting the West, Excluding the Rest: The Impact of the AML/CTF Regime on Financial Inclusion in the Pacific and Potential Responses, 17 MEJ JIL 83, 84 – 7; 93 – 5; 100 – 5 (2016). [De-risking, Financial Inclusion]
11. Maria A. de Dios, The Sixth Pillar of Anti-Money Laundering Compliance: Balancing Effective Enforcement with Financial Privacy, 10 Brook J. Corp. Fin & Com. L. 495 – 500, 502 – 5; 507 – 12; 514 – 6 (2016). [Privacy Concerns, Regulatory Landscape]
12. Kevin Werbach, Trust But Verify: Why the Blockchain Needs the Law, 33 Berkeley Tech. L. J. 487, 507 – 13, 525 – 6, 534 – 41 (2018). [Distributed Ledgers, Centralized Agency, Blockchain, Regulatory Landscape]
13. Dirk A. Zetzsche, Ross P. Buckley & Douglas W. Arner, *The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain*, 2018 UILLR 1361 – 73 (2018). [Distributed Ledgers, Blockchain, Liability Regime]

Optional Materials

14. FFIEC BSA/AML Manual – Information Sharing
15. FFIEC BSA/AML Manual – Suspicious Activity Reporting
16. FFIEC BSA/AML Manual – Customer Due Diligence
17. FinCEN Guidance on Section 314(b) of the USA PATRIOT Act
18. FinCEN Section 314(b) Information Sharing Fact Sheet

19. Dirk A. Zetzsche, Ross P. Buckley & Douglas W. Arner, The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain, 2018 UILLR 1382 – 1404 (2018).
20. Academic Proposal, 17-22 (Sections 1-2), 26-38 (Section 4).
21. FCA Feedback on Distributed Ledger Technology Discussion Paper, 22 – 24 (2017).

HARVARD LAW SCHOOL | The Case Studies

CSP060
APRIL 2020

CLOUD Act Enforcement

RYAN CHAN-WEI AND SEBASTIAN STEUER

Memorandum

DATE: February 18, 2020
TO: Junior Attorneys, Terrorist Financing Task Force
FROM: William Parr, Vice-Chair, Terrorist Financing Task Force
RE: Pursuing enforcement actions under the U.S. CLOUD Act

In one of our most important terrorist finance investigations, we have run into a complex transatlantic data privacy issue involving FinTech customer data stored on a cloud server in Europe. We have a series of urgent meetings with key stakeholders scheduled for next week, and our new Chair would like to be briefed on these matters by the end of this week.

As some of you may know, the [redacted] recently foiled an attempted terrorist attack on [redacted], and subsequent investigations revealed that the operation was partly funded by [redacted]. Early investigative leads have revealed that the mastermind behind the attack was [redacted], working in conjunction with the European branch of the [redacted] [redacted] terrorist organization. One major figure in the planning and financing of the attack might be [redacted], a Swiss citizen currently believed to live in a suburb of Zurich.

However, the investigation into the financier has hit a significant roadblock because we have trouble accessing his financial records. The money has most likely been channeled to the attackers through the financier's account with [redacted], a Paris-based FinTech company specializing in international payments services. Obviously, we would like to get access to these financial records as soon as possible to proceed with our investigation. Unfortunately, the FinTech company is very proud of its privacy policies and it is very unlikely that it would be willing to cooperate on a voluntary basis.

Written by Ryan Chan-Wei and Sebastian Steuer under the supervision of Howell E. Jackson, James S. Reid, Jr., Professor of Law at Harvard Law School. Case development at Harvard Law School is partially funded by a grant from Dechert LLP. Cases are developed solely as the basis for class discussion. They are not intended to serve as endorsements, sources of primary data, legal advice, or illustrations of effective or ineffective management.

Copyright © 2020 President and Fellows of Harvard University. No part of this publication may be reproduced, stored in a retrieval system, used in a spreadsheet, or transmitted in any form or by any means—electronic, mechanical, photocopying, recording, or otherwise—without permission. To order copies or permissions to reproduce materials please visit our website at casestudies.law.harvard.edu or contact us by phone at 617-496-1316, by mail at Harvard Law School Case Studies Program, 1545 Massachusetts Avenue – Areeda 507, Cambridge, MA 02138, or by email at HLSCaseStudies@law.harvard.edu.

A traditional method of getting access to the data would be to rely on mutual legal assistance of our European colleagues under the applicable mutual legal assistance treaties ("MLAT").[1] However, these procedures have often proven inflexible and slow. There is also a high risk that the length of the MLAT process may result in a leak of the investigation to the suspect, which would allow them to evade arrest.

This is why we are currently exploring a different option. We discovered that the FinTech company is a heavy user of remote computing services and stores all of its customer data "in the cloud." Specifically, they employ the services of [redacted], one of the largest U.S.-based internet companies. [redacted], stores the data on servers close to its customers and, in this case, all the data we need is stored on servers in France.

Our aim now is not to get the data from the FinTech company, but from the cloud computing provider. We are aware that the general Department practice is to reach out to the enterprise directly and to avoid asking cloud service providers for enterprise customer data. However, after long discussions with the legal team, we have concluded that the requirements are met for an exception under the relevant Department policies.[2] The U.S. Attorney's Office for the Southern District of New York was eventually able to obtain a warrant issued under the Stored Communications Act ("SCA") as amended by the Clarifying Lawful Overseas Use of Data Act ("CLOUD Act")[3]. Using the powers under the CLOUD Act would allow us, in principle, to sidestep the MLAT process. However, our CLOUD Act approach is not free of problems either and, due to strict European data protection rules, there is now a severe transatlantic conflict of data privacy laws.

As you may have heard, the European Union's approach to privacy and data protection differs fundamentally from the U.S. approach. On the one hand, the field of information privacy law in the U.S. is essentially a patchwork of constitutional and statutory provisions. These rules often address specific and rather narrow aspects of privacy, or set out data protection standards only for certain industries. On the other hand, the European framework is much more uniform and holistic. Another important conceptual difference is that in the U.S., the processing of personal data is generally allowed unless there is a specific law that restricts such processing. The European thinking, by contrast, starts from the notion that every individual has a constitutionally protected right to privacy and data protection that prohibits the collection and processing of personal data. The processing is only lawful if a specific law allows it.

In this case, because both the FinTech company and the cloud service provider have a physical presence in the E.U., the data also falls within the scope of the European General Data Protection Regulation[4] ("GDPR"). Among other things, this regulation sets out tough restrictions for data transfers to third countries (*i.e.*, data transfers to entities located outside of the E.U.). Therefore, from the perspective

[1] *See* Agreement on Mutual Legal Assistance, E.U.–U.S., Jun. 25, 2003, T.I.A.S. No. 10-201.1; see also Instrument as contemplated by Article 3, paragraph 2, of the Agreement on Mutual Legal Assistance between the United States of America and the European Union signed 25 June 2003, as to the application of the Treaty on Mutual Legal Assistance in Criminal Matters Between United States of America and France signed 10 December 1998, Fr.–U.S., Jun. 25, 2003, T.I.A.S. No. 10-201.32.

[2] *See* DOJ, *Seeking Enterprise Customer Data Held by Cloud Service Providers* (Dec. 2017), https://www.justice.gov/criminal-ccips/file/1017511/download.

[3] Stored Communications Act, 18 U.S.C. Chapter 2701, *et seq.*, as amended by the Cloud Act, Pub.L. 115–141 (which also amended the Electronic Communications Privacy Act, 18 U.S.C. 2510, *et seq.*).

[4] Regulation (E.U.) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1.

of European law, the cloud provider cannot easily produce the data stored on its European servers to the U.S. government, because it is obligated to observe the strict GDPR requirements for data transfers to third countries. While going through an MLAT generally satisfies the GDPR transfer requirements, it is very difficult to execute a transfer directly from the provider to the U.S. government without any involvement of E.U. or E.U. Member State authorities.

From the perspective of U.S. law, however, it does not matter where the data is stored. The SCA only requires that the internet company qualifies as a remote computing service provider pursuant to the relevant definition,[5] and that the data is within the provider's "possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States."[6] Thus, we are in a situation where U.S. law potentially demands that the provider violate GDPR transfer provisions by handing over data stored in the E.U. to U.S. authorities.

To refresh your memory of the CLOUD Act, I have attached as Annex A a note circulated by Julia from the Office of Policy and Legislation last year after the Department published its White Paper. For a more detailed introduction, you may also want to refer to the White Paper itself, which is included in the Appendices. Additionally, I have also attached as Annex B a note prepared by Jack giving an overview of the relevant GDPR provisions. For a more detailed overview of the "different visions of data privacy" on the opposite sides of the Atlantic, you may also wish to refer to the appended Georgetown Law Journal article by *Schwartz* and *Pfeifer*.[7]

Unfortunately, this current case only represents the tip of the iceberg. As the investigation progresses, it is inevitable that more essential information will be uncovered, and it is highly probable that the process of obtaining that information will give rise to further data privacy issues and conflicts with the GDPR. Furthermore, in light of the increasingly cross-jurisdictional nature of terrorist funding, similar cases are likely to emerge again soon. Given the manifold ways of storing and encrypting data in the cloud, we will likely be confronted with even more complex problems soon. Future cases may include complications such as non-U.S. based cloud providers, data shards, and data trusts.

Lastly, encryption is another topic that we should keep in mind. This is not a pressing issue at the moment because the cloud provider in this case should be able to give us access to the unencrypted data. However, the CLOUD Act is explicitly "encryption-neutral" and does not require providers to be capable of decrypting their data. Thus, it is highly likely that a case will eventually arise where we obtain a warrant for cloud-stored data only to find out that the data has been encrypted and the cloud-storage provider is not in possession of the keys necessary to decrypt the data. Such encrypted data would pose a severe impediment to law enforcement efforts because the commonly used ciphers cannot be cracked even with the entire computing power of our government. This may change once we have powerful quantum computers, but unfortunately this will still take quite a while, notwithstanding recent advances in that field of technology. Until then, we have to be aware of the limits that encryption sets on our ability to access the global cloud even with the geographically broad access that the CLOUD Act gives us.

It is therefore essential for us to have a deep understanding of these issues and a clear policy on how to deal with the CLOUD Act, especially in relation to data stored in the E.U. To that end, a meeting is

[5] 18 U.S.C. § 2711(2).

[6] 18 U.S.C. § 2713.

[7] Paul M. Schwartz and Karl-Nikolaus Pfeifer, *Transatlantic Data Privacy Law*, 106 GEO. L. J. 115 (2017).

scheduled next week with our new Chair and several key stakeholder groups to explore future steps. In preparation for that meeting, it will be your job to brief the Chair on some of the key issues that will likely be discussed.

Introduction

To get everybody on the same page, we should start the briefing with a quick introduction to the CLOUD Act. The Chair should be briefed on the developments that led to the need for a "clarification" of the extraterritorial reach of SCA warrants, namely the *Microsoft*[8] case, and the purposes that Congress pursued in passing the CLOUD Act. Specifically, the brief should explain why the traditional MLAT process is no longer appropriate in today's highly digitalized and globalized world, and why the CLOUD Act helps law enforcement adapt to the times. Furthermore, the introduction should quickly sketch the main features of the CLOUD Act, highlighting in particular the providers' options to file a motion to quash a warrant. The brief should also address the significance of the so-called "qualifying foreign governments" ("QFG").

The main part of the briefing should then be structured around some specific issues that will likely be brought up by the stakeholder groups. In the remainder of this memorandum, I will call your attention to what I believe are the main issues that should be discussed with the relevant stakeholder groups.

European Data Protection Representatives

The Chair will be meeting with public stakeholders that have an interest in the observance of the GDPR. This includes officials from the European Commission, the European Data Protection Board ("EDPB"), the European Data Protection Supervisor ("EDPS"), and the French Data Protection Authority (the Commission Nationale de l'Informatique et des Libertés, or "CNIL"). The Chair will need to be briefed on the European perspective in this case, namely how the conflict between the CLOUD Act and the GDPR might be resolved, and if it is at all possible to do so.

Unfortunately, at the moment it appears that service providers are caught between a rock and a hard place, because complying with a warrant issued under the CLOUD Act invariably leads to them violating the GDPR. The Chair needs to be briefed on how the Europeans interpret the GDPR provisions regarding data transfers out of the E.U. (see Annex 2 for an overview of these provisions). It would, of course, be desirable if we can find a way to resolve this conflict without the need to enter into any new agreements. I suspect that the officially published communications by the EDPB will take a particularly strict stance on the GDPR's data transfer provisions, and advocate for a very narrow interpretation of any exceptions. However, in practice it is the Member States authorities who make the decisions. In our experience, when it comes to granting exceptions, they often tend to be a bit more flexible than one would expect from a literal reading of the official guidelines. This is especially true for time-sensitive terrorism cases, where bureaucratic blockades of data transfers might have particularly dire consequences.

[8] *Microsoft Corp. v. United States*, 829 F.3d 197 (2d Cir. 2016). In this case, Microsoft successfully challenged a subpoena for data stored on an Irish server. The case was appealed and heard by the Supreme Court, and judgment was vacated and the case remanded with instructions to dismiss the case as moot after the passage of the CLOUD Act, *see United States v. Microsoft Corp.*, 584 U.S. ___, 138 S. Ct. 1186 (2018).

Another possible way out of this dilemma would be if the U.S. were to enter into an executive agreement with the E.U. or individual Member States, recognizing them as a "qualifying foreign government." The existence of an executive agreement might legalize the data transfer under GDPR rules. Even if this was not the case, the executive agreement would open up an avenue by which the CLOUD Act warrant could be quashed or modified (as long as the suspect is neither a United States citizen nor resident in the United States) under the CLOUD Act's specific comity analysis. An executive agreement should also be to the benefit of the E.U. and its Member States. Due to the worldwide operations of the big U.S. tech companies, we receive myriad MLAT requests every year ourselves, including from Europe. An executive agreement would allow law enforcement authorities in E.U. Member States to request data directly from U.S. service providers.

Looking to the future, the Chair also needs to be briefed about the likelihood that transatlantic agreement can be reached on evidence-sharing in criminal procedures and the current state of negotiations. Notwithstanding some differences in the scope of privacy regulation, we have always been able to find common ground for cooperation in the past. Frankly, I would be surprised if the Europeans fundamentally disagreed with the underlying approach of the CLOUD Act. After all, they currently have a proposal pending for an e-Evidence Directive that bears much similarity to the CLOUD Act and, to me, this suggests that the E.U. and the U.S. are generally on the same page concerning the need for reform to adapt to the increasingly digital world in which we now live.

Privacy Advocates

The Chair will also be meeting with stakeholders who resolutely oppose the CLOUD Act, such as the Open Technology Institute, the American Civil Liberties Union, and the Electronic Frontier Foundation. She needs to be briefed on the rationale behind their opposition to the CLOUD Act, and whether those positions can be reconciled with those of the Act's proponents.

The privacy concerns with respect to the U.S. government seeking access to data stored abroad are not necessarily the same as those with respect to qualified foreign governments seeking access to data stored with providers subject to U.S. jurisdiction. To this end, it might be advisable to differentiate between the different parts of the CLOUD Act.

Those who criticize the CLOUD Act for failing to adequately protect human rights often focus on the part of the Act that enables qualified foreign governments to access data without going through the MLAT process. Their key argument is that the Act's human rights and privacy safeguards are not sufficiently rigorous and might therefore threaten the privacy of U.S. citizens whose data can be accessed by foreign governments without any significant involvement from U.S. courts or authorities. In this respect, it is essential to have a clear picture of exactly which aspects of the Act are being criticized by the privacy and human rights advocates.

The Chair will presumably also discuss the encryption problem with these stakeholders.[9] Under the existing legislation, there is virtually nothing we can do to require providers to be capable of

[9] Other teams within the Department have already done substantial work on encryption-related issues. Therefore, we have requested if a member of these teams could participate in the meeting to give a quick summary presentation. In this case, you would not need to include this issue in your brief. Please check with your supervisor if we have received a response from the other teams before you start working on this part of the brief.

decrypting cloud-stored data. They are free to set up their systems so that only the customer has access to the keys necessary to decrypt the stored data, and potentially frustrate any attempt of the government to access the data through the provider. Unsurprisingly, privacy supporters are quite happy with the status quo. On the other hand, the Department has repeatedly urged Congress to adopt laws requiring communication providers to be able to decrypt any customer data (sometimes referred to as "backdoor" policies).

The Attorney General recently reheated this debate in an emphatic speech. Proponents, including our Department leadership, tend to argue that absent backdoor laws, terrorists and criminals can use encryption to operate completely in the dark. As a result, the government would no longer be able to effectively protect national security and the lives of American people. In response, most counterarguments question the technical feasibility of "backdoors," and express concern over the privacy risks that they would inevitably introduce. We certainly do not need to go into all the details and many dimensions of this debate in preparation for the meeting, but it would be helpful if you could briefly summarize the chief arguments on both sides.

Cloud Computing Providers

The Chair will be meeting with representatives of the leading global cloud computing providers (*e.g.*, Google, Amazon, and Microsoft), all of whom are based in the United States. It is important for us to maintain a functioning working level relationship with these providers.

The Chair is interested in understanding their opinions on the CLOUD Act, and if there are any differences between them. Microsoft, for example, is usually mentioned as a *supporter* of the CLOUD Act. This is not self-explanatory given the non-trivial conflict that a CLOUD Act warrant may put them in (*i.e.*, forcing them to violate either the order of the United States government or the GDPR). Furthermore, internet companies usually claim that they have a strong interest in keeping their customers' data private. Therefore, it would be interesting to know what factors drive their support of the CLOUD Act.

Another set of issues that the Chair wishes to discuss with the cloud providers relates to the different technical models by which data can be stored in the cloud, namely data localization models (where the data is stored on one server in a particular country, usually near the customer), data shards (where the data is split up into pieces and stored across many servers in many countries) and data trusts (where the main provider cooperates with a trustee and thus has no immediate access to the data).[10] Presumably, it would be sensible to give the Chair a quick primer on these three models and then analyze if there are any differences as to their treatment under the CLOUD Act. Such differences could potentially exist a) with respect to the question whether the data is in "possession, custody, or control" of the provider, or b) with respect to the comity analysis that has to be carried out if the provider tries to quash the warrant.

[10] We assume that other teams within the Department already have some experience with the data storage models commonly used by U.S. cloud service providers. As with the encryption issues, we have therefore requested if one of their experts could participate in the meeting to give a quick summary presentation. In this case, you would not need to include this issue in your brief. Please check with your supervisor if we have received a response from the other teams before you start working on this part of the brief.

FinTech Coalition

The Chair will be meeting with stakeholders from a FinTech coalition, comprising companies both from the U.S. and abroad. They are concerned about how the CLOUD Act will impact their business model, and the Chair needs to be briefed about the potential implications of the Act on the ability of FinTechs to protect data privacy. While our specific case especially attracted the attention of other FinTech companies, keep in mind that the data privacy issues raised by the CLOUD Act are also of broader relevance for the financial industry and cloud computing customers in general.

To obtain a better understanding of the underlying business considerations, the Chair would first like to obtain a quick overview of the increasing relevance of cloud computing in the financial sector, with a focus on why more and more financial companies are outsourcing their IT to cloud computing providers, and on the risks associated with this practice.

Importantly, the Chair should also be briefed on the options that cloud users have to evade the reach of the CLOUD Act and, thus, potentially enhance the privacy protection of their customers' data. Besides the idea of using data trusts (which we will have already discussed with the cloud computing providers), there are two other strategies that should be considered.

First, cloud computing users could try to switch to providers that are not based in the U.S. or enter into storage agreements only with the foreign subsidiaries of U.S.-based providers. Obviously, this only helps if the foreign provider is not subject to the CLOUD Act as well. Thus, some inquiry into the territorial applicability of the CLOUD Act with respect to providers (and not only to their data) might be necessary.

Second, cloud computing customers may think about using encryption and key management options that would prevent the provider from accessing the unencrypted data from the outset.[11] The Chair is certainly not interested in all the technical details but it would be helpful to provide a brief overview of the common options for customers to encrypt their data in the cloud and the implications of these options for government requests.[12] You can assume that all of the three major cloud providers offer, at least on the level of abstraction that is of interest for us, roughly similar encryption options.

Legal Scholars

Finally, the Chair will be meeting with a group of legal scholars who are experts in data protection law and international law. This meeting is particularly important, because she hopes to obtain the validation and buy-in of key academic stakeholders. Support from the legal academy will be essential in structuring our policy positions, given the number of complex legal issues that arise when pursuing

[11] *EBA, Guidelines on Outsourcing (EBA/GL/2019/02)*, Eur. Bkg. Auth. ¶. 68(e) (Feb. 25, 2019), https://eba.europa.eu/documents/10180/2551996/EBA+revised+Guidelines+on+outsourcing+arrangements.pdf/38c80601-f5d7-4855-8ba3-702423665479, Privacy concerns are not the only reason why financial institutions might be interested in encrypting their data. Encryption is also an important building block of general cybersecurity risk management procedures. According to the European Banking Authority, institutions and payment institutions should, when employing cloud computing services, "consider specific measures, where necessary, for data in transit, data in memory and data at rest, such as the use of encryption technologies in combination with an appropriate key management architecture", *see* Deloitte, *Deloitte Note: EBA Guidelines on Outsourcing (EBA/GL/2019/02)*, DELOITTE ¶ 68(e) (Feb. 25, 2019) (summarizing the EBA Guidelines), https://www2.deloitte.com/content/dam/Deloitte/cy/Documents/risk/CY_Risk_EBA%20outsourcing%20guidelines.pdf.

[12] As indicated earlier (*supra* note 9), other teams within the Department have already done substantial work on encryption-related issues, and we have requested if one of their experts could participate in the meeting. If this is the case, the expert's presentation will likely also cover encryption key management, and you would not need to include this issue in your brief. Please check with your supervisor if we have received a response from the other teams before you start working on this part of the brief.

enforcement actions under the CLOUD Act. Prior to this meeting, the Chair will need to be briefed on a number of normative questions.

In this context, the Chair should first be briefed on the fundamental ways to think about the meaning of "territoriality" when it comes to data and privacy. If the established categories no longer fit, it is easier to justify why we need to explore new regulatory paths and use innovative mechanisms such as those under the CLOUD Act.

Second, we need to brief the Chair on how requests for data under the CLOUD Act interact with, and possibly even threaten, the sovereignty of another country. This requires some analysis on how we should understand sovereignty in the context of the global cloud. There are no straightforward or easy answers to this question. After all, the interests that states have in exercising authority over and protecting the privacy of the data stored on servers in their territory may vary according to the circumstances of the individual case.

We certainly need not reinvent the wheel in these debates. However, it would be helpful for the Chair to have an overview of the key debates in the academic literature before she meets with some of the leading scholars in the field.

Lastly, as you can see, even though the CLOUD Act has the word "*Clarifying*" in its name, many questions still remain to be answered, and the Act opens up yet another chapter in the decades-long transatlantic struggle over data privacy. I hope that your briefings for the Chair will shed some light on these issues and help us gain a better understanding of how best to respond to the changes brought by the digital cloud.

Many thanks, and I look forward to seeing everyone later this week

Appendix I – Note on The CLOUD Act

DATE: April 19, 2019

TO: All Attorneys, Criminal Division

FROM: Julia Ehrenreich, Legal Analyst, Office of Policy and Legislation

RE: U.S. CLOUD Act

You may have already read the Department's White Paper on the CLOUD Act that was published last week, but it may nevertheless be helpful to have a quick internal overview of the underlying purpose of the Act and its key provisions before we use of it in practice.

At its core, the CLOUD Act was introduced to "speed access to electronic information held by U.S.-based global providers" because the mutual legal assistance process occasionally proved "too cumbersome" and hindered electronic evidence from being processed in "a timely manner."[1] To this end, the CLOUD Act compels a U.S. service provider to disclose electronic data "regardless of whether such communication, record, or other information is located within or outside the United States."[2]

From an enforcement perspective, this is a powerful tool. It means that only the ability to access the data matters and not the location where the data is actually physically stored. The Act is, therefore, a significant development, because it represents "a first step in what may be a paradigm shift in how access to digitized data is regulated."[3]

Before the passage of the CLOUD Act, it was unclear whether the mere accessibility of data by a U.S. information service provider sufficed to enforce a warrant under the Secured Communications Act (SCA). The following figure illustrates that shift in paradigm:

[1] U.S. Department of Justice, *Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act*, U.S. DEP'T OF JUSTICE 2 (Apr. 2019), https://www.justice.gov/opa/press-release/file/1153446/download.

[2] 18 U.S.C. § 2713 (2018).

[3] Frederick T. Davis and Anna R. Gressel, *Storm Clouds or Silver Linings? The Impact of the U.S. CLOUD Act*, 45 LITIGATION 1, 5 (2018), https://www.americanbar.org/groups/litigation/publications/litigation_journal/2018-19/fall/storm-clouds-or-silver-linings/, https://www.debevoise.com/insights/publications/2019/02/storm-clouds-or-silver-linings.

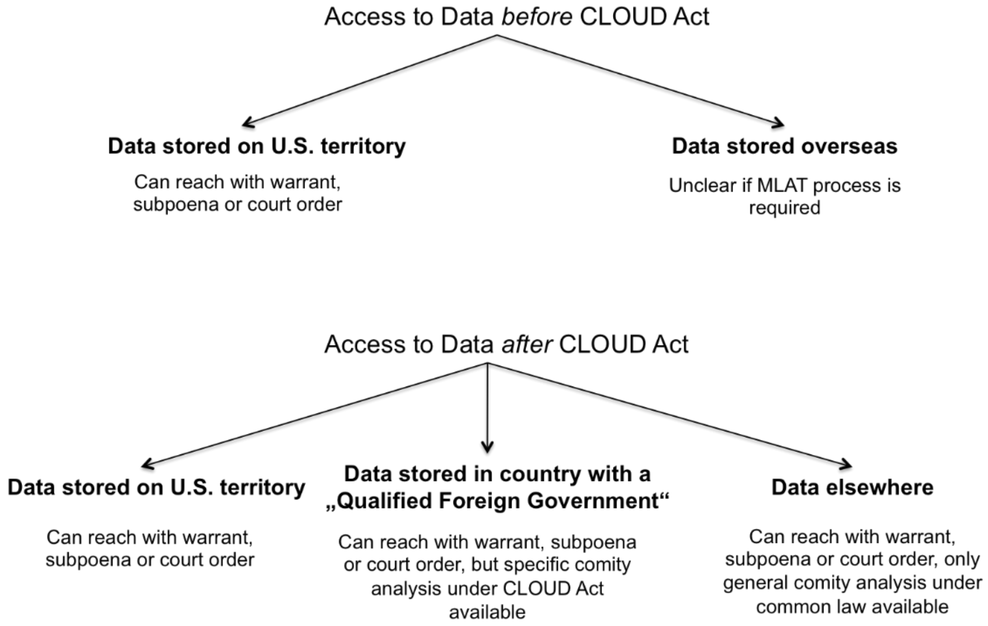

Access to Data *before* CLOUD Act
Data stored on U.S. territory
Can reach with warrant, subpoena or court order
Data stored overseas
Unclear if MLAT process is required
Access to Data *after* CLOUD Act
Data stored on U.S. territory
Can reach with warrant, subpoena or court order
Data stored in country with a „Qualified Foreign Government“
Can reach with warrant, subpoena or court order, but specific comity analysis under CLOUD Act available
Data elsewhere
Can reach with warrant, subpoena or court order, only general comity analysis under common law available

Figure 1. Changes Introduced by the CLOUD Act[4]

However, the extraterritorial reach of the CLOUD Act naturally gives rise to conflicts of laws and the Act, therefore, also provides for the possibility of quashing (or modifying) a CLOUD Act request if, *inter alia*, compliance with the order would breach the laws of a "qualifying foreign government." Whether the United States recognizes another country's government as a "qualifying foreign government" turns on several safeguards, such as whether the country has "adequate substantive and procedural laws on cybercrime and electronic evidence" and "sufficient mechanisms to provide accountability and appropriate transparency regarding the collection and use of electronic data by the foreign government."[5] It is noteworthy that the Act does not preclude courts from quashing the request under a common law comity analysis even when the foreign country does not have a "qualifying foreign government."[6]

The following flowchart, extracted from a Dechert LLP white paper, provides a helpful summary of the new process introduced by the CLOUD Act.[7]

[4] *Id.*; "MLAT" refers to a *mutual legal assistance treaty*, which is a reciprocal agreement between two or more countries to exchange information that aids in the enforcement of criminal law; "belong" refers to "possession, custody, or control" of the data (18 U.S.C. § 2713); the term "United States person" means a citizen or national of the United States, an alien lawfully admitted for permanent residence, an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation that is incorporated in the United States (18 U.S.C. § 2523).

[5] 18 U.S.C. § 2523 (2018).

[6] H.R. 1625, 115th Cong. div. V, § 103(c) (providing a rule of construction for 18 U.S.C. § 2703).

[7] Ben Barnett, Jeffrey A. Brown, Dr. Olaf Fasshauer, Vernon L. Francis and Theodore E. Yale, *Forecasting the Impact of the New US CLOUD Act*, DECHERT (Apr. 2018), https://www.dechert.com/content/dam/dechert%20files/knowledge/publication/2018/4/White%20paper%20-%20Cybersecurity%20-%20Cloud%20Act%20-%2004-18.pdf.

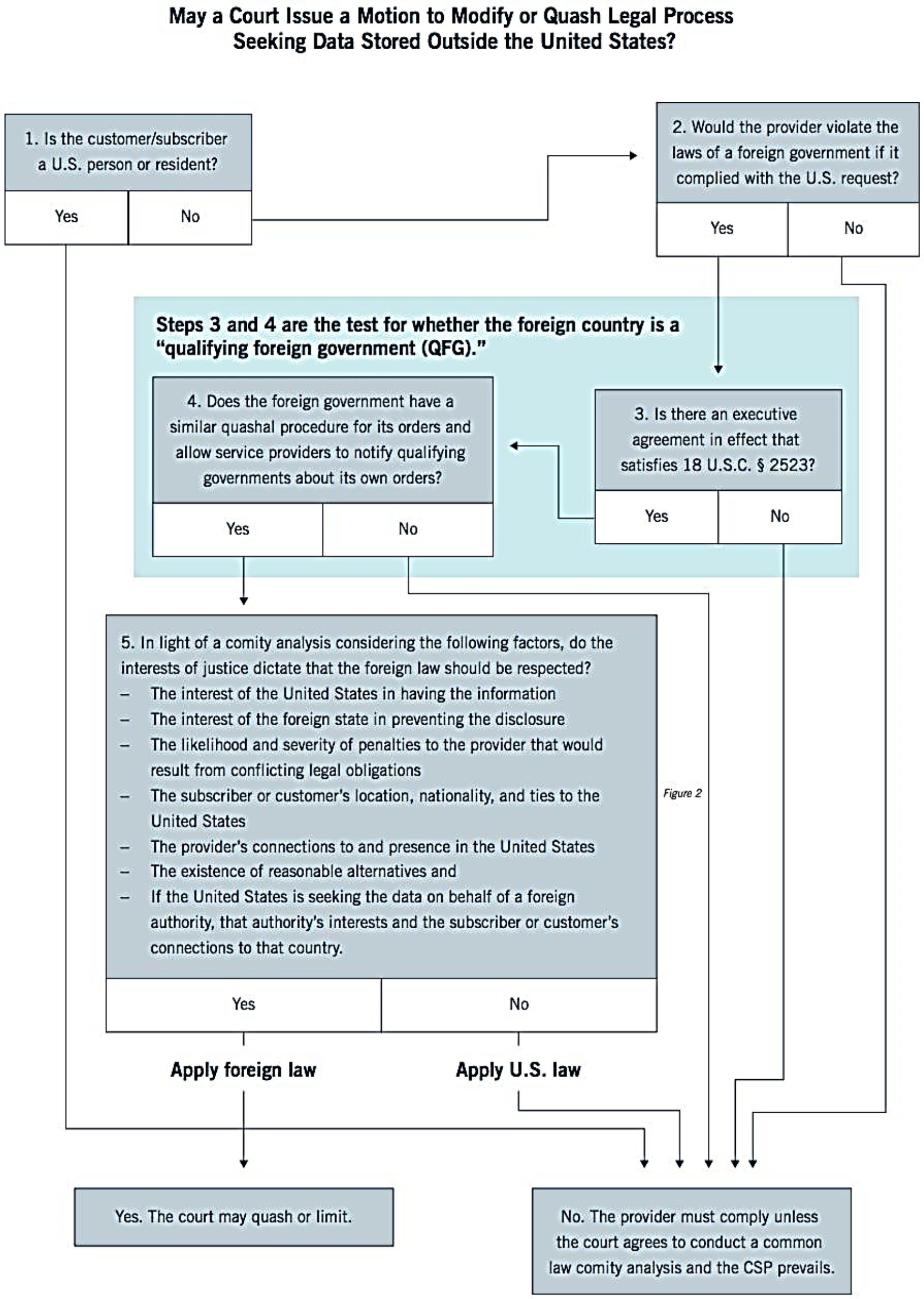

May a Court Issue a Motion to Modify or Quash Legal Process Seeking Data Stored Outside the United States?
1. Is the customer/subscriber a U.S. person or resident?
Yes
No
2. Would the provider violate the laws of a foreign government if it complied with the U.S. request?
Yes
No
Steps 3 and 4 are the test for whether the foreign country is a "qualifying foreign government (QFG)."
4. Does the foreign government have a similar quashal procedure for its orders and allow service providers to notify qualifying governments about its own orders?
Yes
No
3. Is there an executive agreement in effect that satisfies 18 U.S.C. § 2523?
Yes
No
5. In light of a comity analysis considering the following factors, do the interests of justice dictate that the foreign law should be respected?
– The interest of the United States in having the information
– The interest of the foreign state in preventing the disclosure
– The likelihood and severity of penalties to the provider that would result from conflicting legal obligations
– The subscriber or customer's location, nationality, and ties to the United States
– The provider's connections to and presence in the United States
– The existence of reasonable alternatives and
– If the United States is seeking the data on behalf of a foreign authority, that authority's interests and the subscriber or customer's connections to that country.
Figure 2
Yes
No
Apply foreign law
Apply U.S. law
Yes. The court may quash or limit.
No. The provider must comply unless the court agrees to conduct a common law comity analysis and the CSP prevails.

Figure 2. Responding to a CLOUD Act Request[8]

Another key aspect of the CLOUD Act is that it makes it easier for foreign law enforcement agencies to access data held by U.S. providers by allowing QFGs to request data from such providers directly and without going through the MLAT process. Because most of the world's largest internet companies are based in the U.S., the DoJ has to deal with myriad requests by foreign governments under

[8] *Id.*; for the details of what would constitute an executive agreement that satisfies 18 U.S.C. § 2523, see ORIN KERR, COMPUTER CRIME LAW 37-43 (4th ed. Supp. 2018) in the appendix; "CSP" refers to a cloud service provider.

various MLATs. To make this process more efficient, which would be in the interest of both the U.S. and foreign governments, the DoJ had long sought to establish an alternative framework. Notably, this project had started even before the issues pertaining to overseas-stored data attracted considerable attention. The part of the Act dealing with the extraterritorial reach of SCA warrants was added to this project only later, and after the government's defeat in the Second Circuit in the *Microsoft* case.[9]

[9] *Microsoft Corp. v. United States*, 829 F.3d 197 (2d Cir. 2016). In this case, Microsoft successfully challenged a subpoena for data stored on an Irish server. The case was appealed and heard by the Supreme Court, and judgment was vacated and the case remanded with instructions to dismiss the case as moot after the passage of the CLOUD Act, *see United States v. Microsoft Corp.*, 584 U.S. ___, 138 S. Ct. 1186 (2018).

Appendix II – Note on GDPR Data Transfer Rules

DATE: February 15, 2020

TO: William Parr, Vice-Chair, Terrorist Financing Task Force

FROM: Jack Hoffmann, Junior Analyst, Terrorist Financing Task Force

RE: GDPR Data Transfer Rules

This note provides a brief overview of the data transfer rules under the European Union's General Data Protection Regulation (GDPR).[10] The objective is to lay out the core principles, without going into all the details of this complex body of law.[11]

As the first word of its title suggests, the scope of the *General* Data Protection Regulation is extremely broad. It uses very extensive definitions of "personal data" and "processing" (Article 4(1) and (2) GDPR), and is not limited to automated processes. It applies across industries, and to data processing by both the private and the public sector. It is also important to note that the GDPR does not only protect data subjects located in the European Union. So long as an enterprise has a minimal physical—not necessarily legal—establishment in the Union, GDPR requirements apply to all operations in connection with this establishment, regardless of the location of the data subject (Article 3(1) GDPR).[12]

Arguably, the most important GDPR provision is Article 6(1), pursuant to which any processing of personal data is only lawful if at least one of six justifications applies. These justifications are consent, contract, compliance with a legal obligation, vital interests of the data subject, carrying out tasks in the public interest, and legitimate interests. It is important to note that as a general matter that the mere existence of legitimate interests does not suffice to justify the processing under the legitimate interests clause; rather, the legitimate interests have to be of such significance that the relevant rights and interests of the data subject do not outweigh them.

According to European doctrine, a data transfer out of the E.U. constitutes a processing in and of itself and must be justified by one of the justifications under Article 6(1). In addition to Article 6(1), Title V of the GDPR (Articles 44 through 50) includes further restrictions with respect to data transfers to third countries. The objective of these restrictions is to ensure that the strict GDPR standards for data processing cannot simply be undercut by transferring the data from European territory. The penalties

[10] Regulation (E.U.) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1.

[11] One important feature of the GDPR not reflected in this note is the distinction between data controllers and processors. A data controller is any "natural or legal person…which…determines the purposes and means of the processing of personal data" (Art. 4(7) GDPR). A processor is any "natural or legal person…which processes personal data on behalf of the controller" (Art. 4(8) GDPR). The terminology is somewhat confusing, as both the controller and the processor can "process" data (as defined in Art. 4(2) GDPR). In each case, the limitations discussed in this note apply. If a natural person has an account with a cloud computing provider, the provider would be the processor. If an enterprise stores customer data in the cloud, the enterprise would be the controller and the cloud provider the processor. In general, the processing of data by a processor is subject to additional requirements specified in Art. 28 GDRP, and in particular limited by the processing agreement between the processor and the controller. However, we currently assume that the processing agreements used by the major U.S. cloud providers would allowa data transfer in response to an SCA warrant. Under these circumstances, the distinction between processors and controllers would not matter for purposes of the CLOUD Act.

[12] Absent an establishment in the Union, the GDPR may still apply so long as the E.U. market is targeted, *see* Art. 3(2) GDPR. Only in this case the applicability is limited to data subjects who are located in the Union.

imposed for noncompliance with the GDPR are severe. Pursuant to Article 83 of the GDPR, unauthorized "transfers of personal data to a recipient in a third country" can be punished by "administrative fines up to $20 million E.U.R, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher."

According to Article 48 of the GDPR, "[a]ny judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognized or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State." Thus far, only the United Kingdom has entered into an agreement with the U.S. regarding the CLOUD Act that may qualify as an agreement under Article 48.[13] Apart from the special case of the UK, there are only traditional MLAT agreements in place between the U.S. and the E.U. and/or its Members States.

In addition to Article 48, Recital 115 of the GDPR makes very clear that the E.U. is not willing to accept the extraterritorial application of third countries' laws absent any agreement. Apparently, European lawmakers already anticipated the situation under CLOUD Act in this recital:

> Some third countries adopt laws, regulations and other legal acts which purport to directly regulate the processing activities of natural and legal persons under the jurisdiction of the Member States.
>
> This may include judgments of courts or tribunals or decisions of administrative authorities in third countries requiring a controller or processor to transfer or disclose personal data, and which are not based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State.
>
> The extraterritorial application of those laws, regulations and other legal acts may be in breach of international law and may impede the attainment of the protection of natural persons ensured in the Union by this Regulation.
>
> Transfers should only be allowed where the conditions of this Regulation for a transfer to third countries are met.
>
> This may be the case, inter alia, where disclosure is necessary for an important ground of public interest recognized in Union or Member State law to which the controller is subject.

The only transfer rule that would allow a transfer absent an agreement is Article 49 of the GDPR, which permits derogations for specific circumstances. However, it is not clear if data transfers in response to CLOUD Act requests could be based on this exceptional provision, and it appears more likely than not that the leading authorities will interpret the exceptions very strictly, in line with the strong culture of data privacy in Europe.

[13] See Dep't of Justice, *Press Release: U.S. and UK Sign Landmark Cross-Border Data Access Agreement to Combat Criminals and Terrorists Online*, U.S. Dep't of Justice (Oct. 3, 2019), https://www.justice.gov/opa/pr/us-and-uk-sign-landmark-cross-border-data-access-agreement-combat-criminals-and-terrorists. The agreement is available here: https://tinyurl.com/y5mobx8v.

Appendices

Overview / Introduction

1. CLOUD Act, H.R. 1625, 115th Cong. div. V.
2. Brief for the United States, *United States v. Microsoft*, 138 S. Ct. 356 (2017), vacated and dismissed as moot, 138 S. Ct. 1186 (2018). Summary and Section C of Argument, U.S. Department of Justice, *Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act* (2019).
3. Frederick Davis & Anna Gressel, *Storm Clouds or Silver Linings? The Impact of the U.S. CLOUD Act*, 45 LITIGATION 1 (2018).
4. Ben Barnett et al., *Actual Impact of 2018 U.S. CLOUD Act Still Hazy,* LEXOLOGY (July 29, 2019), https://www.lexology.com/library/detail.aspx?g=179b5200-0308-4478-b14f-5e2d027ee058.
5. General Data Protection Regulation (GDPR), Regulation (E.U.) 2016/679 (Apr. 27, 2016). Only the provisions mentioned in the memo and the other annexes need to be considered.
6. *Paul M. Schwartz & Karl-Nikolaus Pfeifer*, Transatlantic Data Privacy Law, 106 GEO. L. J. 115 (2017). Introduction and Section I.

European Data Protection Representatives

7. Council of the European Union, Decision authorizing the opening of negotiations with a view to concluding an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters (May 21, 2019), ST 9114/19 and addendum ST 9666/19.
8. EDPS and EDPB, Initial legal assessment of the impact of the US CLOUD Act on the E.U. legal framework for the protection of personal data and the negotiations of an E.U.-US agreement on cross-border access to electronic evidence, Annex to letter of July 10, 2019 to the Chair of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE).
9. U.S. Dep't of Justice, *Press Release, Joint US-E.U. Statement on Electronic Evidence Sharing Negotiations*, U.S. DEP'T OF JUSTICE (Sept. 26, 2019), https://www.justice.gov/opa/pr/joint-us-eu-statement-electronic-evidence-sharing-negotiations.
10. Jennifer Daskal, *Privacy and Security Across Borders*, 128 YALE L.J. F. 1029 (2019), Introduction and Section II.B. (1039-1043).
11. European Commission, *Press Release, Fact Sheet and Q&A on e-Evidence Proposals*, EUR. COMM. (Apr. 2018), https://europa.eu/rapid/press-release_IP-18-3343_en.htm.

Privacy Advocates

Privacy issues under the CLOUD Act

12. Neema Singh Guliani & Naureen Shah, *The CLOUD Act Doesn't Help Privacy and Human Rights: It Hurts Them*, LAWFARE (Mar. 16, 2018), https://www.lawfareblog.com/cloud-act-doesnt-help-privacy-and-human-rights-it-hurts-them.

13. Christine Galvagna, *The Necessity of Human Rights Legal Protections in Mutual Legal Assistance Treaty Reform*, 9 NOTRE DAME J. INT'L & COMP. L. 57 (2019). Introduction, Section III.A.
14. Secil Bilgic, *Something Old, Something New, and Something Moot: The Privacy Crisis Under the CLOUD Act*, 32 HARV. J.L. & TECH. 321 (2018). Introduction, Sections IV.A. and IV.C.

Encryption

15. Harold Abelson et al., Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications, 1(1) JOURNAL OF CYBERSECURITY 69 (2015).
16. Jim Baker, Rethinking Encryption, LAWFARE (Oct. 22, 2019), https://www.lawfareblog.com/rethinking-encryption. Sections I and II.
17. Josh Benaloh, What if Responsible Encryption Back-Doors Were Possible?, LAWFARE (Nov. 29, 2018), https://www.lawfareblog.com/what-if-responsible-encryption-back-doors-were-possible.
18. William P. Barr, Keynote Address, International Conference on Cyber Security, https://justice.gov/opa/speech/attorney-general-william-p-barr-delivers-keynote-address-international-conference-cyber (July 23, 2019).
19. Sally Q. Yates and James B. Comey, Going Dark: Encryption, Technology, and the Balance between Public Safety and Privacy, Testimony before the Committee on the Judiciary of the United States Senate (July 8, 2015).

Cloud providers

1. Brad Smith, *The CLOUD Act is an important step forward, but now more steps need to follow*, MICROSOFT (Apr. 3, 2018), https://blogs.microsoft.com/on-the-issues/2018/04/03/the-cloud-act-is-an-important-step-forward-but-now-more-steps-need-to-follow/.
2. Michael Punke, *AWS and the CLOUD Act*, AWS SECURITY BLOG (May 27, 2019), https://aws.amazon.com/de/blogs/security/aws-and-the-cloud-act/.
3. Google, *Transparency Report: User Data Requests* (2019), https://transparencyreport.google.com/user-data/overview?hl=en.
4. Google, *White Paper Government Requests Google Cloud* (Oct. 2018),Tech Companies Letter of Support for Senate CLOUD Act (Feb. 6, 2018), https://blogs.microsoft.com/datalaw/wp-content/uploads/sites/149/2018/02/Tech-Companies-Letter-of-Support-for-Senate-CLOUD-Act-020618.pdf.
5. Microsoft Press Release, *Microsoft Announces Plans to Offer Cloud Services from German Datacenters* (Nov. 11, 2015), https://news.microsoft.com/europe/2015/11/11/45283/.
6. Microsoft Press Release, *Microsoft to deliver cloud services from new datacenters in Germany in 2019 to meet evolving customer needs* (Aug. 31, 2018), https://news.microsoft.com/europe/2018/08/31/microsoft-to-deliver-cloud-services-from-new-datacentres-in-germany-in-2019-to-meet-evolving-customer-needs/.
7. Paul Schwartz, *Legal Access to the Global Cloud*, 118 COLUM. L. REV. 1681 (2018). Introduction, Sections I.B. and II.A.2.

FinTech Coalition

8. Hal Scott et al., *Cloud Computing in the Financial Sector: A Global Perspective*, PROGRAM ON INTERNATIONAL FINANCIAL SYSTEMS (Jul. 2019), https://www.pifsinternational.org/wp-content/uploads/2019/07/Cloud-Computing-in-the-Financial-Sector_Global-Perspective-Final_July-2019.pdf. Sections 1 and 2.
9. *Google*, Government requests for customer data: controlling access to your data in Google Cloud (June 2019), https://services.google.com/fh/files/blogs/government_access_technical_whitepaper.pdf.

Legal Scholars

10. Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L. J. 326 (2015). Introduction, Section II.
11. Andrew Keane Woods, *Against Data Exceptionalism*, 68 STAN. L. REV. 729 (2016). Introduction, Section II.
12. Frederick T. Davis, *A U.S. Prosecutor's Access to Data Stored Abroad–Are There Limits?*, 49 INTERNATIONAL LAWYER 1 (2015). Skip Sections I to III.

Bibliography

In working on this eBook, we compiled an informal bibliography of recent articles and working papers exploring issues related to Fintech law. This bibliography is now posted at the Harvard University link given below. We will try to update this bibliography from time to time as more work appears. In the meantime, we welcome any and all suggestions for additions, corrections, or updates.

https://projects.iq.harvard.edu/fintechlaw/bibliography